



Release Notes for Catalyst 6500 Series Software Release 8.x

Current Releases

8.3(7)—April 1, 2005

8.4(2a)—March 31, 2005

Previous Releases: 8.4(2)—deferred, 8.4(1), 8.3(6), 8.3(5), 8.3(4), 8.3(3), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(3), 8.1(2), 8.1(1)



Note

Supervisor Engine 32 with the MSFC2A requires Cisco IOS Release 12.2(17d)SXB7.



Caution

With software release 8.3(1), we recommend that you run Cisco IOS Release 12.2(17d)SXB1 on the MSFC. It is mandatory that you run Cisco IOS Release 12.2(17d)SXB1 if you plan on using any of the following software release 8.3(1) features: Bidirectional PIM, Policy Feature Card 3BXL, IGMP version 3 snooping with Multicast Multilayer Switching (MMLS), or Gateway Load Balancing Protocol (GLBP). Note also that the FlexWAN module requires Cisco IOS Release 12.2(17d)SXB1 when running software release 8.3(1).



Caution

Support for Optical Services Modules (OSMs) and the FlexWAN module in systems with Supervisor Engine 2 running software release 8.1(1) and later releases requires Cisco IOS Release 12.1(19)E or later releases. OSMs are not supported with Supervisor Engine 1 or Supervisor Engine 720. Support for the FlexWAN module in systems with Supervisor Engine 1 running software release 8.1(1) and later releases requires Cisco IOS Release 12.1(19)E or later releases. Support for the FlexWAN module in systems with Supervisor Engine 720 running software release 8.2(1) and later releases requires Cisco IOS Release 12.2(14)SX2 or later releases.

Also note that with software release 8.1(1) and later releases you need to use the Cisco IOS Release 12.1(13)E4 or 12.1(13)E5 bootloader on the MSFC/MSFC2 to boot a Cisco IOS image reliably from sup-slot0 or sup-bootflash. The Cisco IOS Release 12.1(19)E train bootloader, or bootloaders earlier than Cisco IOS Release 12.1(13)E4, do not support booting the MSFC/MSFC2 from sup-slot0 or sup-bootflash due to caveats CSCeb36759, CSCdz60980, and/or CSCdz31321.

See the “Optical Services Modules” section on page 17 for a complete list of OSMs supported with Catalyst software.



Corporate Headquarters:

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

**Caution**

The MSFC3 on Supervisor Engine 720 requires Cisco IOS Release 12.2(14)SX2 or later releases.

**Caution**

The 12.2(14r)S9 MSFC3 ROMMON software upgrade is required if you plan to run Catalyst software release 8.1(x) on Supervisor Engine 720 and Cisco IOS software on the MSFC3. For information on the 12.2(14r)S9 MSFC3 ROMMON software upgrade procedure, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_4497.htm

Contents

This document consists of these sections:

- Release 8.x DRAM Memory Requirements, page 3
- Boot ROM (ROMMON) Requirements, page 3
- Upgrading the Boot ROM, page 4
- Flash PC Card Support, page 4
- Supervisor Engine Bootflash, page 6
- Redundant Supervisor Engine Configurations, page 6
- Product and Software Version Matrix, page 7
- Orderable Software Images, page 24
- Software Image Version Compatibility, page 29
- Catalyst 6500 Series Features, page 30
- Usage Guidelines and Restrictions, page 48
- Open and Resolved Caveats in Software Release 8.4(2a), page 74
- Open and Resolved Caveats in Software Release 8.4(2), page 76
- Open and Resolved Caveats in Software Release 8.4(1), page 82
- Open and Resolved Caveats in Software Release 8.3(7), page 87
- Open and Resolved Caveats in Software Release 8.3(6), page 90
- Open and Resolved Caveats in Software Release 8.3(5), page 94
- Open and Resolved Caveats in Software Release 8.3(4), page 97
- Open and Resolved Caveats in Software Release 8.3(3), page 105
- Open and Resolved Caveats in Software Release 8.3(2), page 113
- Open and Resolved Caveats in Software Release 8.3(1), page 119
- Open and Resolved Caveats in Software Release 8.2(2), page 126
- Open and Resolved Caveats in Software Release 8.2(1), page 133
- Open and Resolved Caveats in Software Release 8.1(3), page 140
- Open and Resolved Caveats in Software Release 8.1(2), page 142
- Open and Resolved Caveats in Software Release 8.1(1), page 145

- Catalyst Software Image Upgrade Procedure, page 149
- Troubleshooting, page 152
- Additional Documentation, page 157
- Obtaining Documentation, page 157
- Obtaining Technical Assistance, page 160
- Obtaining Additional Publications and Information, page 161

Release 8.x DRAM Memory Requirements

Supervisor Engine 32: The Catalyst 6500 series Supervisor Engine 32 ships with 256-MB DRAM, which fully supports software release 8.4(1) and later releases.

Supervisor Engine 720: The Catalyst 6500 series Supervisor Engine 720 ships with 512-MB DRAM, which fully supports software release 8.x.

Supervisor Engine 2: The Catalyst 6500 series Supervisor Engine 2 ships with 256-MB DRAM (WS-X6K-S2U-MSFC2) and the default 128-MB DRAM (WS-X6K-S2-MSFC2), both of which fully support software release 8.x.

Supervisor Engine 1: Early versions of the Catalyst 6500 series Supervisor Engine 1 shipped with 64-MB DRAM which does not support software release 8.x (currently, new Supervisor Engine 1 modules ship with 128-MB DRAM). To support software release 8.x, you need 128-MB DRAM.

With the exception of WS-X6K-SUP1A-MSFC, all other Supervisor Engine 1 modules can upgrade to 128-MB DRAM using the MEM-S1-128MB= upgrade kit. For detailed information on the MEM-S1-128MB= upgrade, refer to the *Catalyst 6500 Series Switch Supervisor Engine 1A DRAM Upgrade Installation Note* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14357.htm

To upgrade to 128-MB DRAM on the WS-X6K-SUP1A-MSFC, use the MEM-S1-128MB-UPG= upgrade kit *which also includes* an MSFC2 upgrade.

Boot ROM (ROMMON) Requirements

For Supervisor Engine 1, the minimum boot ROM (ROMMON) required for software release 5.4(1) and later 5.x(x) releases is 5.2(1). The minimum boot ROM required for software releases 6.x(x), 7.x(x), and 8.x(x) is also 5.2(1). The default (shipping) image for software releases 6.x(x), 7.x(x), and 8.x(x) is 5.3(1).

For Supervisor Engine 2, the minimum boot ROM required for software release 6.2(2) and later releases is 6.1(3).

For Supervisor Engine 720, the minimum boot ROM required for software release 8.1(1) and later releases is 7.7(1).



Note

The supervisor engine boot ROM versions must be identical in redundant systems.

Upgrading the Boot ROM

Follow these guidelines to upgrade the supervisor engine boot ROM (ROMMON) on Supervisor Engine 1 or 1A:

- For supervisor engines with an MSFC, due to the location of the boot ROM, upgrading the boot ROM could damage your supervisor engine. This hardware configuration is not field upgradable.
- For supervisor engines with an MSFC2 or no PFC, the boot ROM upgrade can be done in the field:
 - The boot ROM upgrade kit part number is WS-X6K-BOOT=



Note The boot ROM upgrade kit is not orderable. If an upgrade is needed, contact the Technical Assistance Center (TAC) to verify your hardware configuration and arrange for delivery of the upgrade kit.

- For boot ROM installation information, refer to the *Catalyst 6500 Series Switch Supervisor Engine NMP Boot ROM Upgrade Installation Note* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_10142.htm



Note

For Supervisor Engine 2 with boot ROM version 6.1(3) or later, the boot ROM software image can be upgraded through a software download from Cisco.com. Refer to the boot ROM software upgrade procedure at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_13488.htm

Flash PC Card Support

The following Flash PC cards are supported on Catalyst 6500 series switches:

- MEM-C6K-FLC16M(=)
- MEM-C6K-FLC24M(=)
- MEM-C6K-FLC64M(=)

Supported only on Supervisor Engine 1.

- MEM-C6K-ATA-1-64M(=)

Prior to software release 7.5(1), Supervisor Engine 1 and Supervisor Engine 2 supported the following Flash PC cards:

- 16-MB Flash PC card (MEM-C6K-FLC16M=). The device name is **slot0:**.
- 24-MB Flash PC card (MEM-C6K-FLC24M=). The device name is **slot0:**.

With software releases 7.5(1) and later, additional Flash PC card support was added as follows:

- 64-MB ATA Flash PC card (MEM-C6K-ATA-1-64M=)—Only supported on Supervisor Engine 2. The device name is **disk0:** and the card requires ROMMON version 7.1(1) or later releases.
- 64-MB linear Flash PC card (MEM-C6K-FLC64M=)—Only supported on Supervisor Engine 1. The device name is **slot0:** and the card requires ROMMON software release 5.3(1) or later releases.

**Note**

The MEM-C6K-ATA-1-64M(=) and MEM-C6K-FLC64M= Flash PC cards are not formatted. Although the cards appear to be formatted when first installed, you must format the cards to prevent possible data corruption.

**Note**

The 16-MB MEM-C6K-FLC16M(=) and 24-MB MEM-C6K-FLC24M(=) linear Flash PC cards are not formatted. Supervisor Engine 1 and Supervisor Engine 2 do not support the same Flash PC card format. To use a Flash PC card with Supervisor Engine 2, you must format the card with Supervisor Engine 2. To use a Flash PC card with Supervisor Engine 1, you must format the card with Supervisor Engine 1.

The following Compact Flash cards are supported only on Supervisor Engine 720 with software release 8.1(1) or later releases and Supervisor Engine 32 with software release 8.4(1) or later releases:

- MEM-C6K-CPTFL64M=
- MEM-C6K-CPTFL128M=
- MEM-C6K-CPTFL256M=

**Note**

For Supervisor Engine 720, a Compact Flash card can be installed only in the DISK 0 slot. Do not install it in the DISK 1 slot.

**Note**

For Supervisor Engine 1, software release 7.6(1) or later CV images need a 24-MB or 64-MB linear Flash PC card.

With the 24-MB linear Flash PC card with a Supervisor Engine 1/MSFC or a Supervisor Engine 1/MSFC2 with a 16-MB MSFC2 bootflash, you need to put the Catalyst image on the 24-MB linear Flash PC card, the IOS bootloader on the MSFC bootflash, and the Cisco IOS image on the 16-MB supervisor engine bootflash.

With the 64-MB linear Flash PC card with a Supervisor Engine 1/MSFC or a Supervisor Engine 1/MSFC2 with a 16-MB MSFC2 bootflash, you can put the Catalyst image and the MSFC/MSFC2 Cisco IOS image on the 64-MB linear Flash PC card, and the Cisco IOS bootloader on the MSFC bootflash.

With the 24-MB or 64-MB linear Flash PC card on a Supervisor Engine 1/MSFC2 with 32-MB MSFC2 bootflash, the MSFC2 bootloader and Cisco IOS image can be put on the MSFC2 bootflash, and the Catalyst image can be put on the 24-MB or 64-MB linear Flash PC cards.

Supervisor Engine Bootflash

Supervisor Engine 32: The Catalyst 6500 series Supervisor Engine 32 ships with a 256-MB bootflash device.

Supervisor Engine 720: The Catalyst 6500 series Supervisor Engine 720 ships with a 64-MB bootflash device.

Supervisor Engine 2: The Catalyst 6500 series Supervisor Engine 2 ships with a 32-MB bootflash device.



Note

The default bootflash configuration on Supervisor Engine 2 shipped since late January 2001, is 32 MB. Enter the show version command to determine what size bootflash device is installed on the Supervisor Engine 2. If you have 16 MB, there is an upgrade to 32 MB available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12667.htm

Supervisor Engine 1: The Catalyst 6500 series Supervisor Engine 1 (and 1A) ship with a 16-MB bootflash device. The Supervisor Engine 1 (and 1A) bootflash is not upgradeable.

Redundant Supervisor Engine Configurations

In systems with redundant supervisor engines, both supervisor engines must be identical and have the same daughter card configurations. For example, your switch can have the following configurations:

- Slot 1—Supervisor Engine 2, PFC2, MSFC2
Slot 2—Supervisor Engine 2, PFC2, MSFC2
- Slot 1—Supervisor Engine 2, PFC2
Slot 2—Supervisor Engine 2, PFC2
- Slot 1—Supervisor Engine 1, PFC, MSFC2
Slot 2—Supervisor Engine 1, PFC, MSFC2
- Slot 1—Supervisor Engine 1, PFC, MSFC1
Slot 2—Supervisor Engine 1, PFC, MSFC1
- Slot 1—Supervisor Engine 1, PFC
Slot 2—Supervisor Engine 1, PFC
- Slot 1—Supervisor Engine 1
Slot 2—Supervisor Engine 1

The slot locations for Supervisor Engine 720 (with PFC3 and MSFC3) and Supervisor Engine 32 (with PFC3B and MSFC2A) are chassis dependent:

- With a 3-slot chassis, install the active supervisor engine in slot 1 and the redundant supervisor engine in slot 2.
- With a 6-slot or a 9-slot chassis, install the active supervisor engine in slot 5 and the redundant supervisor engine in slot 6.
- With a 13-slot chassis, install the active supervisor engine in slot 7 and the redundant supervisor engine in slot 8.

These configuration requirements apply to all Catalyst 6500 series switches. We do not support configurations that are not identical.

Product and Software Version Matrix

These sections list the minimum supervisor engine version and the current recommended supervisor engine software version for Catalyst 6500 series modules, power supplies, fan trays, and chassis:

- Supervisor Engines, page 8
- Policy Feature Cards, page 10
- Switch Fabric Modules, page 11
- Small Form-Factor Pluggable Modules (SFPs), page 11
- 10-Gigabit Ethernet Switching Modules, page 12
- Gigabit Ethernet Switching Modules, page 13
- Fast Ethernet Switching Modules, page 14
- Ethernet/Fast Ethernet (10/100) Switching Modules, page 14
- Ethernet Switching Modules, page 16
- Voice Modules, page 16
- FlexWAN Module, page 17
- Optical Services Modules, page 17
- Service Modules, page 18
- ATM Modules, page 19
- Multilayer Switch Module, page 19
- Power Supplies, page 19
- Fan Trays, page 20
- Modular Chassis, page 21

**Note**

There might be additional minimum software version requirements for intelligent modules (those that run an additional, separate software image). Refer to the software release notes for the module type for more information.

Supervisor Engines



Note

Supervisor Engine 32 (WS-SUP32-GE-3B) common features:

- Supports 32-Gbps non-fabric-enabled switching bus (the WS-C6500-SFM and WS-C6500-SFM2 modules are not supported)
- 256-MB bootflash through an internal Compact Flash device (referred to as “bootdisk” in the CLI)
- Compact Flash slot (disk 0)
- One 10/100/1000 Mbps RJ-45 port (port 9)
- Two USB ports
 - Host port (Type B port) interfaces with a standard host such as a PC
 - Device port (Type A port) interfaces with devices such as USB disks or USB keys



Note

The USB ports are not enabled. These ports will be enabled in a future software release.

- QoS port architecture (Rx/Tx): **2q8t/1p3q8t**
- Eight Gigabit Ethernet SFP ports (ports 1 through 8) on WS-SUP32-GE-3B



Note

For a list of supported SFPs, see the “Small Form-Factor Pluggable Modules (SFPs)” section on page 11.

- For Supervisor Engine 32 fan tray requirements, see the “Fan Trays” section on page 20



Note

Supervisor Engine 720 common features:

- Integrated 720-Gbps Switch Fabric
- 64-MB bootflash device
- 2 Compact Flash slots (disk0 and disk1)
- Two Ethernet uplink ports:
 - 1-MB packet buffer per port
 - Port 1—Gigabit Ethernet SFP
 - Port 2—Configurable as Gigabit Ethernet SFP or 10/100/1000 Mbps RJ-45



Note

For a list of supported SFPs, see the “Small Form-Factor Pluggable Modules (SFPs)” section on page 11.

- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- For Supervisor Engine 720 fan tray requirements, see the “Fan Trays” section on page 20

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Supervisor Engine 32			
WS-SUP32-GE-3B	Supervisor Engine 32 with PFC3B: <ul style="list-style-type: none"> • 256-MB DRAM • Policy Feature Card 3B; see the “Policy Feature Cards” section on page 10 • Multilayer Switch Feature Card 2A (MSFC2A) <ul style="list-style-type: none"> – 256-MB DRAM – 32-MB bootflash 	8.4(1)	8.4(1)
Supervisor Engine 720¹			
WS-SUP720-3B ²	Supervisor Engine 720 with PFC3B: <ul style="list-style-type: none"> • 512-MB DRAM • Policy Feature Card 3B; see the “Policy Feature Cards” section on page 10 • Multilayer Switch Feature Card 3 (MSFC3): <ul style="list-style-type: none"> – 512-MB DRAM – 64-MB bootflash <p>Note</p> <ul style="list-style-type: none"> • There are no memory-only upgrade options for WS-SUP720-3B. • Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. Refer to this publication for more information: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm 	8.4(1)	8.4(1)
WS-SUP720-3BXL ²	Supervisor Engine 720 with PFC3BXL: <ul style="list-style-type: none"> • 1-GB DRAM • Policy Feature Card 3BXL; see the “Policy Feature Cards” section on page 10 • Multilayer Switch Feature Card 3 (MSFC3): <ul style="list-style-type: none"> – 1-GB DRAM – 64-MB bootflash <p>Note There are no memory upgrade options for WS-SUP720-3BXL.</p>	8.3(1)	8.3(3)
WS-SUP720	Supervisor Engine 720 with the following features: <ul style="list-style-type: none"> • 512-MB DRAM • Policy Feature Card 3A (PFC3A); see the “Policy Feature Cards” section on page 10 • Multilayer Switch Feature Card 3 (MSFC3) with 64-MB bootflash device and 512-MB DRAM 	8.1(1)	8.3(3)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Supervisor Engine 2			
WS-X6K-S2U-MSFC2	Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, CEF, PFC2, and MSFC2 256 MB on supervisor engine, 256 MB on MSFC2 QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	6.1(1d)	6.4(11)
WS-X6K-S2-MSFC2	Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, CEF, PFC2, and MSFC2 128 MB on supervisor engine, 128 MB on MSFC2 QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	6.1(1d)	6.4(11)
WS-X6K-S2-PFC2	Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled, and PFC2 QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	6.1(1d)	6.4(11)
Supervisor Engine 1³			
WS-X6K-S1A-MSFC2	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, PFC, and MSFC2 QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.4(3)	6.4(11)
WS-X6K-SUP1A-MSFC	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, PFC, and MSFC QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.3(1a)CSX	6.4(11)
WS-X6K-SUP1A-PFC	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks, and PFC QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.3(1a)CSX	6.4(11)
WS-X6K-SUP1A-2GE ⁴	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.3(1a)CSX	6.4(11)

- Supervisor Engine 720 requires a 2500 W or 4000 W power supply in all 6-, 9-, and 13-slot chassis.
- With software release 8.3(1), WS-SUP720-3BXL and WS-SUP720-3B support the same feature set and have the same performance characteristics as WS-F6K-PFC3A.
- Not supported in the WS-C6513 chassis.
- Note that while the WS-X6K-SUP1A-2GE module is supported in software release 8.x; the WS-X6K-SUP1-2GE module is not supported in software release 8.x.

Policy Feature Cards



Note

- The PFC2 supports a theoretical maximum of 128 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 supports a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- You cannot use a PFC3BXL or a PFC3B on one supervisor engine and a PFC3A on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
PFC3B ¹	Policy Feature Card 3B (PFC3B)	8.4(1)	8.4(1)
PFC3BXL ¹	Policy Feature Card 3BXL (PFC3BXL)	8.3(1)	8.3(3)
PFC3A ²	Policy Feature Card 3A (PFC3A)	8.1(1)	8.3(3)

For PFC and PFC2 information, see the “Supervisor Engines” section on page 8.

1. Supported on Supervisor Engine 720 and Supervisor Engine 32.
2. Supported only with Supervisor Engine 720.

Switch Fabric Modules



Note

- The Switch Fabric Modules are not supported with Supervisor Engine 720 because the Supervisor Engine 720 has an integrated switch fabric.
- The WS-C6500-SFM2 and the WS-X6500-SFM are supported only in systems with a Supervisor Engine 2.
- Except in a 13-slot chassis, WS-X6500-SFM2 and WS-C6500-SFM can be used together to provide redundancy.
- 3-slot chassis do not support WS-X6500-SFM2 or WS-C6500-SFM.

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-C6500-SFM	Switch Fabric Module to support fabric-enabled modules	6.1(1d)	6.4(11)
WS-X6500-SFM2	Switch Fabric Module version 2	6.2(2)	6.4(11)

Small Form-Factor Pluggable Modules (SFPs)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
CWDM-SFP	1000BASE-CWDM SFP	8.3(1)	8.3(3)
GLC-T	1000BASE-T SFP	8.3(1)	8.3(3)
GLC-LH-SM	1000BASE-LX/LH SFP	8.1(1)	8.3(3)
GLC-SX-MM	1000BASE-SX SFP	8.1(1)	8.3(3)
GLC-ZX-SM	1000BASE-ZX SFP	8.2(1)	8.3(3)
GLC-FE-100FX ¹	100BASE-FX SFP	8.4(1)	8.4(1)
GLC-FE-100LX ¹	100BASE-LX SFP	8.4(1)	8.4(1)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
GLC-FE-100BX-U ¹ GLC-FE-100BX-D ¹	100BASE-BX SFP	8.4(1)	8.4(1)
GLC-BX-1310 GLC-BX-1490	1000BASE-BX SFP	8.4(1)	8.4(1)

1. Supported with the WS-X6148-FE-SFP module.

10-Gigabit Ethernet Switching Modules

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6502-10GE	1-port 10GBASE-E Serial 10-Gigabit Ethernet, fabric-enabled QoS port architecture (Rx/Tx): 1p1q8t/1p2q1t Note: The WS-X6502-10GE module does not support ISL encapsulation.	7.1(1)	7.6(9)
WS-G6483	10GBASE-ER Serial 1550-nm extended-reach Optical Interface Module (OIM)	7.2(2)	7.6(9)
WS-G6488	10GBASE-LR Serial 1310-nm long-haul OIM	7.1(1)	7.6(9)
WS-X6704-10GE ^{1, 2, 3}	4-port 10-Gigabit Ethernet, requires XENPAKs, fabric-enabled QoS port architecture (Rx/Tx): 1q8t/1p7q8t	8.1(2)	8.3(3)
XENPAK-10GB-LR	Up to 10-kilometer range, 10GBASE-LR Serial 1310-nm long-haul (SMF)	8.1(2)	8.3(3)
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	8.2(1)	8.3(3)
XENPAK-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach (SMF)	8.2(1)	8.3(3)
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multi-mode (MMF)	8.3(1)	8.3(3)
XENPAK-10GB-CX4	10GBASE-CX4 provides support for copper up to 15 meters on CX4 cable	8.3(1)	8.3(3)

1. Not supported in a 6503 chassis in software releases prior to release 8.4(1). Supported in the 6503-E chassis with software release 8.4(1) and later releases.
2. In a 13-slot chassis, this module must be installed in slots 9, 10, 11, 12, or 13.
3. Supported only with Supervisor Engine 720.

Gigabit Ethernet Switching Modules

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6148A-GE-TX WS-X6148A-GE-45AF	48-port 10/100/1000BASE-T switching module, RJ-45 (WS-X6148A-GE-45AF provides inline power to IP telephones) QoS port architecture (Rx/Tx): 1q2t/1p3q8t	8.4(1)	8.4(1)
WS-X6748-GE-TX ^{1, 2, 3}	48-port 10/100/1000BASE-TX switching module, RJ-45, fabric-enabled QoS port architecture (Rx/Tx): 1q8t/1p3q8t	8.1(2)	8.3(3)
WS-X6748-SFP ^{1, 2, 3}	48-port Gigabit Ethernet switching module, requires SFPs, fabric enabled QoS port architecture (Rx/Tx): 1q8t/1p3q8t Note For a list of supported SFPs, see the “Small Form-Factor Pluggable Modules (SFPs)” section on page 11.	8.3(2)	8.3(3)
WS-X6724-SFP ^{1, 3}	24-port Gigabit Ethernet switching module, requires SFPs, fabric-enabled QoS port architecture (Rx/Tx): 1q8t/1p3q8t Note For a list of supported SFPs, see the “Small Form-Factor Pluggable Modules (SFPs)” section on page 11.	8.1(2)	8.3(3)
WS-X6148-GE-TX WS-X6148V-GE-TX WS-X6148-GE-45AF ⁴	48-port 10/100/1000BASE-TX switching module (WS-X6148V-GE-TX and WS-X6148-GE-45AF provide inline power to IP telephones) QoS port architecture (Rx/Tx): 1q2t/1p2q2t	7.6(1)	7.6(9)
WS-X6548-GE-TX WS-X6548V-GE-TX WS-X6548-GE-45AF ⁴	48-port 10/100/1000BASE-TX switching module, fabric-enabled (WS-X6548V-GE-TX and WS-X6548-GE-45AF provide inline power to IP telephones) QoS port architecture (Rx/Tx): 1q2t/1p2q2t	7.6(1)	7.6(9)
WS-X6516A-GBIC	16-port Gigabit Ethernet GBIC switching module, fabric-enabled, 1-MB per-port packet buffers QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	7.5(1)	7.6(9)
WS-X6516-GBIC	16-port Gigabit Ethernet GBIC switching module, fabric-enabled QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	6.1(1d)	6.4(11)
WS-X6516-GE-TX	16-port 10/100/1000BASE-T Ethernet Module, fabric-enabled QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	6.2(2)	6.4(11)
WS-X6416-GBIC	16-port Gigabit Ethernet GBIC switching module QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.4(2)	6.4(11)
WS-X6416-GE-MT	16-port Gigabit Ethernet MT-RJ QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.3(5a)CSX	6.4(11)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6316-GE-TX	16-port 1000BASE-TX RJ-45 Gigabit Ethernet QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.4(2)	6.4(11)
WS-X6408A-GBIC	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): 1p1q4t/1p2q2t	5.3(1a)CSX	6.4(11)
WS-X6408-GBIC	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): 1q4t/2q2t	5.1(1)CSX	6.4(11)

1. Not supported in a 6503 chassis in software releases prior to release 8.4(1). Supported in the 6503-E chassis with software release 8.4(1) and later releases.
2. In a 13-slot chassis, this module must be installed in slots 9, 10, 11, 12, or 13.
3. Supported only with Supervisor Engine 720.
4. Supported in software release 8.2(1) and later releases.

Fast Ethernet Switching Modules

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6148-FE-SFP	48-port 100BASE-FX, requires SFPs QoS port architecture (Rx/Tx): 1p1q4t/1p3q8t Note For a list of supported SFPs, see the "Small Form-Factor Pluggable Modules (SFPs)" section on page 11.	8.4(1)	8.4(1)
WS-X6524-100FX-MM	24-port 100BASE-FX multimode, fabric-enabled QoS port architecture (Rx/Tx): 1p1q0t/1p3q1t	7.1(1)	7.6(9)
WS-X6324-100FX-SM WS-X6324-100FX-MM	24-port 100BASE-FX single mode or multimode, MT-RJ with 128K per-port packet buffers QoS port architecture (Rx/Tx): 1q4t/2q2t	5.4(2)	6.4(11)
WS-X6224-100FX-MT	24-port 100BASE-FX multimode, MT-RJ QoS port architecture (Rx/Tx): 1q4t/2q2t	5.1(1)CSX	6.4(11)

Ethernet/Fast Ethernet (10/100) Switching Modules

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6196-RJ-21 WS-X6196-21AF	96-port, 10/100BASE-TX RJ-21 (WS-X6196-21AF provides inline power to IP telephones) QoS port architecture: 1p1q0t/1p3q1t	8.4(1)	8.4(1)
WS-X6148A-RJ-45 WS-X6148A-45AF	48-port 10/100BASE-TX RJ-45 with 128K per-port packet buffers (WS-X6148A-45AF provides inline power to IP telephones) QoS port architecture (Rx/Tx): 1p1q4t/1p3q8t	8.4(1)	8.4(1)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6148X2-RJ-45 WS-X6148X2-45AF	96-port 10/100BASE-TX RJ-45, (WS-X6148X2-45AF provides inline power to IP telephones using the voice daughter card [WS-F6K-FE48X2-AF]) QoS port architecture (Rx/Tx): 1p1q0t/1p3q1t	8.2(1)	8.3(3)
WS-X6548-RJ-21	48-port 10/100BASE-TX RJ-21, fabric-enabled QoS port architecture (Rx/Tx): 1p1q0t/1p3q1t	6.2(2)	6.4(11)
WS-X6548-RJ-45	48-port 10/100BASE-TX RJ-45, fabric-enabled QoS port architecture (Rx/Tx): 1p1q0t/1p3q1t	6.2(2)	6.4(11)
WS-X6348-RJ21V	48-port 10/100BASE-TX RJ-21 with 128K per-port packet buffers (WS-X6348-RJ21V provides inline power to IP telephones) QoS port architecture (Rx/Tx): 1q4t/2q2t	6.2(2)	6.4(11)
WS-X6348-RJ-45 WS-X6348-RJ-45V	48-port 10/100BASE-TX RJ-45 with 128K per-port packet buffers (WS-X6348-RJ-45 accepts a field-upgradable voice daughter card to provide inline power to IP telephones. Already installed on WS-X6348-RJ-45V) QoS port architecture (Rx/Tx): 1q4t/2q2t	Without WS-F6K-VPWR: 5.4(2) With WS-F6K-VPWR: 5.5(1)	Without WS-F6K-VPWR: 6.4(11) With WS-F6K-VPWR: 6.4(11)
WS-X6148-RJ-45 WS-X6148-RJ-45V	48-port 10/100BASE-TX RJ-45 with 128K per-port packet buffers (WS-X6148-RJ-45V provides inline power to IP telephones) QoS port architecture (Rx/Tx): 1q4t/2q2t	For software releases 6.x: 6.4(1) For software releases 7.x: 7.2(2)	For software releases 6.x: 6.4(11) For software releases 7.x: 7.6(9)
WS-X6148-RJ21 WS-X6148-RJ21V	48-port 10/100BASE-TX RJ-21 with 128K per-port packet buffers (WS-X6148-RJ21V provides inline power to IP telephones) QoS port architecture (Rx/Tx): 1q4t/2q2t	For software releases 6.x: 6.4(1) For software releases 7.x: 7.2(2)	For software releases 6.x: 6.4(11) For software releases 7.x: 7.6(9)
WS-X6148-45AF	48-port 10/100BASE-TX RJ-45 with 128K per-port packet buffers (WS-X6148-45AF has the WS-F6K-FE48-AF daughter card to provide inline power to IP telephones) QoS port architecture (Rx/Tx): 1q4t/2q2t	8.2(1)	8.3(3)
WS-X6148-21AF	48-port 10/100BASE-TX RJ-21 with 128K per-port packet buffers (WS-X6148-21AF has the WS-F6K-FE48-AF daughter card to provide inline power to IP telephones) QoS port architecture (Rx/Tx): 1q4t/2q2t	8.2(1)	8.3(3)
WS-F6K-VPWR	Inline-power field-upgrade module mounts on the 48-port 10/100BASE-TX RJ-45 and RJ-21 modules	5.5(1)	6.4(11)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6248-RJ-45	48-port 10/100BASE-TX RJ-45 QoS port architecture (Rx/Tx): 1q4t/2q2t	5.1(1)CSX	6.4(11)
WS-X6248A-TEL	48-port 10/100BASE-TX RJ-21 with 128K per-port packet buffers QoS port architecture (Rx/Tx): 1q4t/2q2t	5.3(2)CSX	6.4(11)
WS-X6248-TEL	48-port 10/100BASE-TX RJ-21 QoS port architecture (Rx/Tx): 1q4t/2q2t	5.2(1)CSX	6.4(11)

Ethernet Switching Modules

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6024-10FL-MT	24-port 10BASE-FL MT-RJ QoS port architecture (Rx/Tx): 1q4t/2q2t	5.3(3)CSX	6.4(11)

Voice Modules

Product Number append with "=" for spares	Product Description ¹	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-SVC-CMM	Communication Media Module	8.1(1) ²	8.3(3)
WS-SVC-CMM-6E	16-port E1 interface port adapter	8.1 (1)	8.3(3)
WS-SVC-CMM-6T1	6-port T1 interface port adapter	8.1(1)	8.3(3)
WS-SVC-CMM-24FXS	24-port FXS interface port adapter	8.1(1)	8.3(3)
WS-SVC-CMM-ACT	Ad-hoc conferencing and transcoding port adapter	8.1(1)	8.3(3)
WS-X6624-FXS	24-port FXS analog interface module	5.5(1)	6.4(11)
WS-X6608-T1 WS-X6608-E1	8-port T1/E1 PSTN interface modules	5.5(1)	6.4(11)

- The voice modules are not supported with Supervisor Engine 720 in software release 8.1(x). The voice modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases.
- The 12.2(2)YK1 and 12.2(2)ZC CMM trains are deferred. The 12.2(13)ZP2 CMM train is orderable on CCO. For specific information on CMM software release 12.2(13)ZP2, see the CMM software release notes for 12.2(13)ZP2 at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_4847.htm

FlexWAN Module

Product Number append with "=" for spares	Product Description ^{1, 2}	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6182-2PA	FlexWAN Module	5.4(2)	6.4(11)

1. The FlexWAN module is not supported with Supervisor Engine 720 in software release 8.1(x). The FlexWAN module is supported with Supervisor Engine 720 in software release 8.2(1) and later releases. See the first "Caution" on page 1 for detailed information on FlexWAN module support.
2. Refer to the *Catalyst 6500 Series Switch FlexWAN Module Installation and Configuration Note*.

Optical Services Modules

Product Number append with "=" for spares	Product Description ^{1, 2, 3}	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
4-port Gigabit Ethernet WAN			
OSM-4GE-WAN-GBIC	4-port Gigabit Ethernet Optical Services Module	6.1(2)	6.4(11)
OC-12 Packet over SONET⁴			
OSM-2OC12-POS-MM	2-port OC-12c/STM-4c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-2OC12-POS-SI	2-port OC-12c/STM-4c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-2OC12-POS-SL	2-port OC-12c/STM-4c POS Optical Services Module, SM-LR ⁵ , with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-4OC12-POS-MM	4-port OC-12c/STM-4c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-4OC12-POS-SI	4-port OC-12c/STM-4c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-4OC12-POS-SL	4-port OC-12c/STM-4c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OC-3 Packet over SONET³			
OSM-4OC3-POS-SI	4-port OC-3c/STM-1c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	7.1(1)	7.6(9)
OSM-8OC3-POS-MM	8-port OC-3c/STM-1c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-8OC3-POS-SI	8-port OC-3c/STM-1c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-8OC3-POS-SL	8-port OC-3c/STM-1c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-16OC3-POS-MM	16-port OC-3c/STM-1c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OSM-16OC3-POS-SI	16-port OC-3c/STM-1c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)

Product Number append with "=" for spares	Product Description ^{1, 2, 3}	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
OSM-16OC3-POS-SL	16-port OC-3c/STM-1c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)
OC-48 Packet over SONET³			
OSM-10C48-POS-SS	1-port OC-48c/STM-16c POS Optical Services Module, SM-SR, with 4 Gigabit Ethernet ports	6.1(3)	6.4(11)
OSM-10C48-POS-SI	1-port OC-48c/STM-16c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(3)	6.4(11)
OSM-10C48-POS-SL	1-port OC-48c/STM-16c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(3)	6.4(11)

1. The OSMs are not supported with Supervisor Engine 1 or Supervisor Engine 720.
2. Refer to the *Optical Services Module Installation and Configuration Note*.
3. Channelized OSMs are not supported on Catalyst 6500 series switches; they are supported only on the Cisco 7600 series router platform.
4. Also has four Layer 2 Gigabit Ethernet ports.
5. Single-mode, long reach.

Service Modules

Product Number append with "=" for spares	Product Description ¹	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Intrusion Detection System Module (IDSM)²			
WS-X6381-IDS ³	Intrusion Detection System Module	6.1(1d)	6.4(11)
WS-SVC-IDSM2-BUN-K9	Intrusion Detection System Module 2	7.5(1)	7.6(9)
Network Analysis Module (NAM)^{4, 5}			
WS-X6380-NAM ³	Network Analysis Module, 256-MB RAM	5.5(1)	6.4(11)
WS-SVC-NAM-1	Network Analysis Module, 512-MB RAM, fabric-enabled	7.3(1)	7.6(9)
WS-SVC-NAM-2	Network Analysis Module, 1-GB RAM, fabric enabled, accelerator daughter card	7.3(1)	7.6(9)
Firewall Services Module⁶			
WS-SVC-FWM-1-K9	Firewall Services Module	7.5(1)	7.6(9)
SSL Services Module⁷			
WS-SVC-SSL-1	SSL Services Module	7.5(1)	7.6(9)
Content Switching Module (CSM)⁸			
WS-X6066-SLB-APC	Content Switching Module	7.5(1)	7.6(9)
Content Services Gateway (CSG)⁹			
WS-SVC-CSG-1	Content Services Gateway	7.6(1)	7.6(9)

1. The service modules are not supported with Supervisor Engine 720 in software release 8.1(x). The service modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases.

2. Refer to the *Catalyst 6500 Series Switch Intrusion Detection System Module Installation and Configuration Note*.
3. Not supported with Supervisor Engine 720 or Supervisor Engine 32.
4. Refer to the *Network Analysis Module Installation and Configuration Note*.
5. The Network Analysis Module (NAM) application image 1.1(1a) and NAM maintenance image 1.1(1a)m are not supported with supervisor engine software releases 6.3(2) and later. For supervisor engine software releases 6.3(2) and later, use the 1.2 NAM image.
6. Refer to the *Catalyst 6500 Series Switch and 7600 Series Firewall Services Module Installation and Configuration Note*.
7. Refer to the *Catalyst 6500 Series Switch SSL Services Module Installation and Configuration Note*.
8. Refer to the *Cisco Content Switching Module Installation and Configuration Guide*.
9. Refer to the *Cisco Content Services Gateway Installation and Configuration Guide*.

ATM Modules

Product Number append with "=" for spares	Product Description ^{1, 2}	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6101-OC12-SMF	Single-port single-mode OC-12 ATM	5.3(2)CSX	6.4(11)
WS-X6101-OC12-MMF	Single-port multimode OC-12 ATM	5.3(2)CSX	6.4(11)

1. The ATM modules are not supported with the Supervisor Engine 720 in software release 8.1(x). The ATM modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases.
2. Refer to the *ATM Configuration Guide and Command Reference*.

Multilayer Switch Module

Product Number append with "=" for spares	Product Description ^{1, 2}	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X6302-MSM	Multilayer Switch Module	5.2(1)CSX	6.4(11)

1. The Multilayer Switch Module is not supported with the Supervisor Engine 720 (there will be no Supervisor Engine 720 support in any future software releases).
2. Refer to the *Multilayer Switch Module Release Notes*.

Power Supplies

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-CAC-6000W ¹	6000 W AC power supply	8.4(1)	8.4(1)
PWR-2700-AC ²	2700 W AC power supply	8.4(1)	8.4(1)
PWR-2700-DC ²	2700 W DC power supply	8.4(1)	8.4(1)
WS-CAC-1000W	1000 W AC power supply	5.1(1)CSX	6.4(11)
WS-CAC-1300W	1300 W AC power supply	5.1(1)CSX	6.4(11)
WS-CDC-1300W	1300 W DC power supply	5.1(1)CSX	6.4(11)
PWR-1400-AC ³	1400 W AC power supply	8.1(1)	8.3(3)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-CAC-2500W	2500 W AC power supply	5.4(2)	6.4(11)
WS-CDC-2500W	2500 W DC power supply	5.4(2)	6.4(11)
WS-CAC-3000W	3000W AC power supply	7.5(1)	7.6(9)
WS-CAC-4000W	4000 W AC power supply	6.1(3)	6.4(11)
PWR-4000-DC ⁴	4000 W DC power supply	6.1(3)	8.3(3)
PWR-950-AC ³	950 W AC power supply	7.5(1)	7.6(9)
PWR-950-DC ³	950 W DC power supply	7.5(1)	7.6(9)
PWR-1900-AC/6 ⁵	1900 W AC power supply	7.2(2)	7.6(9)
PWR-1900-DC ⁵	1900 W DC power supply	7.2(2)	7.6(9)

- Supported in all 65xx and 65xx-E chassis except for the 6503 and 6503-E (form-factor difference). Only the 6513 and -E chassis support the full 6000W; the other chassis rely on software to current limit the power supply.
- Supported in the 7606 chassis and the 6504-E chassis. Support in the 6504-E chassis requires software release 8.4(2) or later releases.
- Supported only on the WS-C6503, WS-C6503-E, and CISCO7603 chassis.
- The full 4000W is only available with software release 8.1(1) and later releases. With software release 6.1(3) and later 6.x and 7.x releases, the maximum wattage is 2506.56W.
- Supported only on the CISCO7606 chassis.

Fan Trays

Product Number append with "=" for spares	Product Description ¹	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
FAN-MOD-3	Standard-capacity fan tray for 6503 chassis Standard-capacity fan tray for 7603 chassis	7.4(2) 7.1(1)	7.6(9) 7.6(9)
FAN-MOD-3HS	High-capacity fan tray for 6503/7603 chassis	8.1(1)	8.3(3)
FAN-MOD-4HS	High-capacity fan tray for the 6504 chassis	8.4(2)	8.4(2)
WS-C6K-6SLOT-FAN	Standard-capacity fan tray for 6506 chassis	5.2(1)CSX	6.4(11)
WS-C6K-6SLOT-FAN ²	High-capacity fan tray for 6506 chassis	8.1(1)	8.3(3)
WS-C6K-9SLOT-FAN	Standard-capacity fan tray for 6509 chassis	5.1(1)CSX	6.4(11)
WS-C6K-9SLOT-FAN ^{2,3}	High-capacity fan tray for 6509 chassis	8.1(1)	8.3(3)
WS-C6K-13SLOT-FAN	Standard-capacity fan tray for 6513 chassis Standard-capacity fan tray for 7613 chassis	6.2(2) 7.6(1)	6.4(11) 7.6(9)
WS-C6K-13SLT-FAN ²	High-capacity fan tray for 6513/7613 chassis	8.1(1)	8.3(3)
FAN-MOD-6	Standard-capacity fan tray for 7606 chassis	7.2(2)	7.6(9)
FAN-MOD-6HS ²	High-capacity fan tray for 7606 chassis	8.1(1)	8.3(3)
WS-C6506-E-FAN ²	High-capacity fan tray for WS-C6506-E chassis	6.3(7)	8.3(3)
WS-C6509-E-FAN ²	High-capacity fan tray for WS-C6509-E chassis	6.3(7)	8.3(3)
WS-C6503-E-FAN ²	High-capacity fan tray for WS-C6503-E chassis	6.3(7)	8.3(3)

Product Number append with "=" for spares	Product Description ¹	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
FAN-MOD-09	Standard-capacity fan tray for 6509-NEB-A/7609 chassis	8.1(1)	8.3(3)
FAN-MOD-09-HS ²	High-capacity fan tray for 6509-NEB-A/7609 chassis	8.1(1)	8.3(3)
WS-C6509-NEB-FAN	Standard-capacity fan tray for 6509-NEB chassis	5.4(2)	6.4(11)

1. Some chassis require a high capacity fan tray for use with Supervisor Engine 720 and Supervisor Engine 32. To determine which chassis require a fan tray for Supervisor Engine 720 and Supervisor Engine 32, see the "Modular Chassis" section on page 21.
2. These fan trays require a 2500 W or 4000 W power supply.
3. This fan tray is supported in all chassis (except for the 3-slot chassis) and all software releases. The minimum power supply requirement is 2500W. It is important that you determine the power requirements for your hardware configuration to ensure that your switch has adequate power for all modules. To determine power requirements, refer to the CCO power calculator at this URL: <http://www.cisco.com/go/powercalculator>.

Modular Chassis

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-C6513	Catalyst 6513 chassis: <ul style="list-style-type: none"> • 13 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2, Supervisor Engine 720, and Supervisor Engine 32 • Supervisor Engine 720 and Supervisor Engine 32 require WS-C6K-13SLT-FAN2. Each power supply in the chassis must be at least 2500 W 	6.2(2)	6.4(11)
WS-C6509-E ²	Catalyst 6509 chassis: <ul style="list-style-type: none"> • 9 slots • 1024 chassis MAC addresses • Requires WS-C6509-E-FAN 	5.4(2)	6.4(11)
WS-C6509	Catalyst 6509 chassis: <ul style="list-style-type: none"> • 9 slots • 1024 chassis MAC addresses • Supervisor Engine 720 and Supervisor Engine 32 require WS-C6K-9SLOT-FAN2. Each power supply in the chassis must be at least 2500 W 	5.1(1)CSX	6.4(11)
WS-C6509-NEB ¹	Catalyst 6509-NEB chassis: <ul style="list-style-type: none"> • 9 vertical slots • 1024 chassis MAC addresses 	5.4(2)	6.4(11)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-C6509-NEB-A ²	Catalyst 6509-NEB-A chassis: <ul style="list-style-type: none"> • 9 vertical slots • 64 chassis MAC addresses • No fan tray upgrade needed to use Supervisor Engine 720 and Supervisor Engine 32 	8.1(1)	8.3(3)
WS-C6506-E ²	Catalyst 6506 chassis: <ul style="list-style-type: none"> • 6 slots • 1024 chassis MAC addresses • Requires WS-C6506-E-FAN 	5.4(2)	6.4(11)
WS-C6506	Catalyst 6506 chassis: <ul style="list-style-type: none"> • 6 slots • 1024 chassis MAC addresses • Supervisor Engine 720 and Supervisor Engine 32 require WS-C6K-6SLOT-FAN2. Each power supply in the chassis must be at least 2500 W 	5.2(1)CSX	6.4(11)
WS-C6504-E	Catalyst 6504 chassis: <ul style="list-style-type: none"> • 4 slots • 64 chassis MAC addresses • Does not support: <ul style="list-style-type: none"> – WS-X6500-SFM2 – WS-C6500-SFM 	8.4(2)	8.4(2)
WS-C6503-E ³	Catalyst 6503 chassis: <ul style="list-style-type: none"> • 3 slots • 64 chassis MAC addresses • Supervisor Engine 720 and Supervisor Engine 32 require WS-C6503-E-FAN • Does not support: <ul style="list-style-type: none"> – WS-X6500-SFM2 – WS-C6500-SFM 	5.4(2)	6.4(11)
WS-C6503	Catalyst 6503 chassis: <ul style="list-style-type: none"> • 3 slots • 64 chassis MAC addresses • Does not support SFM • Supervisor Engine 720 and Supervisor Engine 32 require FAN-MOD-3HS= 	7.4(2)	7.6(9)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-C6009	Catalyst 6009 chassis: <ul style="list-style-type: none"> • 9 slots • 1024 chassis MAC addresses 	5.1(1)CSX	6.4(11)
WS-C6006	Catalyst 6006 chassis: <ul style="list-style-type: none"> • 6 slots • 1024 chassis MAC addresses 	5.2(1)CSX	6.4(11)
OSR-7609-AC, -DC ¹	Cisco 7609 router chassis: <ul style="list-style-type: none"> • 9 vertical slots • 1024 chassis MAC addresses • Supported only with Supervisor Engine 2 	6.1(1b)	6.4(11)
CISCO7603	Cisco 7603 router chassis: <ul style="list-style-type: none"> • 3 slots • 64 chassis MAC addresses • Does not support SFM • Supervisor Engine 720 and Supervisor Engine 32 require FAN-MOD-3HS= 	7.1(1)	7.6(9)
CISCO7606	Cisco 7606 router chassis: <ul style="list-style-type: none"> • 6 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2 and Supervisor Engine 720 • Supervisor Engine 720 and Supervisor Engine 32 require FAN-MOD-6HS 	7.2(2)	7.6(9)
CISCO7609 ²	Cisco 7609 router chassis: <ul style="list-style-type: none"> • 9 vertical slots • 64 chassis MAC addresses • No fan tray upgrade needed to use Supervisor Engine 720 and Supervisor Engine 32 	8.1(1)	8.3(3)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
CISCO7613	Cisco 7613 router chassis: <ul style="list-style-type: none"> • 13 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2 and Supervisor Engine 720 • Supervisor Engine 720 and Supervisor Engine 32 require WS-C6K-13SLT-FAN2. Each power supply in the chassis must be at least 2500 W 	7.6(1)	7.6(9)

1. These chassis are not supported with Supervisor Engine 720 in Release 8.1(x) and 8.2(x).
2. These chassis require a 2500 W or 4000 W power supply. Lower wattage power supplies are not supported.
3. Supervisor Engine 720 requires software release 8.1(1) or later releases and the WS-C6503-E-FAN tray.

Orderable Software Images

Table 1 lists the software versions and applicable ordering information for the Catalyst 6500 series supervisor engine software.



Caution

Always back up the switch configuration file before upgrading or downgrading the switch software to avoid losing all or part of the configuration stored in nonvolatile RAM (NVRAM). **When downgrading switch software, you will lose your configuration.** Use the **write network** command or the **copy config tftp** command to back up your configuration to a Trivial File Transfer Protocol (TFTP) server. Use the **copy config flash** command to back up the configuration to a Flash device.

Table 1 Orderable Software Images

Software Version	Filename	Orderable Product Number ¹
Supervisor Engine 32		
8.4(2a) Flash image	cat6000-sup32pfc3k8.8-4-2a.bin	SC6K-S323K8-8.4
8.4(2a) Flash image (Secure Shell)	cat6000-sup32pfc3k9.8-4-2a.bin	SC6K-S323K9-8.4
8.4(2a) Flash image (CiscoView) ³	cat6000-sup32pfc3cvk8.8-4-2a.bin	SC6K-S323CVK8-8.4
8.4(2a) Flash image (Secure Shell and CiscoView) ³	cat6000-sup32pfc3cvk9.8-4-2a.bin	SC6K-S323CVK9-8.4
8.4(1) Flash image	cat6000-sup32pfc3k8.8-4-1.bin	SC6K-S323K8-8.4
8.4(1) Flash image (Secure Shell)	cat6000-sup32pfc3k9.8-4-1.bin	SC6K-S323K9-8.4
8.4(1) Flash image (CiscoView) ³	cat6000-sup32pfc3cvk8.8-4-1.bin	SC6K-S323CVK8-8.4
8.4(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup32pfc3cvk9.8-4-1.bin	SC6K-S323CVK9-8.4
Supervisor Engine 720		
8.4(2a) Flash image	cat6000-sup720k8.8-4-2a.bin	SC6K-S7K8-8.4
8.4(2a) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-4-2a.bin	SC6K-S7CVK8-8.4
8.4(2a) Flash image (Secure Shell)	cat6000-sup720k9.8-4-2a.bin	SC6K-S7K9-8.4

Table 1 *Orderable Software Images (continued)*

Software Version	Filename	Orderable Product Number ¹
8.4(2a) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-4-2a.bin	SC6K-S7CVK9-8.4
8.4(1) Flash image	cat6000-sup720k8.8-4-1.bin	SC6K-S7K8-8.4
8.4(1) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-4-1.bin	SC6K-S7CVK8-8.4
8.4(1) Flash image (Secure Shell)	cat6000-sup720k9.8-4-1.bin	SC6K-S7K9-8.4
8.4(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-4-1.bin	SC6K-S7CVK9-8.4
8.3(7) Flash image	cat6000-sup720k8.8-3-7.bin	SC6K-S7K8-8.3
8.3(7) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-7.bin	SC6K-S7CVK8-8.3
8.3(7) Flash image (Secure Shell)	cat6000-sup720k9.8-3-7.bin	SC6K-S7K9-8.3
8.3(7) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-7.bin	SC6K-S7CVK9-8.3
8.3(6) Flash image	cat6000-sup720k8.8-3-6.bin	SC6K-S7K8-8.3
8.3(6) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-6.bin	SC6K-S7CVK8-8.3
8.3(6) Flash image (Secure Shell)	cat6000-sup720k9.8-3-6.bin	SC6K-S7K9-8.3
8.3(6) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-6.bin	SC6K-S7CVK9-8.3
8.3(5) Flash image	cat6000-sup720k8.8-3-5.bin	SC6K-S7K8-8.3
8.3(5) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-5.bin	SC6K-S7CVK8-8.3
8.3(5) Flash image (Secure Shell)	cat6000-sup720k9.8-3-5.bin	SC6K-S7K9-8.3
8.3(5) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-5.bin	SC6K-S7CVK9-8.3
8.3(4) Flash image	cat6000-sup720k8.8-3-4.bin	SC6K-S7K8-8.3
8.3(4) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-4.bin	SC6K-S7CVK8-8.3
8.3(4) Flash image (Secure Shell)	cat6000-sup720k9.8-3-4.bin	SC6K-S7K9-8.3
8.3(4) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-4.bin	SC6K-S7CVK9-8.3
8.3(3) Flash image	cat6000-sup720k8.8-3-3.bin	SC6K-S7K8-8.3
8.3(3) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-3.bin	SC6K-S7CVK8-8.3
8.3(3) Flash image (Secure Shell)	cat6000-sup720k9.8-3-3.bin	SC6K-S7K9-8.3
8.3(3) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-3.bin	SC6K-S7CVK9-8.3
8.3(2) Flash image	cat6000-sup720k8.8-3-2.bin	SC6K-S7K8-8.3
8.3(2) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-3-2.bin	SC6K-S7CVK8-8.3
8.3(2) Flash image (Secure Shell)	cat6000-sup720k9.8-3-2.bin	SC6K-S7K9-8.3
8.3(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-3-2.bin	SC6K-S7CVK9-8.3
8.3(1) Flash image ²	cat6000-sup720k8.8-3-1.bin	SC6K-S7K8-8.3
8.3(1) Flash image (Secure Shell)	cat6000-sup720k9.8-3-1.bin	SC6K-S7K9-8.3
8.2(2) Flash image	cat6000-sup720k8.8-2-2.bin	SC6K-S7K8-8.2
8.2(2) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-2-2.bin	SC6K-S7CVK8-8.2
8.2(2) Flash image (Secure Shell)	cat6000-sup720k9.8-2-2.bin	SC6K-S7K9-8.2
8.2(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-2-2.bin	SC6K-S7CVK9-8.2
8.2(1) Flash image	cat6000-sup720k8.8-2-1.bin	SC6K-S7K8-8.2

Table 1 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number ¹
8.2(1) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-2-1.bin	SC6K-S7CVK8-8.2
8.2(1) Flash image (Secure Shell)	cat6000-sup720k9.8-2-1.bin	SC6K-S7K9-8.2
8.2(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-2-1.bin	SC6K-S7CVK9-8.2
8.1(3) Flash image	cat6000-sup720k8.8-1-3.bin	SC6K-S7K8-8.1
8.1(3) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-1-3.bin	SC6K-S7CVK8-8.1
8.1(3) Flash image (Secure Shell)	cat6000-sup720k9.8-1-3.bin	SC6K-S7K9-8.1
8.1(3) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-1-3.bin	SC6K-S7CVK9-8.1
8.1(2) Flash image	cat6000-sup720k8.8-1-2.bin	SC6K-S7K8-8.1
8.1(2) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-1-2.bin	SC6K-S7CVK8-8.1
8.1(2) Flash image (Secure Shell)	cat6000-sup720k9.8-1-2.bin	SC6K-S7K9-8.1
8.1(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-1-2.bin	SC6K-S7CVK9-8.1
8.1(1) Flash image	cat6000-sup720k8.8-1-1.bin	SC6K-S7K8-8.1.1
8.1(1) Flash image (CiscoView) ³	cat6000-sup720cvk8.8-1-1.bin	SC6K-S7CVK8-8.1.1
8.1(1) Flash image (Secure Shell)	cat6000-sup720k9.8-1-1.bin	SC6K-S7K9-8.1.1
8.1(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup720cvk9.8-1-1.bin	SC6K-S7CVK9-8.1.1
Supervisor Engine 2		
8.4(2a) Flash image	cat6000-sup2k8.8-4-2a.bin	SC6K-SUP2K8-8.4
8.4(2a) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-4-2a.bin	SC6K-S2CVK8-8.4
8.4(2a) Flash image (Secure Shell)	cat6000-sup2k9.8-4-2a.bin	SC6K-SUP2K9-8.4
8.4(2a) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-4-2a.bin	SC6K-S2CVK9-8.4
8.4(1) Flash image	cat6000-sup2k8.8-4-1.bin	SC6K-SUP2K8-8.4
8.4(1) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-4-1.bin	SC6K-S2CVK8-8.4
8.4(1) Flash image (Secure Shell)	cat6000-sup2k9.8-4-1.bin	SC6K-SUP2K9-8.4
8.4(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-4-1.bin	SC6K-S2CVK9-8.4
8.3(7) Flash image	cat6000-sup2k8.8-3-7.bin	SC6K-SUP2K8-8.3
8.3(7) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-7.bin	SC6K-S2CVK8-8.3
8.3(7) Flash image (Secure Shell)	cat6000-sup2k9.8-3-7.bin	SC6K-SUP2K9-8.3
8.3(7) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-7.bin	SC6K-S2CVK9-8.3
8.3(6) Flash image	cat6000-sup2k8.8-3-6.bin	SC6K-SUP2K8-8.3
8.3(6) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-6.bin	SC6K-S2CVK8-8.3
8.3(6) Flash image (Secure Shell)	cat6000-sup2k9.8-3-6.bin	SC6K-SUP2K9-8.3
8.3(6) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-6.bin	SC6K-S2CVK9-8.3
8.3(5) Flash image	cat6000-sup2k8.8-3-5.bin	SC6K-SUP2K8-8.3
8.3(5) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-5.bin	SC6K-S2CVK8-8.3
8.3(5) Flash image (Secure Shell)	cat6000-sup2k9.8-3-5.bin	SC6K-SUP2K9-8.3
8.3(5) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-5.bin	SC6K-S2CVK9-8.3

Table 1 *Orderable Software Images (continued)*

Software Version	Filename	Orderable Product Number ¹
8.3(4) Flash image	cat6000-sup2k8.8-3-4.bin	SC6K-SUP2K8-8.3
8.3(4) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-4.bin	SC6K-S2CVK8-8.3
8.3(4) Flash image (Secure Shell)	cat6000-sup2k9.8-3-4.bin	SC6K-SUP2K9-8.3
8.3(4) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-4.bin	SC6K-S2CVK9-8.3
8.3(3) Flash image	cat6000-sup2k8.8-3-3.bin	SC6K-SUP2K8-8.3
8.3(3) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-3.bin	SC6K-S2CVK8-8.3
8.3(3) Flash image (Secure Shell)	cat6000-sup2k9.8-3-3.bin	SC6K-SUP2K9-8.3
8.3(3) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-3.bin	SC6K-S2CVK9-8.3
8.3(2) Flash image	cat6000-sup2k8.8-3-2.bin	SC6K-SUP2K8-8.3
8.3(2) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-3-2.bin	SC6K-S2CVK8-8.3
8.3(2) Flash image (Secure Shell)	cat6000-sup2k9.8-3-2.bin	SC6K-SUP2K9-8.3
8.3(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-3-2.bin	SC6K-S2CVK9-8.3
8.3(1) Flash image ²	cat6000-sup2k8.8-3-1.bin	SC6K-SUP2K8-8.3
8.3(1) Flash image (Secure Shell)	cat6000-sup2k9.8-3-1.bin	SC6K-SUP2K9-8.3
8.2(2) Flash image	cat6000-sup2k8.8-2-2.bin	SC6K-SUP2K8-8.2
8.2(2) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-2-2.bin	SC6K-S2CVK8-8.2
8.2(2) Flash image (Secure Shell)	cat6000-sup2k9.8-2-2.bin	SC6K-SUP2K9-8.2
8.2(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-2-2.bin	SC6K-S2CVK9-8.2
8.2(1) Flash image	cat6000-sup2k8.8-2-1.bin	SC6K-SUP2K8-8.2
8.2(1) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-2-1.bin	SC6K-S2CVK8-8.2
8.2(1) Flash image (Secure Shell)	cat6000-sup2k9.8-2-1.bin	SC6K-SUP2K9-8.2
8.2(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-2-1.bin	SC6K-S2CVK9-8.2
8.1(3) Flash image	cat6000-sup2k8.8-1-3.bin	SC6K-SUP2K8-8.1
8.1(3) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-1-3.bin	SC6K-S2CVK8-8.1
8.1(3) Flash image (Secure Shell)	cat6000-sup2k9.8-1-3.bin	SC6K-SUP2K9-8.1
8.1(3) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-1-3.bin	SC6K-S2CVK9-8.1
8.1(2) Flash image	cat6000-sup2k8.8-1-2.bin	SC6K-SUP2K8-8.1
8.1(2) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-1-2.bin	SC6K-S2CVK8-8.1
8.1(2) Flash image (Secure Shell)	cat6000-sup2k9.8-1-2.bin	SC6K-SUP2K9-8.1
8.1(2) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-1-2.bin	SC6K-S2CVK9-8.1
8.1(1) Flash image	cat6000-sup2k8.8-1-1.bin	SC6K-SUP2K8-8.1.1
8.1(1) Flash image (CiscoView) ³	cat6000-sup2cvk8.8-1-1.bin	SC6K-S2CVK8-8.1.1
8.1(1) Flash image (Secure Shell)	cat6000-sup2k9.8-1-1.bin	SC6K-SUP2K9-8.1.1
8.1(1) Flash image (Secure Shell and CiscoView) ³	cat6000-sup2cvk9.8-1-1.bin	SC6K-S2CVK9-8.1.1
Supervisor Engine 1		
8.4(2a) Flash image	cat6000-supk8.8-4-2a.bin	SC6K-SUPK8-8.4

Table 1 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number ¹
8.4(2a) Flash image (CiscoView) ³	cat6000-supcvk8.8-4-2a.bin	SC6K-SCVK8-8.4
8.4(2a) Flash image (Secure Shell)	cat6000-supk9.8-4-2a.bin	SC6K-SUPK9-8.4
8.4(2a) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-4-2a.bin	SC6K-SCVK9-8.4
8.4(1) Flash image	cat6000-supk8.8-4-1.bin	SC6K-SUPK8-8.4
8.4(1) Flash image (CiscoView) ³	cat6000-supcvk8.8-4-1.bin	SC6K-SCVK8-8.4
8.4(1) Flash image (Secure Shell)	cat6000-supk9.8-4-1.bin	SC6K-SUPK9-8.4
8.4(1) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-4-1.bin	SC6K-SCVK9-8.4
8.3(7) Flash image	cat6000-supk8.8-3-7.bin	SC6K-SUPK8-8.3
8.3(7) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-7.bin	SC6K-SCVK8-8.3
8.3(7) Flash image (Secure Shell)	cat6000-supk9.8-3-7.bin	SC6K-SUPK9-8.3
8.3(7) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-7.bin	SC6K-SCVK9-8.3
8.3(6) Flash image	cat6000-supk8.8-3-6.bin	SC6K-SUPK8-8.3
8.3(6) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-6.bin	SC6K-SCVK8-8.3
8.3(6) Flash image (Secure Shell)	cat6000-supk9.8-3-6.bin	SC6K-SUPK9-8.3
8.3(6) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-6.bin	SC6K-SCVK9-8.3
8.3(5) Flash image	cat6000-supk8.8-3-5.bin	SC6K-SUPK8-8.3
8.3(5) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-5.bin	SC6K-SCVK8-8.3
8.3(5) Flash image (Secure Shell)	cat6000-supk9.8-3-5.bin	SC6K-SUPK9-8.3
8.3(5) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-5.bin	SC6K-SCVK9-8.3
8.3(4) Flash image	cat6000-supk8.8-3-4.bin	SC6K-SUPK8-8.3
8.3(4) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-4.bin	SC6K-SCVK8-8.3
8.3(4) Flash image (Secure Shell)	cat6000-supk9.8-3-4.bin	SC6K-SUPK9-8.3
8.3(4) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-4.bin	SC6K-SCVK9-8.3
8.3(3) Flash image	cat6000-supk8.8-3-3.bin	SC6K-SUPK8-8.3
8.3(3) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-3.bin	SC6K-SCVK8-8.3
8.3(3) Flash image (Secure Shell)	cat6000-supk9.8-3-3.bin	SC6K-SUPK9-8.3
8.3(3) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-3.bin	SC6K-SCVK9-8.3
8.3(2) Flash image	cat6000-supk8.8-3-2.bin	SC6K-SUPK8-8.3
8.3(2) Flash image (CiscoView) ³	cat6000-supcvk8.8-3-2.bin	SC6K-SCVK8-8.3
8.3(2) Flash image (Secure Shell)	cat6000-supk9.8-3-2.bin	SC6K-SUPK9-8.3
8.3(2) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-3-2.bin	SC6K-SCVK9-8.3
8.3(1) Flash image ²	cat6000-supk8.8-3-1.bin	SC6K-SUPK8-8.3
8.3(1) Flash image (Secure Shell)	cat6000-supk9.8-3-1.bin	SC6K-SUPK9-8.3
8.2(2) Flash image	cat6000-supk8.8-2-2.bin	SC6K-SUPK8-8.2
8.2(2) Flash image (CiscoView) ³	cat6000-supcvk8.8-2-2.bin	SC6K-SCVK8-8.2
8.2(2) Flash image (Secure Shell)	cat6000-supk9.8-2-2.bin	SC6K-SUPK9-8.2

Table 1 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number ¹
8.2(2) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-2-2.bin	SC6K-SCVK9-8.2
8.2(1) Flash image	cat6000-supk8.8-2-1.bin	SC6K-SUPK8-8.2
8.2(1) Flash image (CiscoView) ³	cat6000-supcvk8.8-2-1.bin	SC6K-SCVK8-8.2
8.2(1) Flash image (Secure Shell)	cat6000-supk9.8-2-1.bin	SC6K-SUPK9-8.2
8.2(1) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-2-1.bin	SC6K-SCVK9-8.2
8.1(3) Flash image	cat6000-supk8.8-1-3.bin	SC6K-SUPK8-8.1
8.1(3) Flash image (CiscoView) ³	cat6000-supcvk8.8-1-3.bin	SC6K-SCVK8-8.1
8.1(3) Flash image (Secure Shell)	cat6000-supk9.8-1-3.bin	SC6K-SUPK9-8.1
8.1(3) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-1-3.bin	SC6K-SCVK9-8.1
8.1(2) Flash image	cat6000-supk8.8-1-2.bin	SC6K-SUPK8-8.1
8.1(2) Flash image (CiscoView) ³	cat6000-supcvk8.8-1-2.bin	SC6K-SCVK8-8.1
8.1(2) Flash image (Secure Shell)	cat6000-supk9.8-1-2.bin	SC6K-SUPK9-8.1
8.1(2) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-1-2.bin	SC6K-SCVK9-8.1
8.1(1) Flash image	cat6000-supk8.8-1-1.bin	SC6K-SUPK8-8.1.1
8.1(1) Flash image (CiscoView) ³	cat6000-supcvk8.8-1-1.bin	SC6K-SCVK8-8.1.1
8.1(1) Flash image (Secure Shell)	cat6000-supk9.8-1-1.bin	SC6K-SUPK9-8.1.1
8.1(1) Flash image (Secure Shell and CiscoView) ³	cat6000-supcvk9.8-1-1.bin	SC6K-SCVK9-8.1.1

1. Installed on system; append with “=” for spare on floppy media.

2. There are no CiscoView images in software release 8.3(1). CiscoView images are scheduled for software release 8.3(2).

3. CiscoView images are available approximately 2 weeks after the Flash images are released.

Software Image Version Compatibility

With high-availability versioning enabled, you can have two different but compatible images on the active and standby supervisor engines. The active supervisor engine exchanges image version information with the standby supervisor engine and determines whether the images are compatible for enabling high availability. If the active and standby supervisor engines are not running compatible image versions, you cannot enable high availability.

Image versioning is supported in supervisor engine software releases 5.4(1) and later. With versioning enabled, high availability is fully supported with the active and standby supervisor engines running different images as long as the images are compatible. The only fully compatible images are as follows:



Note

There is no software image version compatibility in the 8.x software release train. This includes major releases such as 8.1(x) to 8.2(x) to 8.3(x) and so on. This also includes subreleases such as 8.1(1) to 8.1(2), 8.2(1) to 8.2(2) and so on.

- Supervisor Engine 1
 - 5.5(3) and 5.5(4)
 - 6.1(3) and 6.1(4)
 - 6.2(2) and 6.2(3)

- 6.3(2) and 6.3(3)
- 6.3(4) and 6.3(5)
- 6.3(6) and 6.3(7)
- Supervisor Engine 2
 - 6.1(3) and 6.1(4)
 - 6.2(2) and 6.2(3)
 - 6.3(2) and 6.3(3)

Images that are compatible with all modules except Gigabit Ethernet switching modules are as follows:

- Supervisor Engine 1
 - 5.4(3) and 5.4(4)
 - 5.5(3) and 5.5(5)
 - 5.5(4) and 5.5(5)

Images that are compatible with Gigabit Ethernet switching modules but not compatible with 10/100BASE-T modules are as follows:

- Supervisor Engine 1
 - 5.5(6a) and 5.5(7)

Images that are compatible with all modules except the SFM/SFM2 and fabric-enabled modules are as follows:

- Supervisor Engine 2
 - 6.3(4) and 6.3(5)
 - 6.3(6) and 6.3(7)



Note

Attempting to run incompatible image versions could result in configuration loss.

Catalyst 6500 Series Features



Note

For complete hardware requirements for the software features listed, see the *Catalyst 6500 Series Software Configuration Guides*.

These sections describe the Catalyst 6500 series features:

- Features for Supervisor Engine Software Release 8.4, page 31
- Features for Supervisor Engine Software Release 8.3, page 35
- Features for Supervisor Engine Software Release 8.2, page 41
- Features for Supervisor Engine Software Release 8.1, page 44
- Features for Supervisor Engine Software Releases 7.1 Through 7.6, page 47
- Features for Supervisor Engine Software Releases 6.1 Through 6.4, page 47
- Features for Supervisor Engine Software Releases 5.1 Through 5.5, page 47

Features for Supervisor Engine Software Release 8.4



Note

Maximum switching performance is achieved when all switch components are fabric enabled. The presence of nonfabric-enabled switching modules might impact overall switching performance.

These sections describe the features in software release 8.4, 29 December 2004:

- Software Release 8.4 Hardware Features, page 31
- Software Release 8.4 Software Features, page 32
- Software Release 8.4 Unsupported Software Features, page 34
- Software Release 8.4 Unsupported Hardware, page 34

Software Release 8.4 Hardware Features

Software release 8.4 provides initial support for these modules and chassis:

- Supervisor Engine 32 (WS-SUP32-GE-3B) with PFC3B and MSFC2A
- 6000 W power supply (WS-CAC-6000W)

Supported in all Catalyst 65xx and Catalyst 65xx-E chassis except for the 6503 and 6503-E (form-factor difference). Only the 6513 and -E chassis support the full 6000 W; the other chassis rely on software to current limit the power supply.

- 2700 W power supply (PWR-2700-AC, PWR-2700-DC)

Supported in the Cisco 7606 chassis. Cannot be used in the 65xx chassis.

- Catalyst 6500 E-series chassis enhancements

Enhanced power capacity allowing higher-powered modules to be installed (including PoE support for 30 W per-port devices). Additionally, support for the 67xx switching modules in the 6503-E chassis is provided with software release 8.4(1) and later releases.

- WS-X6148A-GE-TX, WS-X6148A-GE-45AF

48-port 10/100/1000BASE-T, RJ-45 connectors. WS-X6148A-GE-45AF provides inline power for IP telephones with the WS-F6K-GE48-AF daughter card.

- WS-X6148-FE-SFP

48-port 100FX Ethernet, requires SFPs. The following SFPs are introduced with the WS-X6148-FE-SFP module:

- GLC-FE-100FX (100BASE-FX SFP)
- GLC-FE-100LX (100BASE-LX SFP)
- GLC-FE-100BX-U, GLC-FE-100BX-D (100BASE-BX SFP)

- WS-X6148A-RJ-45, WS-X6148A-45AF

48-port 10/100BASE-TX, RJ-45 connectors. WS-X6148A-45AF provides inline power for IP telephones with the WS-F6K-GE48-AF daughter card.

- WS-X6196-RJ-21, WS-X6196-21AF

96-port 10/100BASE-TX, RJ-21 connectors. WS-X6196-21AF provides inline power for IP telephones with the WS-F6K-FE48X2-AF daughter card.

- 1000BASE-BX SFP (GLC-BX-1310, GLC-BX-1490)

- 4-slot 6504-E chassis (WS-C6504-E) (Supported in software release 8.4(2) and later releases.)

Software Release 8.4 Software Features

Software release 8.4 provides support for these software features:

- EtherChannel enhancements:

Provides for an automatic failover of traffic from one port in an EtherChannel to another port in the same EtherChannel when one of the ports in the channel exceeds a configurable error threshold within the specified interval. The port failover only occurs if there is an operational port left in the EtherChannel. If the failed port is the last port in the EtherChannel, the port does not enter the “port failover” state and continues to pass traffic regardless of the type of errors being received. Single, nonchanneling ports do not go into the port failover state; these ports go into the errdisable state when the error threshold is exceeded within the specified interval.
- VLAN translation:

VLAN mapping has been enhanced to allow you to map *any* type of VLAN to any other type of VLAN without any VLAN range restrictions. VLAN mapping is now configurable on a per-port or per-ASIC basis.
- MAC-based ACLs:

PFC3B and PFC3BXL allow the ACL lookups on *all* packet types using the MAC ACL. This feature is useful for doing MAC-based matching on all packets regardless of whether the packet is IP version 4, IP version 6, IPX, MPLS, and so on. You can utilize this feature to rate limit all traffic ingressing a VLAN to some specific value by coupling an aggregate policer with a match-all MAC ACL.
- SmartPorts enhancements:
 - Ciscorouter SmartPorts template
 - Ciscoswitch SmartPorts template
 - Ciscodesktop SmartPorts template
 - Ciscoipphone SmartPorts template
 - Ciscosoftphone SmartPorts template
 - Global SmartPorts template
- System profiles (lockdown profiles):

With the profile files, you can eliminate the features or processes that may pose security risks (for example, disabling CDP or turning off auto-trunking on a port) to your switch. A profile file that has most of the security risks disabled is also known as a “lockdown” profile. A lockdown profile changes the functionality of the switch from enabling access to preventing access by default. When a lockdown profile is applied, you must manually enable the features that were disabled by the profile file.
- CRAM algorithm:

The compression and reordering of the ACL masks (CRAM) feature optimizes the mask usage across the different ACLs. This optimization promotes mask sharing and results in more efficient usage of the TCAM and the ability to program more ACLs in the TCAM.
- ACL statistics:

When you select the **statistics** keyword with the **set security acl** command set, the statistics are stored for the ACEs or the ACLs (VACLs and PACLs). The ACL statistics are disabled by default and can be enabled on a per-ACL, per-VLAN, or per-ACE basis.

- NetFlow top talkers:

The **show mls statistics entry ip top-talkers** command can display the statistics for the netflows with the maximum amount of network usage. The NetFlow entries are pulled out of the NetFlow table based on the number of packets that each flow has. The results are displayed in descending order with the top talkers being the entries with the largest packet count. You can get the statistics for the network (the top 32 talkers will be displayed) or for a specified number of flows such as the top 1 or 2 talkers.

- NetFlow export with autonomous system information:

Provides for exporting the autonomous system numbers for peer or source destinations with the correct (nonzero) values in the NDE records. You can enable this feature to allow the NDE records to carry the correct autonomous system values or disable this feature to have the NDE records carry a value of zero. You may export either the peer autonomous system number or the origination autonomous system number.

- Configuration rollback:

Provides for rolling back the current switch configuration file to a previously saved configuration file if the current file produces undesirable system results. This rollback feature provides a command to set multiple configuration “checkpoint” files. If you no longer want the current configuration file to run on the switch, you can return to one of these configuration checkpoint files quickly and with the least possible disturbance to switch functionality.

- SPAN—Multiple destination ports can be specified in each local SPAN session.

- NetFlow—Create NetFlow table entries on a per-VLAN basis.

- Time domain reflectometer (TDR) support added for the following modules: WS-X6748-GE-TX, WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6148A-RJ-45, and WS-X6148A-45AF.

- Layer 2 protocol tunneling enhancements:

Provides for specifying the drop and shutdown thresholds for individual protocols on a per-port basis. If you configure thresholds only and do not specify a protocol, the packets are rate limited cumulatively irrespective of protocols. If you specify a threshold for a protocol on a port, the packets are rate limited on a cumulative basis and then per-protocol thresholds are applied to the packets.

- 802.1X authentication failure VLAN:

On a traditional 802.1X port, the switch does not provide access to the network until the supplicant that is connected to the port is authenticated by verifying its identity information with an authentication server. With the authentication failure VLAN feature, you can configure the authentication failure VLAN on a per-port basis and after three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network.

- 802.1X RADIUS server failover enhancements:

Before software release 8.4(1), when the active RADIUS server went down or was unreachable, the 802.1X authentication timed out before the backup RADIUS server could become active. With software release 8.4(1) and later releases, some RADIUS server timer values are now configurable and the **show radius** command has been enhanced to show the active RADIUS server.

- Shaped round robin (SRR):

Provides egress traffic shaping and is supported as an option on Supervisor Engine 32 **1p3q8t** ports. If you do not enable SRR, weighted round robin (WRR) is used. SRR only allows a queue to use the specific amount of bandwidth that the weight allocates.

- Support for the following MIBs:
 - CISCO-SECURE-SHELL-MIB
 - CISCO-RADIUS-MIB
 - CISCO-COPY-CONFIG-MIB
 - CISCO-VLAN-TRANSLATION-MIB
 - MAU-MIB
 - CISCO-MAU-EXT-MIB
 - POWER-ETHERNET-MIB
 - CISCO-POWER-ETHERNET-EXT-MIB
 - CISCO-NETFLOW-MIB
 - HC-ALARM-MIB
 - CISCO-VMPS-MIB enhancement
 - RMON-MIB enhancement
 - CISCO-STP-EXTENSIONS-MIB enhancement
 - CISCO-CATOS-ACL-QOS-MIB enhancement
 - SMON-MIB/CISCO-RMON-CONFIG-MIB enhancement
 - CISCO-QOS-PIB-MIB enhancement
 - CISCO-SWITCH-ENGINE-MIB enhancement
 - CISCO-L2-TUNNEL-CONFIG-MIB enhancement

Software Release 8.4 Unsupported Software Features

This section lists the unsupported software features in software release 8.4(x):

- The following QoS features and the commands that are used to configure them are not supported in a system with a Supervisor Engine 720 in software release 8.4(x):
 - RSVP
 - COPS
 - NBAR
- The following features are not supported with a Supervisor Engine 720 or Supervisor Engine 32 in software release 8.4(x):
 - TCP Intercept.
 - WCCP.

Software Release 8.4 Unsupported Hardware

This section lists the unsupported hardware in software release 8.4(x):

- The OSMs are not supported with Supervisor Engine 720 in software release 8.4(x). The “Optical Services Modules” section on page 17 lists the OSMs.
- The IPsec Virtual Private Network (VPN) Acceleration Services Module (WS-SVC-IPSEC-1) is not supported in software release 8.4(x).

Features for Supervisor Engine Software Release 8.3



Note

Maximum switching performance is achieved when all switch components are fabric enabled. The presence of nonfabric-enabled switching modules might impact overall switching performance.

These sections describe the features in software release 8.3, 3 May 2004:

- Software Release 8.3 Hardware Features, page 35
- Software Release 8.3 Software Features, page 36
- Software Release 8.3 Unsupported Software Features, page 41
- Software Release 8.3 Unsupported Hardware, page 41

Software Release 8.3 Hardware Features

Software release 8.3 provides initial support for these modules and chassis:



Note

With software release 8.3(1), WS-SUP720-3BXL and WS-SUP720-3B support the same feature set and have the same performance characteristics as WS-F6K-PFC3A.

- WS-SUP720-3BXL—Supervisor Engine 720 with PFC3BXL:
 - 1-GB DRAM
 - Policy Feature Card 3BXL
 - Multilayer Switch Feature Card 3 (MSFC3):
 - 1-GB DRAM
 - 64-MB bootflash
- WS-F6K-PFC3BXL—Policy Feature Card 3BXL:

Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 with a PFC3BXL. WS-F6K-PFC3BXL= includes 1-GB memory upgrades for the Supervisor Engine 720 and the MSFC3. Refer to this publication for more information:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm
- WS-SUP720-3B—Supervisor Engine 720 with PFC3B:
 - 512-MB DRAM
 - Policy Feature Card 3B
 - Multilayer Switch Feature Card 3 (MSFC3):
 - 256-MB DRAM
 - 32-MB bootflash
- WS-F6K-PFC3B—Policy Feature Card 3B:

There are no memory-only upgrade options for WS-SUP720-3B.

Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. Refer to this publication for more information:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_16220.htm

- Dense Wavelength Division Multiplexing (DWDM) GBIC transceivers
- Coarse Wave Division Multiplexer SFP (CWDM-SFP) (1000BASE-CWDM SFP)
- GLC-T (1000BASE-T SFP)
- XENPAKs:
 - XENPAK-10GB-SR—10GBASE-SR Serial 850-nm short-reach multimode (MMF)
 - XENPAK-10GB-CX4—10GBASE-CX4 provides support for copper up to 15 meters
- WS-X6748-SFP module (48-port Gigabit Ethernet SFP)



Note Support for the WS-X6748-SFP module started in software release 8.3(2) and later releases.

Software Release 8.3 Software Features

Software release 8.3 provides support for these software features:

- DHCP snooping:

DHCP snooping provides security against Denial-Of-Service (DoS) attacks that are launched using DHCP messages by filtering DHCP packets and building and maintaining a DHCP-snooping binding table. DHCP snooping uses trusted and untrusted ports to filter the DHCP packets that are received by the switch.
- IP source guard:

IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port.
- Dynamic ARP inspection:

Dynamic ARP inspection (DAI) uses the binding information that is built by DHCP snooping to enforce the advertisement of bindings to prevent “man-in-the-middle” attacks. These attacks can occur when an attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entries in a communication association. DAI adds an extra layer of security to ARP inspection by verifying that the ARP packet's MAC address and IP address match an existing DHCP snooping binding in the same VLAN.
- Port ACLs (PACLs):

Prior to software release 8.3(1), there were two types of access-lists—VACLs and IOS ACLs. The VACLs are applied to Layer 2 and Layer 3 forwarded traffic while the Cisco IOS ACLs are only applied to Layer 3 forwarded packets. Both access list types are applied to VLANs and filter traffic based on the packet header information.

Typically, a VLAN is composed of many physical ports. A PACL provides you with the extra granularity to filter traffic on a specific physical port. A PACL is an access list that is mapped to a physical port. Like VACLs, PACLs are applied to both Layer 2 and Layer 3 forwarded packets.
- Fabric enhancements with Supervisor Engine 720:

The integrated 720-Gbps switch fabric supports a high-availability failover to the standby switch fabric.
- Automatic QoS enhancement:

Allows you to clear the automatic QoS configuration by using a port-based **clear** command and a global **clear** command.

- **Multiple collectors for NDE:**
Allows NetFlow export data to be sent to two destinations simultaneously.
- **PBF enhancements:**
Simplifies the process of setting and committing the security ACLs and adjacency information.
- **EtherChannel enhancements:**
Clears and restores channel-based counters on a per-protocol and per-channel basis.
- **Disables an auxiliary VLAN until an IP phone is detected:**
Provides security for the auxiliary VLANs by ensuring that the auxiliary VLAN is not enabled until an IP phone is detected. As soon the switch detects the presence of an IP phone, the auxiliary VLAN is enabled.
- **802.1X unidirectional controlled port:**
Allows you to use wake-on LAN technology (also referred to as remote wake-up) to perform unattended system backups or software upgrades on hosts attached to the switch.
- **802.1X with ACL assignments:**
When you configure 802.1X with ACL assignments, you can automatically configure the QoS ACLs and VACLs to a user once the user is authenticated. The RADIUS server sends a QoS VLAN-based ACL, QoS port-based ACL, or VACL policy name with the authentication success packet. The policy that is associated with the policy name is already configured on the switch through the CLI. The policy is converted into a set of ACEs and then installed on the switch. Once you configure the 802.1X ACL assignments, the switch does the following:
 - Authenticates the user(s)
 - Uses DHCP snooping or dynamic ARP inspection to obtain the IP address of the user(s)
 - Expands the ACL using the IP address(es) and programs the PFC
- **802.1X user distribution:**
Configuring the 802.1X user distribution feature allows you to distribute users that have the same group name across multiple VLANs. Prior to software release 8.3(1), the RADIUS VLAN assignment feature supported by 802.1X took the VLAN number obtained from the RADIUS server and added all users to that VLAN. With software release 8.3(1) and later releases, you can load balance 802.1X-authenticated users that are configured under one group name by distributing them evenly between VLANs.
- **802.1X RADIUS accounting and tracking:**
Allows you to send 802.1X user accounting information to the RADIUS server.
- **802.1X authenticated identity-to-port description mappings:**
Assigns a port description to the 802.1X port based on the information received from the RADIUS server. This feature makes use of an AV-Pair, “Supplicant Name,” to uniquely assign a port description for an authenticated user.
- **DNS resolution for a RADIUS server configuration:**
Allows you to configure the RADIUS server using a DNS name in addition to IP addresses.
- **VTP version 3 enhancement—MST mapping propagations:**
Provides the ability to distribute the MST database across the network using VTP version 3.
- **802.1s:**

The Multiple Spanning Tree (MST) feature is the IEEE 802.1s and is an amendment to 802.1Q. MST extends the 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides for both rapid convergence and load balancing in a VLAN environment. In software release 8.3(1), the MST protocol is compliant with IEEE 802.1s and is backward compatible with 802.1D STP, 802.1w, the Rapid Spanning Tree Protocol (RSTP), and the Cisco PVST+ architecture that was implemented in previous software releases.

- Layer 2 PDU rate limiting:

The Layer 2 PDU rate limiters are supported in hardware, and they rate limit traffic on the Local Target Logic (LTL) index. You can configure up to four rate limiters. You can configure rate limiters to limit the following PDU types globally on the switch:

- Spanning-tree BPDUs—IEEE and SSTP, CDP, UDLD, VTP, and PAgP
- Layer 2 protocol tunnel-encapsulated PDUs
- 802.1X port security

- Automatic module shutdown:

Automatically shut down any module based on the number of times that the module resets itself within a specified time frame. A module that frequently resets itself can disrupt traffic load balancing. By setting the automatic module shutdown, you can limit the number of times that the module resets itself before shutting down completely.

- System crash-info files:

The crash-info file contains extended system information that is captured very quickly when the system reloads due to an error condition. Like the core-dump file, the crash-info file is stored in the file system. The information in the crash-info file should be used in addition to the core-dump information and does not replace that information. By examining both the crash-info file and core-dump file, Cisco TAC can better analyze the error condition.

- MSFC autostate enhancements:

- Normal autostate mode—Autostate shuts down (or brings up) Layer 3 interfaces/subinterfaces on the MSFC and the Multilayer Switch Module (MSM) when specific port configuration changes occur on the switch.
- Autostate exclude mode—Allows you to specify the ports to exclude from autostate.
- Autostate track mode—Tracks key VLAN or port connections to the MSFC.

- Port security on trunk ports

- MAC address monitoring:

Because the Catalyst 6500 series switches learn the source MAC addresses automatically, the system is vulnerable to flooding of spoofed traffic and potential Denial of Service (DoS) attacks. To prevent traffic flooding and DoS attacks, you can monitor the number of MAC addresses that are learned by the system on a per-port, per-VLAN, or per-port-per-VLAN basis.

- CoS-to-CoS maps on IEEE 802.1Q tunnel ports:

Ingress Cos-to-CoS mapping is supported on 802.1Q tunnel ports on WS-X6704-10GE, WS-X6724-SFP, and WS-X6748-GE-TX switching modules. The CoS-to-CoS mapping feature is disabled on ports that are not configured as 802.1Q tunnel ports.

- Back up the VMPS configuration file:

When you reboot a Catalyst 6500 series switch that is configured as a VMPS server, the VMPS requests that are sent by the clients are queued by the TFTP server until the VMPS server downloads the VMPS configuration file from the VMPS server. To ensure that client access is not delayed

during a system reboot, you can configure the switch to back up the VMPS configuration file locally and use this file until it has downloaded the current VMPS configuration file from the remote TFTP server.

- **SCP:**
Secure Copy (SCP) provides a secure method for copying crypto image files. SCP relies on Secure Shell (SSH) and allows you to copy a crypto file to and from the system through an encrypted channel.
- **Comparing configuration files:**
You can compare the configuration files that are stored on the system to determine the differences between the configuration files or to check if changes have been made to the system configuration.
- **Using Secure Shell Encryption for Telnet sessions (support for SSH version 2)**
Secure Shell encryption provides security for Telnet sessions and other remote connections to the switch. Secure Shell encryption is supported for remote logins to the switch only. Telnet sessions that are initiated from the switch cannot be encrypted. To use this feature, you must install the application on the client accessing the switch, and you must configure Secure Shell encryption on the switch. The current implementation of Secure Shell encryption supports SSH version 1 and version 2. SSH version 1 supports the DES and 3DES encryption methods, and SSH version 2 supports the 3DES and AES encryption methods. Secure shell encryption can be used with RADIUS and TACACS+ authentication.
- **GLBP:**
Gateway Load Balancing Protocol (GLBP) provides load-balancing over multiple gateways through a single virtual IP address and multiple virtual MAC addresses. This protocol is similar to Host Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP). GLBP protects data traffic from a failed router or circuit, while allowing packet load sharing between a group of redundant routers.
- **IGMP version 3 snooping with Multicast Multilayer Switching (MMLS):**
Prior to software release 8.3(1), IGMP version 3 snooping operated only with MMLS disabled on the supervisor engine. This resulted in the IGMP version 3 snooping capability being available on individual bridged VLANs but there was no IGMP version 3 snooping support for hardware-switched Layer 3 flows. Software release 8.3(1) and later releases provides IGMP version 3 snooping with MMLS integration.
- **CLI command logging:**
Entering the **show log command** displays recorded commands executed from the CLI through Telnet, SSH, or console sessions. The log provides a history of the events and operations performed by users.
- **Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) support on Supervisor Engine 720**
- **Verify software images:**
Because a software image goes through a sequence of transfers before it is copied into the memory of the switch, the integrity of the image is at risk each time that it is downloaded from Cisco.com. The image size and checksum are automatically checked when the image is copied, but these types of checks do not ensure that the downloaded image has not been corrupted. To ensure the integrity of any images that you download, you can use the **set image-verification** command. You can set image verification to work when booting, after the image has been copied, or before a system reset.
- **Bidirectional PIM:**

Supervisor Engine 720 supports hardware forwarding of bidirectional PIM groups. To support bidirectional PIM groups, the Supervisor Engine 720 implements a new mode called designated forwarder (DF) mode. The designated forwarder is the router that is elected to forward packets to and from a segment for a bidirectional PIM group. In DF mode, the supervisor engine accepts packets from the reverse path forwarding (RPF) interface and from the DF interface.

- VLAN manager enhancements:

Instead of reserved VLANs, we now have only user and internal VLANs. VLAN manager no longer permanently sets aside VLANs for features that require them; they are now dynamically assigned as needed. The entire VLAN range (1 to 4094) is now available for user (and internal) VLANs.

- QoS policer burst value change:

The burst value changed from 1–32000 (1 Kb to 32 Kb) to 1–256000 (1 Kb to 256 Mb)

- PFC3 output QoS ACLs trust change:

Egress traffic uses the same trust values as ingress traffic when attaching ACLs to a VLAN. Any traffic trusted at ingress will also be trusted at egress.

- Unique device identifier:

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a Cisco Unique Device Identifier (UDI). The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN). The PID is the name by which the product can be ordered and is also called the “Product Name” or “Part Number.” You can use this identifier to order an exact replacement part. The VID is the version of the product. Whenever a product has been revised, the VID is incremented. The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory; this number identifies a specific instance of a product.

- System sanity check:

The **show system sanity** command runs a series of checks on the configuration and highlights possible conditions that could lead to problems with your configuration.

- System health check:

The **show system health** command tracks registers, counters, and software patch “kick-ins” and compiles a list of entities it considers as “unhealthy” for the system. The feature also lists CPU and memory utilization.

- Expanded memory support:

Software release 8.3(1) and later releases support up to 1-GB DRAM on the Supervisor Engine 720.

- SmartPort macros:

SmartPort macros provide a convenient way to save and share common configurations. You can use SmartPort macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

- Virtual Router Redundancy Protocol (VRRP)

VRRP eliminates the single point of failure inherent in the static default routed environment.

Software Release 8.3 Unsupported Software Features

This section lists the unsupported software features in software release 8.3(x):

- The following QoS features and the commands that are used to configure them are not supported in a system with a Supervisor Engine 720 in software release 8.3(x):
 - RSVP
 - COPS
 - NBAR
- The following features are not supported with a Supervisor Engine 720 in software release 8.3(x):
 - TCP Intercept.
 - WCCP.

Software Release 8.3 Unsupported Hardware

This section lists the unsupported hardware in software release 8.3(x):

- The OSMs are not supported with Supervisor Engine 720 in software release 8.3(x). The “Optical Services Modules” section on page 17 lists the OSMs.
- The IPSec Virtual Private Network (VPN) Acceleration Services Module (WS-SVC-IPSEC-1) is not supported in software release 8.3(x).

Features for Supervisor Engine Software Release 8.2



Note

Maximum switching performance is achieved when all switch components are fabric enabled. The presence of nonfabric-enabled switching modules might impact overall switching performance.

These sections describe the features in software release 8.2, 4 December 2003:

- Software Release 8.2 Hardware Features, page 41
- Software Release 8.2 Software Features, page 42
- Software Release 8.2 Unsupported Software Features, page 44
- Software Release 8.2 Unsupported Hardware, page 44

Software Release 8.2 Hardware Features

Software release 8.2 provides initial support for these modules and chassis:

- The 96-port 10/100BASE-TX switching module (WS-X6148X2-RJ-45) is supported. WS-X6148X2-45AF has the voice daughter card (WS-F6K-FE48X2-AF).

Voice daughter card features include the following:

- Inline power for Cisco IP phones, Cisco Aironet wireless access points, and IEEE 802.3af-compliant devices
- Power to any of the 96 ports
- Up to 15.4 W per port (limited to a total of 740 W per daughter card)

- 48 ports may be powered at 15.4 W each
- 96 ports may be powered at 7 W each
- Two additional voice daughter cards are supported:
 - WS-F6K-FE48-AF for the WS-X6148-RJ-45 and WS-X6148-RJ21 48-port 10/100BASE-TX switching modules
 - WS-F6K-GE48-AF for the WS-X6148-GE-TX and WS-X6548-GE-TX 48-port 10/100/1000BASE-TX switching modules

These voice daughter card features are supported:

- Inline power for Cisco IP phones, Cisco Aironet wireless access points, and IEEE 802.3af-compliant devices.
- Power to all 48 ports (up to 15.4 W per port)



Note To determine your exact power needs, use the CCO power calculator at this URL:

<http://www.cisco.com/go/powercalculator>

- The 1000BASE-ZX SFP (GLC-ZX-SM), single mode only, dual LC connector is supported.
- XENPAK-10GB-LX4—10GBASE-LX4 Serial 1310-nm multimode (MMF)
- The Catalyst 6500 series switch service modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases. The “Service Modules” section on page 18 lists the service modules.
- The Catalyst 6500 series switch voice modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases. The “Voice Modules” section on page 16 lists the voice modules.
- The ATM modules are supported with Supervisor Engine 720 in software release 8.2(1) and later releases. The “ATM Modules” section on page 19 lists the ATM modules.
- The FlexWAN module is supported with Supervisor Engine 720 in software release 8.2(1) and later releases. The “FlexWAN Module” section on page 17 lists the FlexWAN module.

Software Release 8.2 Software Features

Software release 8.2 provides support for these software features:

- Specifying a custom 802.1Q EtherType field

By specifying a custom EtherType field, your network can support Cisco and non-Cisco switches that do not use the standard 0x8100 EtherType to identify 802.1Q-tagged frames.
- Supervisor Engine 720 supports these QoS-related features:
 - Egress QoS
 - Egress DSCP mutation
 - Optional egress DSCP rewrite
 - Disable DSCP rewrite
 - QDE
 - Automatic QoS

- IEEE 802.3af power compliance
- Cisco IP Phone support enhancements:
 - Support for a high-powered phone to negotiate a low-power mode (dimmed screen) when powered by a pre-standard Cisco PoE daughter card.
 - Support for a high-powered phone to negotiate a high-power mode (full screen brightness) when powered by a IEEE 802.3af Cisco PoE daughter card.
- Support for new SFPs and XENPAKs:

For information on SFP and XENPAK support, see the “SFP, XENPAK, and GBIC Behavior” section on page 56.
- New **auto-10-100** keyword for the **set port speed** command:

Use the **auto-10-100** keyword on ports that support speeds of 10/100/1000 Mbps. Using the **auto-10-100** keyword makes the port behave the same as a 10/100-Mbps port that has the speed set to **auto**. The speed and duplex are negotiated (the 1000-Mbps speed does not take part in the negotiation).
- New **auto-configure** keyword for the **set port security** command:

Automatically configured addresses are not aged out and are retained across reboots. These addresses are retained if a secure port shuts down because of a security violation, if the port is administratively disabled, or if port security is disabled.
- Auto-MDI/MDIX capability:

You can use either straight or crossover cable, and the module will automatically detect and adjust for the cable type. For complete details, see the “Auto-MDI/MDIX” section on page 67.
- In software release 8.2.2, improved supervisor engine failover rates with high-availability enabled are as follows:
 - In flow-through, truncated and compact modes, the Supervisor Engine 1 and Supervisor Engine 2 failover time is less than 500 ms.
 - In flow-through mode, the Supervisor Engine 720 failover time is about 1.5 seconds. In truncated or compact mode, the Supervisor Engine 720 failover time is less than 3 seconds.
- In software release 8.2.1, the supervisor engine failover rates with high-availability enabled are as follows:
 - In flow-through mode, the Supervisor Engine 1 and Supervisor Engine 2 failover time is less than 500 ms. With Supervisor Engine 720, the failover time is approximately 1.5 seconds.
 - In truncated or compact mode, the Supervisor Engine 2 failover time is about 1.5 seconds. With Supervisor Engine 720, the failover time is approximately 3.5 seconds.
- The maximum number of permanent CAM entries has been increased from 128 to 256.
- Support for the following MIBs:
 - CISCO-VLAN-MEMBERSHIP-MIB enhancement
 - CISCO-CATOS-ACL-QOS-MIB enhancement

Software Release 8.2 Unsupported Software Features

This section lists the unsupported software features in software release 8.2(x):

- The following QoS features and the commands that are used to configure them are not supported in a system with a Supervisor Engine 720 in software release 8.2(x):
 - RSVP
 - COPS
 - NBAR
- The following automatic QoS **clear** commands are visible in the CLI but are not supported in software release 8.2(x):
 - **clear qos autoqos**
 - **clear port qos *mod/port* autoqos**
- The following features are not supported with a Supervisor Engine 720 in software release 8.2(x):
 - TCP Intercept.
 - WCCP.
 - IGMP version 3.

Software Release 8.2 Unsupported Hardware

This section lists the unsupported hardware in software release 8.2(x):

- The OSMs are not supported with Supervisor Engine 720 in software release 8.2(x). The “Optical Services Modules” section on page 17 lists the OSMs.
- The IPSec Virtual Private Network (VPN) Acceleration Services Module (WS-SVC-IPSEC-1) is not supported in software release 8.2(x).

Features for Supervisor Engine Software Release 8.1



Note

Maximum switching performance is achieved when all switch components are fabric enabled. The presence of nonfabric-enabled switching modules might impact overall switching performance.

These sections describe the features in software release 8.1, 30 June 2003:

- Software Release 8.1 Hardware Features, page 44
- Software Release 8.1 Software Features, page 45
- Software Release 8.1 Unsupported Software Features, page 46
- Software Release 8.1 Unsupported Hardware, page 47

Software Release 8.1 Hardware Features

Software release 8.1 provides initial support for these modules and chassis:

- Supervisor Engine 720 (WS-SUP720)
- 4000 W DC-power supply (PWR-4000-DC)

- Cisco 7609 router chassis, 9 vertical slots (CISCO7609)
- Catalyst 6509-NEB-A chassis, 9 vertical slots (6509-NEB-A)
- 48-port 10/100/1000 Ethernet Module, RJ-45, fabric enabled (WS-X6748-GE-TX)
- 24-port Gigabit Ethernet Module, requires SFPs, fabric enabled (WS-X6724-SFP)
- 4-port 10-Gigabit Ethernet Module, requires XENPAKs, fabric enabled (WS-X6704-10GE)
- XENPAK—Up to 10-kilometer range, 10GBASE-LR Serial 1310-nm long-haul (SMF) (XENPAK-10GB-LR)

Software Release 8.1 Software Features

Software release 8.1 provides support for these software features:

- VTP version 3—VTP version 3 differs from earlier VTP versions in that it does not directly handle VLANs. VTP version 3 is a protocol that is only responsible for distributing a list of opaque databases over an administrative domain. When enabled, VTP version 3 provides the following enhancements to previous VTP versions:
 - Support for extended VLANs.
 - Support for the creation and advertising of private VLANs.
 - Improved server authentication.
 - Protection from the “wrong” database accidentally being inserted into a VTP domain.
 - Interaction with VTP version 1 and VTP version 2.
 - Ability to be configured on a per-port basis.
- CallHome—You can use the CallHome feature to set your switch to e-mail or you can page a syslog message of a specified severity to a specified e-mail or pager address or a set of e-mail or pager addresses.
- Logging system information to a TFTP, FTP, or rcp server—You can configure your system to periodically execute up to 15 **show** commands and log the output of these commands in a file on a specified server. The information in the output can be used for debugging and troubleshooting purposes.
- TCL scripting—Tool Command Language (TCL) is a simple, programmable, text-based language that allows you to write command procedures that expand the capabilities of the built in set of commands. It is used primarily with interactive programs such as text editors, debuggers, illustrators, and shells. The Catalyst 6500 series switch software supports TCL version 7.4.
- VLAN port-provisioning verification—When VLAN port-provisioning verification is enabled, you must specify the VLAN name in addition to the VLAN number when assigning switch ports to VLANs. Because you are required to specify both the VLAN name and the VLAN number, this verification feature helps ensure that ports are not inadvertently placed in the wrong VLAN.
- FTP support for downloading software images.
- Increased number of command aliases—Use the **set alias** command to define up to 100 command aliases (shorthand versions of commands) for frequently used or long and complex commands.
- Increased number of MAC addresses supported (4097) for port security.
- Configure 802.1X guest VLANs on a per-port basis.
- Pipe command—Introduces a UNIX style output piping functionality to the Catalyst software. This feature enables you to *pipe* the output of a command, such as **show port**, to another command for post-processing.

- Support for the following MIBs:
 - ENTITY-MIB enhancement
 - CISCO-UDLD-MIB enhancement
 - CISCO-RF-MIB
 - CISCO-CALLHOME-MIB
 - CISCO-VTP-MIB enhancement
 - CISCO-SYS-INFO-LOG-MIB
 - CISCO-CAT6K-CROSSBAR-MIB enhancement
 - CISCO-ENTITY-ASSET-MIB
 - CISCO-SWITCH-ENGINE-MIB enhancement
 - CISCO-CATOS-ACL-QOS-MIB enhancement
 - CISCO-PAGP-MIB enhancement
 - CISCO-LAG-MIB enhancement
 - CISCO-IGMP-SNOOPING-MIB enhancement

Software Release 8.1 Unsupported Software Features

This section lists unsupported software features:

- The following QoS commands are present in software release 8.1(x) images, but are not tested or supported:
 - **set qos dscp-rewrite enable**
 - **set qos dscp-rewrite disable**
 - **output** keyword for the **set qos acl** and **clear qos acl** commands
 - **set qos dscp-mutation-map**
 - **clear qos dscp-mutation-map**
 - **dscp-mutation-map** keyword for the **show qos** commands
- The following QoS features and the commands used to configure them are not supported in a system with a Supervisor Engine 720 in software release 8.1(x):
 - No DSCP rewrite
 - Egress QoS
 - PFC3 egress DSCP mutation
 - Automatic QoS
 - RSVP
 - COPS
 - QoS and voice macros
 - NBAR
 - QDE
- The following features are not supported with a Supervisor Engine 720 in software release 8.1(x):
 - TCP Intercept.

- WCCP.
- IGMP version 3.

Software Release 8.1 Unsupported Hardware

This section lists unsupported hardware:

- The OSMs and the FlexWAN module are not supported with Supervisor Engine 720 in software release 8.1(x). The “Optical Services Modules” section on page 17 lists the OSMs.
- The Catalyst 6500 series switch service modules are not supported with Supervisor Engine 720 in software release 8.1(x). The “Service Modules” section on page 18 lists the service modules.
- The Catalyst 6500 series switch voice modules are not supported with Supervisor Engine 720 in software release 8.1(x). The “Voice Modules” section on page 16 lists the voice modules.
- The ATM modules are not supported with Supervisor Engine 720 in software release 8.1(x). The “ATM Modules” section on page 19 lists the ATM modules.
- The external Switch Fabric Modules are not supported with Supervisor Engine 720 because the Supervisor Engine 720 has an integrated switch fabric. The “Switch Fabric Modules” section on page 11 lists the Switch Fabric Modules.
- The Multilayer Switch Module is not supported with Supervisor Engine 720 in software release 8.1(x). The “Multilayer Switch Module” section on page 19 lists the Multilayer Switch Module.
- The Distributed Forwarding Card (WS-F6K-DFC) and 16-port Gigabit Ethernet switching module (WS-X6816-GBIC) are not supported in systems running Catalyst software on the supervisor engine and Cisco IOS software only on the MSFC.

Features for Supervisor Engine Software Releases 7.1 Through 7.6

For a complete list of hardware and software features for software releases 7.1 through 7.6, refer to the *Release Notes for Catalyst 6500 Series Switch Software Release 7.x* at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_1982.htm

Features for Supervisor Engine Software Releases 6.1 Through 6.4

For a complete list of hardware and software features for software releases 6.1 through 6.4, refer to the *Release Notes for Catalyst 6500 Series Switch Software Release 6.x* at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_11235.htm

Features for Supervisor Engine Software Releases 5.1 Through 5.5

For a complete list of hardware and software features for software releases 5.1 through 5.5, refer to the *Release Notes for Catalyst 6500 Series Switch Software Release 5.x* at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_6218.htm

Usage Guidelines and Restrictions

These sections provide usage guidelines and restrictions for the Catalyst 6500 series switches:

- System and Supervisor Engine, page 48
- Modules and Switch Ports, page 52
- SFP, XENPAK, and GBIC Behavior, page 56
- EtherChannel, page 56
- Quality of Service, page 57
- Automatic Quality of Service with Cisco IP Phones, page 59
- Multicast, page 59
 - IGMP Version 3 with MMLS, page 61
- Spanning Tree, page 62
- Access Control, page 62
- High Availability, page 63
- Multilayer Switching, page 64
- MIBs, page 64
- VLANs, VTP, and VLAN Trunks, page 65
- Authentication, Authorization, and Accounting, page 66
- TDR, page 66
- Auto-MDI/MDIX, page 67
- Bidirectional PIM, page 67
- Binary and Text File Configuration Modes, page 68
- 802.1X Authentication, page 70
- CiscoView, page 70

System and Supervisor Engine

This section contains usage guidelines, restrictions, and troubleshooting information that apply to the supervisor engine and to the switch at the system level:



Note

For information about AC power requirements and heat dissipation, refer to Chapter 2, “Preparing for Installation,” of the *Catalyst 6500 Series Switch Installation Guide*:
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/index.htm>

- Moving a Supervisor Engine 2 and MSFC2 between a Catalyst 6509 switch and a Catalyst 6503 switch may corrupt the MSFC2 NVRAM.

Workaround: Save the configuration to Flash memory and restore the configuration after the move. (CSCdy83320)
- Cisco 1200 series wireless access points may not receive power from a Catalyst 6500 series switch. This problem usually happens if the switch is reset or power cycled, if the module in the switch to which the access point is connected is reset or power cycled, or if a fast switchover occurs.

When this problem happens, a syslog message such as the following is displayed:

```
%SYS-3-PORT_DEVICENOLINK:Device on port m/p powered but no link up
```

However, this syslog message may not always be seen depending on the type of module used.

Workaround: Disable the Ethernet port that the access point is connected to for 2 to 3 minutes and then enable the port again. If this does not resolve the problem, replace the AIR-RM20A radio module with the AIR-RM21A module. (CSCeg05847)

- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
 - A 64-byte packet should be counted as 4 but is counted as 3
 - 65- to 79-byte packets are correctly counted as 4
 - An 80-byte packet should be counted as 5 but is counted as 4
 - 81- to 95-byte packets are correctly counted as 5
 - A 96-byte packet should be counted as 6 but is counted as 5
 (CSCdr56784)
- For software release 8.3(4) and later releases, the **show fabric status** command does not indicate the fabric speed.
- The **set option** command set was inadvertently removed from software releases 7.6(7) and 8.3(1). The **set option** command set will be available again (engineering mode only) in software releases 7.6(8) and 8.3(3).
- If you are running software release 8.3(1) or later on a Supervisor Engine 720 in text configuration mode and downgrade to software releases 8.1(x) or 8.2(1), the switch will crash with a TLB exception when the downgraded image is booted.

Workaround: To prevent this problem, enter the **clear config all** command before doing the downgrade. This problem is applicable only to the Supervisor Engine 720 in text configuration mode. Note that you do not see this problem when downgrading to software release 8.2(2). (CSCec56329)

- With Supervisor Engine 720, there is a CLI inconsistency between Cisco IOS images for the MSFC and Catalyst images for the supervisor engine due to changes to rate-limiter groups. The inconsistency does not affect rate limiting; it only affects the data displayed using the **show mls rate** command on the MSFC and **show rate limit** command on the supervisor engine. The inconsistency may cause the supervisor engine to enable/disable TTL Fail rate limiters as a side effect when some rate limiters, including RPF Fail, No-route, and ICMP unreachable, are enabled/disabled.

The inconsistency is due to a group change on the MSFC. There are two rate-limiter groups that were previously defined as follows:

- a) ACL input and ACL output
- b) RPF Fail, No-route, ICMP unreachable, and TTL Fail

In group b, for the MSFC, “TTL Fail” was replaced with “IP errors” in Cisco IOS Release 12.2(17a)SX1 but this change was not made in the supervisor engine software until software release 8.3(1).

If the MSFC and Catalyst images do not use the same grouping policy, the inconsistency problem remains. To avoid the inconsistency, note the following software guidelines:

- With Catalyst software release 8.3(1) and later releases, you must use Cisco IOS Release 12.2(17a)SX1 or later images.
- With Catalyst software releases 8.1(x) and 8.2(x), you must use images earlier than Cisco IOS Release 12.2(17a)SX1.

- When you save your configuration to a file when running software release 8.3(1), all trunk configurations are saved with the allowed VLAN range of 1 to 4094. If you try to reuse this configuration when downgrading to an earlier software release, all trunk-related commands fail because the earlier software release is expecting a VLAN range of 1 to 1005 and 1025 to 4094.
- MAC addresses—Theoretical and recommended limits
 - PFC/PFC2: 128K theoretical maximum, 32K recommended
 - PFC3: 64K theoretical maximum, 32K recommended
- A Supervisor Engine 2 might show 100 percent traffic utilization in the **show system** and **show traffic** command displays. This problem is a cosmetic issue. To correct the problem, you need to reprogram the Supervisor Engine 2 EPLD. To reprogram the EPLD, download the `epld-sup2-trafficmeter-swupdate.hz` image and follow the instructions documented in the `README.epld_update` file. (CSCdx54751)
- The **standby use-bia** option should not be used in an HSRP configuration. MLS entries are not created when you use the **standby use-bia** option. When you configure the **standby use-bia** option, if an HSRP active interface goes up and down, there will be no router CAM address for the standby VLAN interface. Without the router CAM entry, no shortcuts are created. This problem is independent of any MSFC Cisco IOS release. (CSCdz17169)
- When upgrading an image (image synchronization) from the active supervisor engine to the standby supervisor engine, the standby supervisor engine and possibly other modules might report “Minor hardware problem in Module X” to the console display.

Workaround: Either reset the individual modules reporting this error, or reset the switch. (CSCdv51172)

- ATA Flash PC cards are supported with software release 7.5(1) and later releases. However, we recommend using software release 7.6(1) or later releases because these releases have corrected earlier Flash file corruption issues.
- When the diagnostic mode is set to **complete** (`set test diaglevel complete` command), the system might display “local bus stall error” messages when modules come online. The messages are erroneous and can be ignored. This problem does not occur when the system is configured to run **minimal** (default) diagnostics.

Workaround: Do not set diagnostics to **complete**. (CSCdw09555)

- In a redundant supervisor engine configuration, both supervisor engines must be running the same boot ROM version. For information on upgrading the boot ROM version, refer to the *Catalyst 6500 Series Switch Supervisor Engine 2 Boot ROM and Bootflash Device Upgrade Installation Note* at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_12667.htm#xtocid41960
- For Supervisor Engine 1, the minimum boot ROM required for software release 5.4(1) and later releases is 5.3(1). For Supervisor Engine 2, the minimum boot ROM required for software release 6.2(2) and later releases is 6.1(3).
- IPX Layer-3 switched traffic with a SAP encapsulation type (Novell Ethernet 802.2) to non-SAP encapsulation type (Novell Ethertype's: Ethernet 802.3, Ethernet II, and Ethernet SNAP) and vice versa, follows the software forwarding path (via MSFC/MSFC2) on the PFC and PFC2 forwarding engines. This might cause high CPU utilization on the MSFC/MSFC2.

Workaround: Avoid SAP to non-SAP and vice versa encapsulation changes when doing IPX Layer 3 switching.

- When a Supervisor Engine 2 is running in truncated mode with QoS enabled and policers configured, the traffic subject to policing that is received on a fabric-enabled switching module destined to a non-fabric-enabled switching module is overpoliced. The traffic is policed to half the value configured in the policer. (CSCds02280)
- If you perform a manual switchover or reset a switch while high-availability events are waiting in the queue of the standby supervisor engine, when the events will be completely processed is not known, and all configurations might not synchronize to the standby supervisor engine properly. (High-availability events are the result of changing the configuration through the CLI.) We suggest that after changing the configuration, you allow additional time before resetting the switch to allow the supervisor engine to process all synchronized events. (CSCdp59261)
- With a PFC2, traffic that matches an egress reflexive ACL is handled by the MSFC2 as a partially switched flow. (CSCds09775)
- Changing the console port baud rate from 19,200 to 38,400 incorrectly sets the console port to 9600 baud. After a reset, the console port baud rate is 38,400. Changing the rate to 38,400 from any other setting works correctly. (CSCdk86876)
- In extremely rare conditions, if you enter the **show module** command, the status of the MSFC on the standby supervisor engine might be displayed as **other**. This has no impact on MSFC behavior and you should ignore this display. (CSCdp87997)
- With PFC or PFC2 and a standard network topology as shown below where you have multicast senders in the core and multicast receivers on the access layer:

		Layer 3 distribution No. 1		
	/		\	
Layer 2 access				Core
	\		/	
		Layer 3 distribution No. 2		

If both distribution switches have two supervisor engines and MSFCs and are configured to provide multicast functionality for the same access VLANs, then you will see high CPU utilization on the non-DR routers due to non-RPF traffic. (CSCdr74908)

- If you configure aging for UDP, it could slow down the removal of TCP entries belonging to a terminated connection. You might see entries no longer used in the NetFlow table being aged with the regular aging time of all the NetFlow entries instead of the very fast LDA aging.
Workaround: Enable the fast UDP aging only when it is really needed (for example, when load balancing UDP). (CSCdp79475)
- In a system with a Supervisor Engine 2 and WS-X6101 (ATM LANE) modules, ACLs that you configured from the CLI or COPS on the ATM LANE module ingress ports do not work. (CSCds09425)
- With Supervisor Engine 1 and PFC, online diagnostic failures are experienced on modules during bootup, online insertion, or module reset if you reconfigure the QoS default-action MAC ACL to include an aggregate policer with an action of drop. The system default does not include an aggregate policer in the default-action MAC ACL. The likelihood of the diagnostics failures increases as the amount of traffic being policed (dropped) by that aggregate policer increases. As the rate value specified in the policer decreases, the amount of traffic matching all ACLs specifying that aggregate policer increases. (CSCdp15471)



Note For switches with Supervisor Engine 2 and PFC2, CSCdp15471 is resolved in software release 6.1(1a).

- In a 13-slot chassis with redundant Supervisor Engine 2s, if the diagnostic mode is set to **bypass**, the bringup time of the system may be longer.

Workaround: Set the diagnostic mode to **minimal** or **complete**. (CSCdw09563)

- In a 13-slot chassis with a large number of installed modules (especially 48-port 10/100 modules), there might not be enough NVRAM to save the configuration. In this event, use the text file configuration mode.

Modules and Switch Ports

This section contains usage guidelines, restrictions, and troubleshooting information that apply to modules and switch ports:

- With software release 8.2(1), new CLI commands have been developed to deal with packet buffer memory errors that could occur with the WS-X6248-RJ-45, WS-X6348-RJ-45, and WS-X6348-RJ45V modules (these errors are documented in CSCec37610).

You are given two options to deal with these errors. The first option is to put the ports with this error condition in err-disable state. The second option is to power cycle the module. Putting the ports in the errdisable state is configured as the default. Additionally, there is a new errdisable-timeout cause: packet-buffer-error. The new CLI is as follows:

```
Console>(enable) set errordetection packet-buffer ?
errdisable
powercycle
Console>(enable) set errordetection packet-buffer errdisable
Packet buffer error detection set to errdisable.
Console>(enable) set errordetection packet-buffer powercycle
Packet buffer error detection set to powercycle.
Console>(enable)
```

```
Console> show errordetection
Inband error detection: disabled
Memory error detection: disabled
Port counter error detection: disabled
Packet buffer error detection: powercycle
Console> show errdisable-timeout
ErrDisable Reason      Timeout Status
-----
bpdu-guard              disable
channel-misconfig      disable
duplex-mismatch         disable
udld                    disable
crossbar-fallback       disable
packet-buffer-error     disable
other                    disable
```

Interval: 300 seconds

Port	ErrDisable Reason
5/1	packet-buffer-error
5/2	packet-buffer-error
5/3	packet-buffer-error
5/4	packet-buffer-error

- The WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX modules do not support the following:
 - More than 1 Gbps of traffic per EtherChannel
 - ISL trunking
 - VLAN translation
 - Jumbo frames
 - 802.1Q tunneling
 - Traffic storm control
 - In software release 7.6(x) and earlier releases: Ingress SPAN sources when the switch is operating in truncated and compact modes (also applies to the WS-X6516A-GBIC module)



Note With software release 8.2(1), due to firmware enhancements, the oversubscription problems associated with EtherChannel are no longer an issue with the WS-X6548-GE-TX module.

- If a link partner has auto-mdix enabled, this will interfere with the TDR cable diagnostics test and the test results will be misleading. Auto-mdix should only be enabled on one end of the link. (CSCea73643)
- With some legacy modules (such as WS-X6148-RJ45/RJ21, WS-X6248, and WS-X6348), jumbo frames are passing through even though jumbo frames have been disabled on the ports. This behavior is expected for the port ASICs on these legacy modules. (CSCeb20374)
- The 8-port T1 PSTN interface module (WS-X6608-T1) voice ports will not retain their configuration across switch reboots if the switch is in text config mode.

Workaround: Manually configure the T1 voice module after each switch reset. This problem only applies if the switch is in text config mode. (CSCdv04864)

- When the WS-X6548-RJ-45 is operating at 10Mb mode, pre-1994 NICs on ports 7, 15, 23, 31 and 39 may have connectivity problems. If these ports are having connectivity problems, enable auto-polarity detection in the NIC driver (where this is available) or use any of the other module ports. For additional information, refer to CSCdx15951.
- With a Switch Fabric Module installed and the switch in flow-through mode, resetting a fabric-enabled module during periods of high traffic might cause other modules to reset. This situation can cause temporary traffic loss until the reset module comes back online. This problem is only seen when the diagnostics are set to **minimal** or **complete** (**set test diaglevel** command).

Workaround: Power cycle the module (**set module power up/down mod_num**) or set the diagnostic mode to **bypass**. (CSCdw04861)

- When you connect a Cisco IP Phone 7960 to a port on the 10/100 Ethernet switching module that supplies inline power, the phone might lose power after switching from wall power back to inline power. The link remains up but the phone is down. This problem only occurs at 10 Mbps.

Workaround: Disconnect and then reconnect the cable between the switch port and the phone. (CSCdr37056)

- If a module fails to come online after a software upgrade, as a workaround, reset the module to bring it online. (CSCdu77125)
- When a module is reset due to a firmware download, the module may take 30 to 50 seconds (depending on the type of module) to come online and another 2 to 30 seconds (depending upon whether PortFast is configured or not) for spanning tree related events.
- The Distributed Forwarding Card (WS-F6K-DFC) and 16-port Gigabit Ethernet switching module (WS-X6816-GBIC) are not supported in systems running Catalyst software on the supervisor engine and Cisco IOS software only on the MSFC. These items are supported on systems running Cisco IOS Release 12.1(8a)E or later on both the Supervisor Engine 2 and the MSFC2. For more information, refer to the Release Notes for 12.1(8a)E on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/ol_2310.htm

- You cannot reset individual ports on WS-X6608-T1 or -E1 modules. To reset a port, reset the module. (CSCds19417)
- When you hot insert a module into a Catalyst 6000 or 6500 series chassis, be sure to 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.

If you see minor hardware failures or sync errors on bootup, reconfirm that the supervisor engine and all the switching modules are fully seated, the ejector levers are fully depressed, and the thumbscrews are fully tightened.

- There is a cabling issue with the 48-port 10/100BASE-TX switching module (WS-X6248-TEL). The WS-X6248-TEL module RJ-21 connectors **do not** support Category 3 RJ-21 telco connectors and cabling. Using Category 3 connectors and cabling causes carrier sense errors. The connectors are keyed for Category 5 telco connectors and cables. You **must** use Category 5 RJ-21 telco connectors and cables.
- 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower only support IEEE 802.1Q VLAN trunking; they do not support ISL trunking. Do not configure ISL trunks on 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower. The restriction against ISL VLAN trunking is the only known problem with hardware version 1.1 or lower of these modules. If you do not require ISL VLAN trunking, these modules are fully functional. The ISL VLAN trunking problem has been corrected in hardware version 1.2 or later of these modules. If you wish to return a WS-X6224-100FX-MT module with a hardware version of 1.1 or lower, contact Cisco Systems.

You can identify WS-X6224-100FX-MT hardware versions using one of the following two methods:

- Command-line interface (CLI) method—Use the **show version** command to identify the hardware version of the WS-X6224-100FX-MT module as follows:

```

Console> show version
< ... output truncated ... >
Mod Port Model                               Serial #    Versions
-----
< ... output truncated ... >
5   24   WS-X6224-100FX-MT   SAD02470006 Hw : 1.1
< ... output truncated ... >
Console>

```

The example shows a WS-X6224-100FX-MT module with a hardware version of 1.1; this version does not support ISL VLAN trunking.

- Physical inspection method—Look for the part number that is printed on a label on the outer edge of the component side of the module. Versions 73-3245-04 or lower do not support ISL trunking.
- When multiple instances are configured over a LANE trunk and when the root for one of the instances is moved, the other instances stop receiving BPDUs. The fix for this problem will be available in a Cisco IOS Release for the ATM LANE module later than Release 12.1(2)E1. (CSCdr88794)
- The **show module** command might show different versions for different modules in the chassis when upgraded with versioning enabled. (CSCdr55665)
- The following **debounce timer** command options have been added to increase the jitter tolerance on 10/100 UTP ports to make them interoperable with out-of-spec NICs:
 - set option debounce enable**—Sets debounce to 3.1 seconds on 10/100 cards.
 - set option debounce disable**—Sets debounce to 300 ms. The default is 300 ms debounce. (CSCdp56343)
- If a 16-port Gigabit Ethernet fabric-enabled GBIC switching module (WS-X6516-GBIC) is fully populated with 1000BASE-T GBICs (WS-G5483), it might be difficult to access the insertion/removal bracket on the module.

Workaround: Remove at least two of the 1000BASE-T GBICs before removing the module. (CSCdw25775)
- If a 16-port Gigabit Ethernet fabric-enabled GBIC switching module (WS-X6516-GBIC) is fully populated with 1000BASE-T GBICs (WS-G5483), it might be difficult to remove the module in the slot above the WS-X6516-GBIC module.

Workaround: Remove at least two of the 1000BASE-T GBICs before removing the module above the WS-X6516-GBIC module. (CSCdx19538)
- A SPAN session with a 10/100 source port and a Gigabit destination port might result in duplicated packets on the destination port. (CSCea32926)
- Voice modules, such as a WS-X6624-FXS and a WS-X6608-T1/E1, fail to register with the Cisco CallManager if a WS-X6148-GE-TX is used for the Cisco CallManager connection.

Workaround: Use another type of module, such as a WS-X6148-RJ45V, for the Cisco CallManager connection.

This problem is resolved in Cisco CallManager Release 3.3(3)sr1. (CSCeb38168)
- The WS-X6748-GE-TX module, and possibly other modules, might take an unusually long time to come online. This problem is seen only when Layer 2 port security ratelimiters *are not* enabled, there is significant traffic from Ixia on all the trunk ports, and the switch is rebooting. The problem is not seen when Layer 2 port security ratelimiters are enabled.

Workaround: Enable Layer 2 port security ratelimiters by entering the **set rate-limit l2port-security enable** command. Note that this command is not supported in truncated mode and is supported only on PFC3. (CSCee44405)

SFP, XENPAK, and GBIC Behavior

This section contains usage guidelines, restrictions, and troubleshooting information that apply to SFP, XENPAK, and GBIC behavior:

- All non-Cisco SFPs and XENPAKs come up as “Faulty” and will not work. The port is marked “Failed.” A syslog is printed stating that the integrity check on the transceiver has failed. This behavior is true for SFPs since software release 8.1(1), and XENPAKs since software release 8.1(2).
- All unsupported Cisco SFPs and XENPAKs come up as “Unknown”. A syslog is printed stating that the transceiver is unsupported. This behavior is true for unsupported Cisco SFPs and XENPAKs in software release 8.2(1) only. In software release 8.1(x), all unsupported Cisco SFPs and XENPAKs come up as “Faulty.”
- All Cisco and non-Cisco SX, LX, LH and ZX GBICs will work with the correct port type. Other third-party GBICs (non-SX, non-LX, non-LH and non-ZX) may or may not work starting with software release 7.2(1). That is, the GBIC might be marked “Faulty,” and the port marked “Failed” or they might come up as “Unknown.” Some third-party GBICs recognized by the software as “Unknown” may work.

EtherChannel

This section contains usage guidelines, restrictions, and troubleshooting information that apply to EtherChannel:

- The WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX modules have a limitation with EtherChannel. EtherChannel is supported on these modules for all configurations (10, 100, and 1000 Mbps speeds) but be aware of the following cases of oversubscription when you are configuring these modules:



Note With software release 8.2(1), due to firmware enhancements, the following oversubscription problems are no longer an issue with the WS-X6548-GE-TX and WS-X6548V-GE-TX modules.

- On these modules there is a single 1-Gigabit Ethernet uplink from the port ASIC that supports eight ports. For EtherChannel, the data from all links in a bundle goes to the port ASIC, even though the data is destined for another link. This data consumes bandwidth in the 1-Gigabit Ethernet link. For these modules, the sum total of all data on an EtherChannel cannot exceed 1 Gigabit.
- You could also run into the oversubscription problem if you have four WS-X6148-GE-TX or WS-X6148V-GE-TX modules running at 100 Mbps with 48 EtherChannels, and each channel having 4 ports (1 port per module).
- If you use the Switch Fabric Module with the WS-X6548-GE-TX or WS-X6548V-GE-TX modules, that configuration would avoid the oversubscription problem. The Switch Fabric Module interface filters and distributes the packets to the correct module per the EtherChannel bundle hash. However, you must have one port per module in the bundle. Once you have more than one port of a WS-X6548-GE-TX or WS-X6548V-GE-TX module in an EtherChannel bundle it will start oversubscribing.



Note Using channeling for Layer 1 redundancy is a valid configuration option with these modules.

- Catalyst switches running supervisor engine software releases 6.2(x) and later cannot form a channel with HP-server NICs. TLV checking, which was added for PAgP packets in software release 6.2(1), uncovered a problem with HP-UX systems where the packet length was set incorrectly. HP has an updated driver available that can solve the problem; contact HP Technical Support for details. (CSCdu84575)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a 4-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower 4-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)

Quality of Service

This section contains usage guidelines, restrictions, and troubleshooting information that apply to QoS:

- The rate and burst parameters for microflow/aggregate policing are specified in terms of kbps (kilobits per second) and Kb (kilobits). However, the following should be noted:
 - Rate specification—1 kbps is equivalent to 1000 bits per second (as opposed to 1024 bits per second)
 - Burst specification—1 Kb is equivalent to 1024 bits
- Running two or more QoS commands from different Telnet or SSH sessions could cause the switch to hang or reset. We recommend that you do not execute two or more QoS commands simultaneously from different Telnet, SSH, or console sessions. (CSCdy74994)
- With Supervisor Engine 1 and Supervisor Engine 2, the **set port qos mod/port {port-based | vlan-based}** command configures all ports on switching modules with **1p1q0t/1p3q1t** QoS port architecture.
- Microflow policing does not support policing of identical flows arriving on different interfaces simultaneously. Attempts to do so lead to incorrectly policed flows. (CSCdt72147)
- If there is an error in installing any COPS policy, a successful commit is sent to the PDP even if the policy was not correctly installed. In such situations, any modifications to the port's role combination does not install the correct policy on the port and might result in a switch reset. (CSCdp66572)
- If you create a security ACL with the redirect option and then replace the module that has the redirect port with another kind of module, the security ACL does not have the redirect port list anymore.

Workaround: Manually modify the security ACL with the new redirect port information. (CSCdp74757)
- If you download a COPS ACL containing a policer to the switch and the switch cannot support the exact rate/burst supplied by the policer, no message informs you that the rate/burst was rounded off to the nearest value that the hardware could support. (CSCdr28715)
- If the QoS policy source is set to COPS, Catalyst 6500 series switches do not support nonzero WRED minimum values. If a COPS QPM server sends down a COPS policy with a nonzero WRED minimum value, no error report is returned to the COPS server. As a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)

- On a Catalyst 6500 series switch, when the switch QoS policy source is COPS, no COPS roles are defined for a port, and the port policy source is COPS, the values that you set for the QoS configuration (such as queue mappings and sizes) are inappropriate. For example, all CoS values get mapped to the strict-priority queue on a 1p2q2t or 1p1q4t port type. This situation can lead to bandwidth starvation for other ports in the switch, especially, if these ports with a strict-priority queue are generating high rates of traffic.

Workaround: Avoid this problem is to either configure a COPS role on all ports in the switch or configure all ports without a COPS role to use local policy. (CSCdp44965)

- If a large number of QoS ACLs are defined on the system during switch bootup, some packets might get switched before the QoS ACLs are installed in hardware. This scenario would result in some packets getting an incorrect ToS or no policing applied. After the QoS ACLs are installed in hardware, the correct ToS and policers are applied. It is considered inappropriate to block traffic from flowing until all the QoS policy is installed. (CSCdp68608)
- After setting the QoS policy source to local, you might need to wait approximately 20 seconds before the QoS policy source can be set back to COPS. (CSCdp34367)
- The COPS policy fails to install on ports with a large number of QoS policers.

Workaround: Unmap the local ACLs before installing the COPS policy. (CSCdp63138)

- Use the QoS strict-priority queues for your highest-priority traffic only. The strict-priority queues are designed to accommodate only a limited volume of traffic. If you overload the strict-priority queues, the supervisor engine cannot service the standard queues. (CSCdm90683)
- With QoS disabled, an EtherChannel can contain ports with both strict-priority queues and ports without strict-priority queues. With QoS enabled, an EtherChannel cannot contain both port types. If you enable QoS, ports drop out of any EtherChannels that contain both port types.
- When COPS is the QoS policy source, TFTP traffic and switching might be affected if a COPS policer is configured with a rate or burst value that the Catalyst 6500 series switch cannot support. (CSCds16976)
- Except for ports that support 1p1q0t/1p3q1t and 1q2t/1p2q2t, the **set port qos trust** command and the **trust-ipprec** and **trust-dscp** port keywords are not supported on 10-, 10/100-, and 100-Mbps ports. Instead, configure ACLs with the **trust-cos**, **trust-dscp**, and **trust-ipprec** ACE keywords. Note that the **trust-cos** port keyword can be used on 10-, 10/100-, and 100-Mbps ports to enable receive-queue drop thresholds.



Note The WS-X6148-RJ45, WS-X6148-RJ45V, WS-X6148-RJ21, and WS-X6148-RJ21V modules also support trust-cos, trust-ipprec, and trust-dscp.

- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.
- With heavy COPS protocol traffic between either the COPS-DS client or the COPS-RSVP client and the PDP, it is possible for a connection keep-alive timeout event to occur and for the COPS connection manager to miss a Client Close from the PDP. When this happens, the switch might have an exception later. (CSCdp64213)

Automatic Quality of Service with Cisco IP Phones

This section contains usage guidelines, restrictions, and troubleshooting information that apply to configuring automatic QoS with Cisco IP Phones:

- Cisco IP Phone 79xx phone marking—The Cisco IP Phone 79xx does not mark its protocol packets such as DHCP, TFTP, and DNS packets with nonzero DSCP values. This causes the IP phone to see DHCP, DNS, and/or TFTP timeouts when an uplink port on a switch is oversubscribed. This results in the IP phone taking a long time to register with the Cisco CallManager or the IP phone might not register at all. Additionally, phone directories, IP phone services, call logs, ring tones, and so on become unavailable or do not work correctly for the IP phone user.

Workaround: Use custom QoS ACLs instead of automatic QoS on the switch. For this problem, caveat CSCdy62735 has been logged against the Cisco IP phone.

- Cisco CallManager is not marking protocol packets—This Cisco CallManager issue is similar to the above issue (CSCdy62735). If uplink ports are oversubscribed, TFTP packets from the Cisco CallManager are dropped by the switch.

Workaround: Use custom QoS ACLs instead of automatic QoS on the switch.

- Cisco IP Phone 79xx phone reset problem—The Cisco IP Phone 79xx resets when the IP phone's PC port is oversubscribed. This problem is seen in rare circumstances; the IP phone's PC port should not get oversubscribed unless there is a broadcast storm or some other outage in the network. This problem was addressed with caveat CSCdy50584 and has been resolved in Cisco CallManager release 3.3(2) SPC.
- CDP issue—CDP protocol packets are not CoS labeled correctly. This problem prevents the switch from properly prioritizing the “hello” packets being sent to and from the IP phone. Under heavy traffic conditions, this results in losing the IP phone from the CDP perspective. This problem was addressed with caveat CSCdy53339 and has been resolved in software release 7.6(1) and later releases.
- Cisco SoftPhone does not tag any voice signaling packets—With this problem, voice signaling packets from Cisco SoftPhones get dropped and Cisco Soft Phones fail to connect to the Cisco CallManager and the user cannot make or receive calls if the switch uplink ports are oversubscribed.

Workaround: Use custom QoS ACLs instead of automatic QoS on the switch. For this problem, caveat CSCdy60186 has been logged against Cisco SoftPhone.

Multicast

This section contains usage guidelines, restrictions, and troubleshooting information that apply to multicast protocols and traffic on the switch:

- With bidirectional PIM enabled, a TTL=1 multicast packet is not bridged to the ingress VLAN when rate limiting of TTL failure is enabled and index redirection of TTL failure is configured. This problem is seen with PFC, PFC2, and PFC3A. It is not seen with PFC3BXL. (CSCed66503)
- The Cisco IOS **last-member-query-interval** command allows you to increase the time that the router waits for host responses to IGMP GS queries (group-specific queries). The switch implements this interval statically, as defined in RFC 2236 (the default is 1000 ms). If you configure a router that is connected to the switch with a “last-member-query-interval” that is greater than the default interval as defined in RFC 2236, and you enable IGMP snooping on the switch, then hosts connected to the switch might have packets discarded if these hosts are unable to respond to GS queries within the interval implemented on the switch. The supervisor engine software does not modify its behavior

based on the last-member-query-interval that is configured on the connected routers. Do not modify the last-member-query-interval on the routers that are connected to the switch if IGMP snooping is enabled.

Workaround: Disable IGMP snooping on the switch. (CSCdu72041)

- A new command, **set igmp ratelimit [disable | enable]**, has been added to the 6.x, 7.x, and 8.x software releases starting with the following releases:
 - 6.4(7)
 - 7.6(5)
 - 8.2(1)

IGMP rate limiting is disabled by default. In the 6.4(x) software release, rate-limit counters are supported only in text configuration mode. The **set igmp ratelimit [disable | enable]** command is supported in both text and binary configuration modes in all software release trains.

If IGMP rate limiting and multicast are enabled, multicast router ports might age out sporadically because the rate of the multicast control packets (such as PimV2-hellos or IGMP-General Queries) exceed the IGMP rate-limit watermarks that were configured. The default values for these watermarks is 100. The workaround (documented in CSCea44331) is to increase the PimV2-hellos rate limit; we recommend that you set the value to 3000 using the **set igmp ratelimit pimv2 3000** command. You can also increase the IGMP-General Queries rate limit; we recommend that you set the value to 500 using the **set igmp ratelimit general-query 500** command.

- In software release 8.3(1) and later releases, IGMP rate-limiting commands are deprecated and a multicast rate-limiting mechanism is introduced. Through this mechanism, IGMP control packets are rate limited. Because the IGMP rate-limiting mechanism is deprecated and a new multicast rate-limiting mechanism is introduced, all caveats specific to IGMP rate limiting do not apply to software release 8.3(1) and later releases. The new commands introduced in software release 8.3(1) are the **set multicast ratelimit** commands and the **show multicast ratelimit-info** command. For details on these commands, see the *Catalyst 6500 Series Switch Command Reference*, software release 8.3(1).
- The maximum number of supported user-configured multicast CAM entries is 256. After adding 256 permanent or static multicast CAM entries, the switch produces the error “Failed to add CAM entry.” After adding 256 static or permanent CAM entries, all attempts to add more static or permanent multicast entries fail. This is true for the same port/same VLAN, different port/same VLAN, and different port/different VLAN.
- If you install an MSFC2 and the VLAN interface that is defined on the MSFC2 is in shutdown mode, bridged IP multicast traffic will not be policed. (CSCdu12731)
- The only ports that send out the GMRP LeaveAll messages are the ports that have previously received GMRP joins.
- With software releases 7.1(1) and later, the maximum number of Layer 2 multicast entries is 15488.
- If RGMP-enabled routers connected to an RGMP-enabled Catalyst 6500 series switch join many groups, the switch might run out of memory. Ensure that the total number of entries displayed by the **show rgmp group count** command is fewer than 800. The actual maximum number of entries will vary depending on the features enabled on the Catalyst 6500 series switch and the amount of memory installed.
- When a multicast goes to both bridged and routed addresses, the multicast packets going to the routed addresses are Layer 3 switched, and the multicast matches an ACL so that QoS rewrites the ToS byte in the multicast packet. QoS does not rewrite the ToS byte for the multicast packets that are bridged.
- We recommend that you do not use more than 1500 multicast groups with GMRP. This restriction does not apply to IGMP.

- In extremely rare conditions, multicast traffic might be blocked due to a mismatch between hardware and software entries. (CSCdp81324)
- SPAN, RSPAN, Private VLANs, and RGMP are not supported with IGMP version 3 snooping.
- Be aware of the following multicast traffic caveats specific to Supervisor Engine 2 (these caveats apply to *all* software releases supporting Supervisor Engine 2):
 - If an outgoing IOS ACL is configured on an interface, Supervisor Engine 2 based systems will match/apply the IOS ACL in software. This results in *all* outgoing multicast flows for that interface being handled in software (based upon specific **deny/permit all** statements). MMLS is effectively disabled for the interface. Be aware that handling outgoing IOS ACLs in software increases CPU utilization.
 - Outgoing VACLs are not applied to multicast traffic with Supervisor Engine 2.
- IGMP version 3 reports are flooding on VLANs. The reports should be sent only to IGMP version 3 router ports and IGMP version 3 hosts. This problem only occurs with PFC2. There is no problem with PFC3. (CSCdx51216)
- Under conditions of severe load on the switch, such as either a large number of VLAN ports and their port-state changes or a high rate of multicast control traffic, IGMP snooping may get automatically disabled for approximately 2 minutes. When IGMP snooping is automatically disabled, a syslog is generated and the **show igmp mode** command and the **show multicast protocol status** command show that IGMP is operationally disabled.

IGMP Version 3 with MMLS

This subsection contains usage guidelines, restrictions, and troubleshooting information that apply to IGMP version 3 with MMLS on the switch:

- IGMP version 3 with MMLS applies *only* to Supervisor Engine 720. On Supervisor Engine 2, IGMP version 3 snooping cannot be performed for MMLS-switched flows; therefore, MMLS cannot be enabled when IGMP version 3 is enabled.
- IGMP version 3 with MMLS applies to the SSM-Range configured on the MSFC. The SSM-Range should be either the default, or the ACL that you use to configure a range should have ACEs with the action as permit only.
- On Supervisor Engine 720, IGMP version 3 snooping works only with MMLS hardware-switched flows (as documented in CSCin51214). Therefore, IGMP version 3 snooping should be enabled if MMLS is enabled.
- With software release 8.3(3) and later releases, IGMP version 3 snooping does not work with static multicast CAM entries configured. If there are user-configured static multicast CAM entries that correspond to a multicast group operating in IGMP version 3, the multicast traffic directed to the multicast group does not reach the ports that are configured in the static multicast CAM entry. A symptom of this problem is when ports that are configured in the static multicast CAM entry do not receive traffic destined for that GDA MAC address.

Workaround: Disable IGMP version 3 snooping by entering the **set igmp v3-processing disable** command. (CSCee36768)

Spanning Tree

This section contains usage guidelines, restrictions, and troubleshooting information that apply to Spanning Tree:

- After upgrading from software release 5.x to software release 8.3(1), the switch comes up with Rapid-PVST+ as the default spanning tree protocol. Prior to the upgrade, the default spanning tree protocol was IEEE 802.1D bridge Spanning Tree Protocol. With IEEE 802.1D, the **show spantree summary** command shows the listening port count as 0 and constant. With Rapid-PVST+, the **show spantree summary** command shows the listening port count fluctuating. Resetting the switch does not correct the problem.

Workaround: Upgrade to software release 6.x and then upgrade to software release 8.3(1). (CSCee43648)

- MST problem—Powering down the Switch Fabric Module usually takes between 3 and 5 seconds. During this time, traffic and protocol packets are disrupted. The MST root port does not receive BPDUs during this period and the re-root mechanism is called (the re-root mechanism causes the root port to go to the blocking state). As soon as the MST port starts receiving BPDUs, the topology reconverges. (CSCdv86120)
- If the **forward delay**, **max age**, and **hello time** Spanning Tree Protocol (STP) parameters are reduced in value, ensure that the number of instances of STP are also reduced proportionally to avoid STP loops in the network.
- Occasionally (less than once in every 100 attempts), the console process might lock when an STP mode changes from PVST+ to MISTP.

Workaround: Reset the switch. (CSCds20952)

- If you have a Catalyst switch in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected switches to avoid undesirable root election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

Therefore, if another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could claim and win root bridge ownership because of the finer granularity in the selection of its bridge ID.



Note

The MAC address reduction feature is enabled by default on Cisco switches that have 64 MAC addresses (Cisco 7606, CISCO7603, WS-C6503, and WS-C6513).

Access Control

This section contains usage guidelines, restrictions, and troubleshooting information that apply to security:

- A security ACL will not take effect for sources that are present in the INCLUDE list if the IGMP version 3 state is in INCLUDE mode and the multicast source and receiver are in the same VLAN. (CSCdy15849)

- Note that the VACLs access-control **all** traffic passing through a VLAN. This includes broadcast traffic and packets going to and from the router. Therefore, you must use care when defining a VACL.

For example, to allow traffic from a local IPX client (daf11511) to a remote server (daf00402), the following VACL is configured (remote server is learned through a routing protocol):

```
set security acl ipx jg_ipx_permit
-----
1. permit any DAF00402 DAF11511
2. permit any DAF11511 DAF00402
3. permit any DAF01023 DAF01023
4. permit any DAF11511 0
5. permit any 0 0
6. permit any DAF11511 DAF11511
```

The VACL description is as follows:

- 1, 2. Allow IPX between client and server.
- 3. The router needs to see the RIP/SAP packets.
- 4. If packets are dropped during a connection, the client tries to find another route to the server by sending out RIP requests to IPX network 0.ffff.ffff.ffff. Not doing this results in a lost connection after packet drop.
- 5. Upon startup, a client sends its first packets to 0.ffff.ffff.ffff and uses 0.ffff.ffff.ffff as its one IPX address.
- 6. When a server connection socket is timed out, the client reconnects by sending a request to its local network to find its server.

As the example shows, just 1 and 2 is not enough; you also have to define 3 through 6 to achieve the goal. (CSCdm55828)

- Make sure that the redirect port defined in a VACL is on the same VLAN as the “incoming” VLAN for the packet that is to be redirected. Otherwise, the redirected packet will be dropped.

For example, a redirect VACL is defined on VLAN 5 and the redirect destination port is also on VLAN 5. If an MLS entry is destined to VLAN 5, packets that are coming from VLAN 2 hit this MLS entry and also hit the VACL redirect ACE (both VLAN 2 and VLAN 5 ACLs will be checked) and are redirected in the incoming VLAN, VLAN 2. The redirect destination port will drop them on VLAN 5 rather than on VLAN 2.

- In a Catalyst 6500 series switch with two Supervisor Engine 2s, if you have more than 300 QoS ACLs and each QoS ACL is mapped to a different VLAN, the active supervisor engine might reset after clearing all the QoS ACLs and then committing the change. (CSCdu85021)

High Availability

This section contains usage guidelines, restrictions, and troubleshooting information that apply to high availability:

- In single router mode (SRM) or dual router mode, when configuration changes are made in the running configuration of the designated router while the nondesignated router is either not fully up or has not completed the high-availability handshakes, negate (**no**) commands (such as **no shut** and **no ip address**) may not show up on the nondesignated router once the running configuration synchronization completes. After the high-availability switchover, the affected negate commands do not show up in the running configuration of the designated router either. This problem is documented in caveat CSCeg19764.

- MSFC configuration synchronization is only supported for IP and IPX configurations. Before enabling synchronization, you must ensure that both MSFCs have identical configurations for all protocols. If you are using AppleTalk, DECnet, VINES, or any other routing, you must manually ensure that identical configurations are on both MSFCs for all protocols.
- Redundant supervisor engines must be of the same type with the same model feature card. Note that WS-X6K-SUP1-2GE and WS-X6K-SUP1A-2GE (both without PFCs) are compatible for redundancy. For supervisor engines with PFCs, the PFCs must be identical for redundancy (two PFCs or two PFC2s).
- High availability does not support use of the Reset button. Pressing the Reset button to initiate a switchover results in a high-availability switchover failure.
Workaround: Make the active supervisor engine the standby supervisor engine first, and then remove it from the chassis. (CSCdp76806)
- NVRAM synchronization and high-availability synchronization does not work between supervisor engine software release 6.3(1) and any later version. (CSCdv43206)

Multilayer Switching

This section contains usage guidelines, restrictions, and troubleshooting information that apply to MLS:

- If you have routed flows with MLS disabled (no shortcuts created), candidate entries age out rapidly to ensure that the forwarding table is used as much as possible by shortcut flows. A side effect of this rapid aging of candidate entries is that the microflow policer does not work accurately because its policing history is lost when the entries age out. When the same flow creates a new entry, it gets the entire traffic contract again even if it had exceeded the contract before the entry aged out. (CSCdp59086)
- Layer 3 switching on the Catalyst 6500 series switches does not support full or destination-source flows for IPX traffic. With Supervisor Engine 1 and PFC, when the MLS flow mask is destination-source or full-flow, the **show mls entry ipx destination** command that should select a specific destination displays all IPX Layer 3 entries rather than just those for a specific destination IPX address. (CSCdm46984)

MIBs

This section contains usage guidelines, restrictions, and troubleshooting information that apply to SNMP MIBs, RMON groups, and traps:



Note

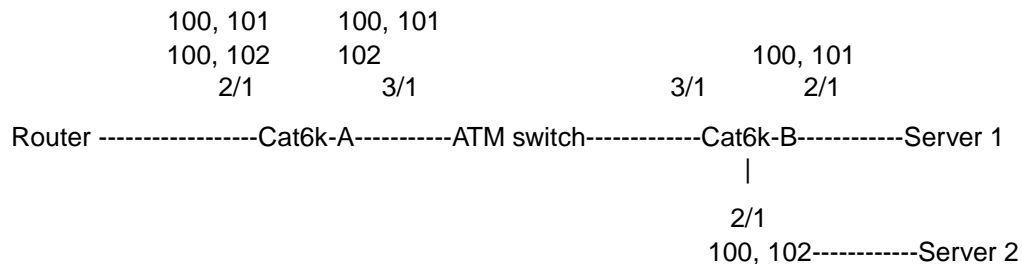
For information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory located at this URL:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

- You cannot use the tftpGrp MIB object to download Catalyst 6000 ATM software. (CSCdp16574)

VLANs, VTP, and VLAN Trunks

This section contains usage guidelines, restrictions, and troubleshooting information that apply to VTP, VLANs, and VLAN trunks:

- When manually pruning VLANs on trunks, if you have more than 64 trunks you need to run in text configuration mode; you cannot manually prune VLANs in binary configuration mode if there are more than 64 trunks.
- The VLAN locking feature causes configuration loss in text configuration mode. Therefore, the VLAN locking feature is not supported in text configuration mode. (CSCeb34004)
- Use caution when including the sc0 interface in a normal or private VLAN. Under heavy traffic conditions, there is a risk of losing connectivity with the interface. We recommend that you do not configure the sc0 interface in any VLAN with user data. (CSCdv12023)
- This problem is related to the following configuration:



The Cat6k-A configuration is as follows:

- 100—Primary VLAN
- 101—Secondary VLAN (isolated/community/two-way community)
- 102—Secondary VLAN (isolated/community/two-way community)
- 2/1—Promiscuous port carrying the mapping from VLAN 101 to VLAN 100 and VLAN 102 to VLAN 100
- 3/1—ATM trunk port carrying VLANs 100, 101, 102, 200, 300

The Cat6k-B configuration is as follows:

- 100—Primary VLAN
- 101—Secondary VLAN (isolated/community/two-way community)
- 102—Secondary VLAN (isolated/community/two-way community)
- 3/1—ATM trunk port carrying VLANs 100, 101, 102
- 2/1—Private port with VLAN 101 to VLAN 100 association
- 2/2—Private port with VLAN 102 to VLAN 100 association

In this configuration, assume that Server 1 is interacting with the router and there is no traffic between Server 2 and the router. If Server 2 suddenly starts interacting with the router, the traffic between Server 1 and the router might stop. This happens when the Cat6k-A 3/1 port is on the WS-X6101-OC12-MMF ATM module.

In summary, do not have a configuration with a promiscuous port on switch A and secondary ports on switch B connected through an ATM trunk on the WS-X6101-OC12-MMF module. (CSCdy03515)

- When using a VLAN interface other than the VLAN 1 interface, a VLAN added on a Catalyst 3500XL running 120.5.1-XP does not appear in the Catalyst 6500 series switch database. As soon as management interfaces are put back in VLAN 1, a VLAN configured on the 3500XL is sent properly to the Catalyst 6500 series switch through VTP. Check the status of CSCdr80902 in your Cisco IOS release. (CSCdr66376)
- In a redundant configuration, if you modify the VLAN mapping on the active supervisor engine and a high-availability switchover occurs before the VLAN mapping is synchronized between the supervisor engines, you might experience a mapping inconsistency (VLANs claimed by two different instances) if you reenter the mapping command.

Workaround: Recreate a new mapping on a different instance after the switchover. On the newly active supervisor engine, enter the **set vlan *vlan_num* mistp none** command and reenter the mapping. (CSCds27902)

Authentication, Authorization, and Accounting

This section contains usage guidelines, restrictions, and troubleshooting information that apply to authentication, authorization, and accounting (AAA):

- For login authentication, starting from software releases 5.5(15), 6.3(7), and 7.3(1), if you press the Enter key and then type in your password (<Enter> <password>) the ACS TACACS+ server will treat it as an indication that you are attempting to change your password. This behavior is related to CSCdx08395. Before the CSCdx08395 fix, the user privilege level was hard coded to 15 in the TACACS+ authentication request packet. With the CSCdx08395 fix, the user privilege level is set based on the privilege level that the user is authenticated as. For example, if the user is doing a login authentication, the privilege level would be 1. If the user is doing an enable authentication, the privilege level would be 15.

The Cisco ACS TACACS+ server acts differently for <Enter> <password>. For login authentication, if the user priv-lvl is hard coded to 15, <Enter> <password> is treated as a regular password attempt. If the user priv-lvl is set to 1 (CSCdx08395) during login authentication, then <Enter> <password> is treated as an indication of a changing password. The latter case is a behavior consistent with TACACS+ enable authentication and Cisco IOS software handling of <Enter> <password>. (CSCdy35129)

TDR

This section contains usage guidelines, restrictions, and troubleshooting information that applies to the time domain reflectometer (TDR) feature:

- The TDR test can only be run on 16 ports at a time. (CSCea46739)
- The TDR test does not provide accurate results if it is run on a link where the remote link partner is configured at 100-Mbps fixed speed (CSCea70930). 10 Mbps, 1000 Mbps, and auto speeds on the remote link partner will not interfere with the TDR test. Also, a 100-Mbps port without a link partner will complete the TDR test successfully.
- The WS-X6148 and WS-X6548 GE-TX modules have the following cable restrictions with the TDR test: If a Revision B0 Marvell PHY is used, the maximum cable length that can be detected is 115 meters. If a Revision C0 Marvell PHY is used, the maximum length that can be detected is 168 meters. (CSCea76395)

Auto-MDI/MDIX

With auto-MDI/MDIX you can use either a straight or crossover cable, and the module will automatically detect and adjust for the cable type. Auto-MDI/MDIX works with the speed set to auto/1000 Mbps, but not with the speed set to 10 Mbps or 100 Mbps. This means that the link will come up with either a straight or crossover cable if the speed is set to auto/1000 using the **set port speed mod/port auto** command or the **set port speed mod/port 1000** command. The link comes up even if the speed is autonegotiated at 10 Mbps or 100 Mbps in **auto** mode. However, if you enter the **set port speed mod/port 10** command or the **set port speed mod/port 100** command, the link fails to come up if the wrong cable is used.

Auto-MDI/MDIX has always been enabled on the following modules:

- WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6148-GE-TX, WS-X6548-GE-TX
Auto-MDI/MDIX works in 10-, 100-, and 1000-Mbps modes with autonegotiated and fixed speeds.
- WS-X6516-GE-TX
Auto-MDI/MDIX works with the speed set to auto/1000 Mbps, but not with the speed set to 10 Mbps or 100 Mbps.

- WS-X6316-GE-TX

With software release 8.2(1) and later releases, auto-MDI/MDIX is also enabled on the following modules:

- WS-X6748-GE-TX, Supervisor Engine 720 port 2 (RJ-45)
Auto-MDI/MDIX works with the speed set to auto/1000, but not with the speed set to 10 Mbps or 100 Mbps
- WS-X6148X2-RJ-45, WS-X6148X2-45AF
Auto-MDI/MDIX works with the speed set to auto, but not with the speed set to 10 Mbps or 100 Mbps.



Note

Auto-MDI/MDIX is not supported on any other 10/100-Mbps Ethernet modules or GBIC, SFP, and XENPAK ports.

With software release 8.3(1) and later releases, the **set port auto-mdix mod/port {enable | disable}** command is introduced to disable auto-MDI/MDIX on all the modules that currently have this feature enabled by default. Use the **show port auto-mdix [mod[/port]]** command to display auto-MDI/MDIX settings.

Bidirectional PIM

This section contains usage guidelines, restrictions, and troubleshooting information that apply to bidirectional PIM:

- Bidirectional PIM is supported on Supervisor Engine 720 and Supervisor Engine 32 (with Supervisor Engine 32, you need Cisco IOS Release 12.2(17d)SXB7).
- When configuring bidirectional PIM group ACEs, a deny is not accepted. Groups can only be included.
- (*,G/m) entries are installed on a best-effort basis as an optimization on source-only networks. There are several conditions where (*,G) may be installed on a source-only network.
- Bidirectional PIM flows related to only four route processors are hardware switched.

- With multiple bidirectional PIM route processors, flows related to only four route processors are hardware switched and these four route processors are chosen depending on the order in which they come up.

Binary and Text File Configuration Modes

The main purpose of storing configuration information in NVRAM blocks is to restore the system configuration when the switch comes up after a reset. The supervisor engine bring-up process includes reading the NVRAM blocks and using the configuration information in the blocks to configure the system. Before restoring the configuration from an NVRAM block, a new checksum is generated on the data in the block and the new checksum is compared with the checksum stored in the block itself. If both the checksums match, the data is determined to be valid and the data in the block is used to restore the configuration. If the checksum matching fails, the NVRAM block is deallocated and the default configuration is used.

There are two modes for storing the configuration file, binary configuration mode and text file configuration mode. These modes are described in the following sections.

Binary Configuration Mode

In binary configuration mode, the NVRAM configuration model uses binary data structures to save information. The NVRAM is allocated in blocks, and each data structure is stored as an NVRAM block as follows:

- A global block is statically allocated for saving global configuration information.
- Per-module NVRAM blocks are allocated for each module to store information for every module and port.
- Other NVRAM blocks include blocks for SNMP, VTP, SSH, NVRAM logging, and so on.

When you enter a command to configure a feature, the information is stored immediately in one of the NVRAM blocks. Some blocks are allocated at startup, such as the global block, the SNMP block, and the VTP block. Other blocks are allocated as needed. For example, a module block is only allocated when a nondefault setting is configured for the module or configured for a port on the module. Some NVRAM blocks also grow dynamically. The VTP block, by default, allows for 256 VLANs to be configured. If more than 256 VLANs are configured, the VTP block is expanded to allow 256 additional VLANs. Binary configuration mode provides an easy way to store the configuration immediately without the need for a **write memory** command to commit the configuration to NVRAM.

Binary storage of data is also space efficient. For example, remembering if a feature is enabled or not requires a single bit of NVRAM.

Text File Configuration Mode

A disadvantage of the binary configuration mode is that although configured features can be stored efficiently, a lot of NVRAM space can be wasted by features that are not configured by the user. For example, the global block currently requires approximately 150 KB, but users may have configured only a few features. Similarly, a 48-port module consumes approximately 25 KB of NVRAM space (about 0.5 KB per port) even if only a single port on the module has been configured with a nondefault setting.

With software release 6.3(1) and later releases, the text file configuration mode was introduced to support the new 13-slot chassis and all the configurable options on the switch. With text file configuration mode, you can store the configuration as a text file in Flash memory or NVRAM. In text

file configuration mode, the binary NVRAM data structures are deleted from NVRAM. The only blocks not deleted from NVRAM are those that contain information not stored in the configuration file. These blocks include the following:

- Boot block (B_BOOTAREA)—This block must stay in NVRAM. It contains information about the location of configuration blocks (NVRAM or DRAM).
- Option block (B_OPTION)—Contains the configuration for hidden commands.
- Module logging block (B_MODULELOG)—Contains the NVRAM log traces (NVLOG).
- Command logging block (B_CMDLOG)—Contains the command history log.
- RSAKEY (B_RSAKEY)—Contains encrypted key information that should not be regenerated every time.
- I/F index block (B_MODULEIFINDEX)—Contains SNMP interface index information that is not in the text configuration file.
- RMON blocks (B_RMON, B_RMON2, and B_EXTENDED_RMON)—Contains RMON information that is not in the text configuration file.
- SNMP block (B_SNMP)—Contains SNMP-related information that is not in the text configuration file. Additionally, fields in this block can be specified as non-volatile by the user through SNMP; those fields must be saved immediately to non-volatile storage.
- VTP blocks—Need to stay in NVRAM to be compliant with the VTP specification in VTP server mode.

The NVRAM blocks are copied to DRAM before being deleted. Except for some isolated code dealing with the copying of the NVRAM blocks into DRAM, this change is transparent to the rest of the software. The data structures are manipulated and accessed as before, the only difference being that they are now stored in the DRAM instead of the NVRAM memory region.

A new B_GENERAL NVRAM block is also created when operating in text configuration mode. This block contains any configuration from a deleted block that must still be saved in NVRAM. For example, there are time zone and encryption-related fields in the global block that must be stored in NVRAM. These fields are moved to the new B_GENERAL block whenever text configuration mode is selected. The B_GENERAL block is deleted when moving back to binary configuration mode.

When operating in text file configuration mode, most user settings are no longer saved immediately to NVRAM. Configuration changes instead are only written to DRAM. You must enter the **write memory** command to store the configuration in non-volatile storage. The non-volatile storage may be either the Flash file system or NVRAM. Because the text file configuration file in most cases requires less space than the binary data structures, NVRAM is a good place for the configuration file. Alternatively, you may specify a file in the Flash file system.



Note

When a new VLAN is added (created), the VTP domain information fields (such as VtpDomainName, VtpPassword, VtpMode, VtpInterval, VtpRevisionNo, VtpVlanCount, VtpUdpater, VtpDomainIndex, VtpPruningMode, and VtpV2Enabled) are updated if their values are different from the current values in NVRAM. Out of all of these information fields, the VtpVlanCount field is the only one that is changed when a VLAN is added or deleted. When the VtpVlanCount field is changed, the global block in NVRAM is changed resulting in the following trap being sent: “Global block changed by Console//.” This behavior is documented in caveat CSCea23160.

802.1X Authentication

This section contains usage guidelines, restrictions, and troubleshooting information that apply to 802.1X authentication:

- A problem is seen when Microsoft IAS is configured as the authentication server for 802.1X user authentication purposes. If the username does not exist in the active directory, the supplicant is not providing a popup window for entering the username and password. Instead, if the user enters the nonexistent username for the first time, the supplicant sends the stored username with every response for the request. This problem is not an issue with the switch or the authenticator. The problem is with the supplicant or active directory configuration that is used for creating the usernames in the domain.

Workaround: Create the username in the active directory so that the popup window for entering the username and password appears.

CiscoView

This section contains usage guidelines, restrictions, and troubleshooting information that apply to CiscoView:

- With software releases 8.3(x) and 8.4(x), the CiscoView image cannot be launched on HP-UX platforms. (CSCsa21515)
- With CiscoView, the Firewall Services Module, Content Services Module, and SSL Services Module features might not work consistently with Windows NT. When you try to launch CiscoView ADP on Windows NT, the progress dialog either runs for a long time and then stops or it might launch suddenly. This problem is occurring only with Windows NT with Internet Explorer and Netscape browsers. There is no problem with Windows 2000 or Solaris platforms.

Workaround: Because the problem is intermittent, the workaround is to close the dialog and try launching the application again. (CSCin41067)

- In rare occurrences, when trying to launch the CiscoView image with the FWSM, CSM, and SSL service module features, the progress dialog might occasionally hang. The frequency of the problem varies by platform as follows:
 - Windows NT, approximately 30 percent to 40 percent of the time
 - Windows 2000, approximately 2 percent to 5 percent of the time
 - Solaris, approximately 2 percent to 5 percent of the time

Workaround: Close the progress dialog and try launching again. (CSCin42718)

- In rare occurrences with CiscoView, you might experience the following two problems:

Case 1: Clicking the “Cancel” button causes an exception when you perform this procedure: When you launch any FWSM, CSM, or SSL dialog, such as “FWSM - Assign Vlans to Firewall blade,” the progress dialog bar displays. Then, if you click the cancel button, the “Aborting the operation. Please wait” message displays. After a period of time, the “Failed to retrieve category: Assign VLANs to Firewall Blade.java.lang.NullPointerException” window displays. If you close this window, the “Aborting the operation, please wait” main window closes. Although this problem occurs intermittently, the cancel operation for the VLAN flows dialogs works correctly.

Workaround: Close the exception and try to launch the dialog again.

Case 2: Close the progress dialog bar by clicking the asterisk (*) button (this is not applicable for Solaris platforms) then launch any dialog such as “FWSM - Assign Vlan to blade.” The progress bar appears, now close the progress bar by clicking the “X” button. This results in a “CiscoView Error” message and the application might hang.

Workaround: Close the session and try launching it again. Instead of using the “X” button to close the progress bar, use the cancel button. (CSCin43633)

- CiscoView device discovery fails when Supervisor Engine 1 in slot 1 is in ROMMON mode and Supervisor Engine 2 in slot 2 is active. This problem is resolved in software release 8.1(2). (CSCin43526)
- The 7.1(1) and 7.1(2) CiscoView + SSH images may fail to boot on Supervisor Engine 1 systems with 64-MB DRAM. This problem applies to all models of Supervisor Engine 1 (WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE, WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2). Due to this problem, the cat6000-supcvk9.7-1-1.bin and cat6000-supcvk9.7-1-2.bin CCO images have been deferred. As an alternative, the cat6000-supcvk8.7-1-1.bin or the cat6000-supcvk8.7-1-2.bin images may be used if SSH support is not required. If both CiscoView and SSH support is required, the 6.3(x) supcvk9 images or the 7.2(x) and later supcvk9 images should be used. This issue is documented in open caveat CSCdw70549.
- The supported client platforms, browsers, and Java Plug-in versions supported by CiscoView are as follows:

Client Platform	Web Browser	Java Plug-in
Solaris 2.7/2.8	Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)
Windows 98 Windows NT 4.0 Windows 2000	Internet Explorer 5.5 Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0-C (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)
HPUX 11.0	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.2.2 (JRE 1.2.2) Java Plug-in 1.3.1 (JRE 1.3.1)
AIX 4.3.3	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)



Note The Java Plug-in can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin>



Note Java Plug-in versions 1.3.0_01 and 1.3.0_02 do not work with CiscoView.



Note Java Plug-in versions 1.3.1_01 and later are not supported by CiscoView.

- If the CiscoView chassis scrollbar does not appear, resize the browser window. Another workaround is to right-click on the chassis and select “Resize” to decrease the size of the chassis view.

On Windows NT machines with Java Plug-in 1.3.0 installed and Netscape running, the CiscoView chassis scrollbar does not appear, even after resizing it. To correct the problem, upgrade to Java Plug-in 1.3.1. (CSCdw58407)

- On Solaris machines with Java Plug-in 1.3.1 installed, if you are running either Netscape Navigator 4.77, 4.78, or 4.79, you might see a blank screen after launching CiscoView. (CSCdw13384)

To correct the problem, perform these steps:

-
- Step 1** Uninstall the current Java Plug-in from your machine.
- Step 2** Download the Java Plug-in from the following location and install it on your machine:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin>
- Step 3** Clear the cache by entering the following CLI command: **rm -rf ~/.netscape**
- Step 4** Enter the following CLI command: **export NPX_PLUGIN_PATH = /usr/j2se/jre/plugin/sparc/ns4**
- Step 5** Launch Netscape Navigator.
- Step 6** Select **Edit > Preferences**, and then click **Advanced** in the navigation tree.
- Step 7** Make sure the **Enable Java** checkbox is *not* selected.
- Step 8** Specify the IP address of the device you want to access and launch CiscoView. The Java console is displayed, but the chassis view does not appear.
- Step 9** Select **Edit > Preferences**, and then click **Advanced** in the navigation tree.
- Step 10** Select the “Enable Java” checkbox.
- Step 11** Specify the IP address of the device you want to access and launch CiscoView. Both the Java console and chassis view should now be displayed.
- If you are running Netscape and have a Java Plug-in earlier than version 1.3.0 installed, you might get a blank screen when you launch CiscoView. (CSCdw59601)
 To correct the problem, download Java Plug-in 1.3.0 or later from the following location:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin>
 - If your machine is running Windows 2000, Windows NT, or Windows 98 and the chassis view does not appear, you should disable the Java Plug-in’s JAR caching feature, as follows:
 - For Java Plug-in 1.3.1:
 - 1) Select **Start > Settings > Control Panel > Java Plug-in 1.3.1**.
 - 2) Click the **Cache** tab.
 - 3) Click **Clear JAR Cache**.
 - For Java Plug-in 1.3.0:
 - 1) Select **Start > Settings > Control Panel > Java Plug-in**.
 - 2) Click the **Basic** tab.
 - 3) Make sure the “Cache JARs In Memory” checkbox is not selected.
 - 4) Click **Apply**.
 - If your machine runs on the HP-UX platform, we recommend that you use the HP release of Netscape. The HP release of Netscape can be downloaded from the following location:
<http://www.hp.com/workstations/products/unix/software/netscape/index.html>
 (CSCdw59617)
 - CiscoView images take approximately 12 minutes to download from a TFTP server to a Flash PC card. (CSCdr14437)

- In the VLAN & Bridge dialog box (**Device > Configure > VLAN & Bridge**), deleting the primary VLAN after unbinding the secondary VLAN returns an error message.

Workaround: Close and reopen the dialog box and then delete the primary VLAN.

After binding a secondary VLAN to the primary VLAN, delete the primary VLAN and the following error message is displayed: “Set failed due to snmpRspGenErr for vtpVlanEditRowStatus.1.199.”

Workaround: Close and then reopen the dialog box. You should now see the correct error message: “The Primary is bounded ...” (CSCdt65530)

- The Carrier Alarm LED status on WAN modules is not supported by SNMP. (CSCdw50111)
- CWDM GBICs and 1000BASE-TX (copper) GBICs installed in WAN modules display as normal GBIC ports in CiscoView. (CSCdy18652)
- If you have configured Internet Explorer to bypass certain addresses in the proxy server (such as the IP address of the switch), the Java applet on the PC will still try to connect to the switch through the proxy server. For security reasons, this may cause the CiscoView GUI to fail if the proxy server cannot talk to the switch directly. (CSCdw48852)
- In the Ether Channel dialog box (**Port > Configure > Ether Channel**), when Ether Channel Operation Mode is changed from “pagpOn” to “off/manual,” click **Refresh** and the PAGP dialog box displays “N/A” for every field. To work around the problem, close and reopen the dialog box. (CSCdw76309)
- If you use QoS Device Management to create a policy name and try to delete the policy name, the following incorrect error message appears:

Unable to set row status

(CSCdu11333)

- If you use QoS Device Management to add an IP ACL, select the **Add/Edit ACE** option, select an entry and make some changes, and then either click **Cancel** or **OK**. The configuration fails due to misconfigurations when you select **OK**; the previously entered values will appear as defaults when you attempt to edit your configuration.

Workaround: Overwrite the values in the fields if necessary.

(CSCdu05678 and CSCdu15066)

- If you use QoS Device Management to add or edit an IP/IPX/MAC ACL, no buttons are available to move ACE entries up and down.

Workaround: Select the entry that needs to be moved and click on **Edit** and select **OK**. This entry is then moved to the bottom of the ACE list. (CSCdt64023)

- If you use QoS Device Management and select **Policy Selection, Add/Edit Policies > Change**, and then select a policy and click **OK**, selecting **Cancel** when the confirmation window displays will not cancel the operation. The policy is still added to the Policy Selection.

Workaround: Delete the policy selection entry that was added. (CSCdu43690)

- The Catalyst 6000 CiscoView (CV) images do not support the Carrier Alarm LED for WAN modules. (CSCdt52011)
- There is a problem when you highlight the MultiChannel DS3 Port Adapter in the WS-X6182-PA module, and then select **Configure > Interface**. The dialog box displays “n/a” or the incorrect values in every field. Also, if you select **Monitor > Interface**, the charts in the resulting dialog box do not get updated, and an error message is displayed in the status bar. This problem is corrected in MSFC Cisco IOS Releases 12.1(13)E, E1, and E2. (CSCdr39591)
- Disabled WAN modules are placed in the power-down state. This problem is resolved in software release 7.2(2). (CSCdw50083)

- 802.1X Authentication timer fields are available in the port-level PAE dialog box (**Port > Config > PAE > Port Authenticator**). This problem is resolved in software release 7.3(1). (CSCdw86044)
- The Redetect Protocol function in the MST Port Status dialog box (**Port > Configure > Spanning Tree > MST Port Status**) does not work on voice ports. This problem is resolved in software release 7.3(1). (CSCdx04800)
- When a device is set to MST Spanning Tree mode, the “Path Cost” and “Priority” fields in the Bridge Details dialog box (**Port > Configure > Bridge > Bridge Details**) cannot be set on a channeling port that is using PAGP or LACP. This problem is resolved in software release 7.3(1). (CSCdx23200 and CSCdx23217)
- With CiscoView, the SVI configuration dialog is still shown under “Device ->Configure->VLAN&Bridge” for the Firewall Services Module, Content Services Module, and SSL Services Module when a Supervisor Engine 1 module is installed. Since these modules require a Supervisor Engine 2, the dialog should not be displayed. (CSCin43687)

Open and Resolved Caveats in Software Release 8.4(2a)

These sections describe open and resolved caveats in supervisor engine software release 8.4(2a):

- Open Caveats in Software Release 8.4(2a), page 74
- Resolved Caveats in Software Release 8.4(2a), page 76

Open Caveats in Software Release 8.4(2a)

This section describes open caveats in supervisor engine software release 8.4(2a):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.
Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online. (CSCed79483)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)

- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x) and 8.4(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.4(2a)

This section describes resolved caveats in supervisor engine software release 8.4(2a):

- In redundant systems running software release 8.4(2), the switch might crash after entering the **switch supervisor** command or during system bootup. This problem affects all supervisor engines when the switch is populated with multiple inline power switching modules that contain the WS-F6K-GE48-AF and WS-F6K-FE48-AF daughter cards.

Workaround: Reset the system or insert the inline power switching modules one by one. This problem is resolved in software release 8.4(2a). (CSCeh47719)

Open and Resolved Caveats in Software Release 8.4(2)

These sections describe open and resolved caveats in supervisor engine software release 8.4(2):

- Open Caveats in Software Release 8.4(2), page 76
- Resolved Caveats in Software Release 8.4(2), page 78

Open Caveats in Software Release 8.4(2)

This section describes open caveats in supervisor engine software release 8.4(2):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.

Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)

- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online. (CSCed79483)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)

- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x) and 8.4(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.4(2)

This section describes resolved caveats in supervisor engine software release 8.4(2):

- The T1, E1, and FXS voice modules may not come online in text configuration mode.
Workaround: Manually reset the module after the switch fully boots up. This problem is resolved in software release 8.4(2). (CSCed12999)
- The **show module** command displays the Supervisor Engine 720 firmware version (FW) as version 8.1.3; this version is inconsistent with the other FW versions—the version should be 8.1(3). This problem is resolved in software release 8.4(2). (CSCeg66140)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. This problem is resolved in software release 8.4(2). (CSCee44277)

- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. This problem is resolved in software release 8.4(2). (CSCee44285)

- If you have a configured startup file with the boot environment variable CONFIG_FILE set, the startup file might be read before the modules in the switch are completely online. As a result, the configuration for the modules specified in the startup file is lost. In some cases, the switch might still boot correctly if the diagnostic level is changed to a lower level. This problem is resolved in software release 8.4(2). (CSCec08789)
- In a two-port EtherChannel, when the second port is added to the EtherChannel, the first port leaves and then rejoins the EtherChannel (this leaving and rejoining process occurs twice).

Workaround: The problem does not occur if the EtherChannel mode is set to “on.” This problem is resolved in software release 8.4(2). (CSCee76807)

- With port security enabled on a port, if the port goes up and down during the programming of the secure MAC address, you will lose connectivity. This problem is resolved in software release 8.4(2). (CSCef06707)
- You might experience a problem with an SSH login. The login prompt appears and you enter your login name and get a password login prompt. After entering the password, there is no reply; you see a blank line and pressing Enter again does nothing. If you try to enter a command, there is no echo on the screen *but* the output from the command is displayed on the screen. This problem is not affecting the ability of the switch to function correctly. Once the problem happens, it is continuous. Logging off and back on does not clear the problem. You must reboot the switch to clear the problem. If you attempt an SSH login on an affected switch and it fails, you can immediately do an SSH login to an unaffected switch from the same session without a problem. This problem is resolved in software release 8.4(2). (CSCef54438)
- You might see a VTP pruning failure with spanning tree PortFast enabled. This problem is resolved in software release 8.4(2). (CSCef86022)
- The system passwords (both console and enable passwords) might not work after loading the passwords from a previously saved password configuration file. This problem is resolved in software release 8.4(2). (CSCeg05183)
- If a port in a Gigabit EtherChannel goes down, you might experience packet loss for 5 or 6 seconds. This problem is resolved in software release 8.4(2). (CSCeg28124)
- Out-Discard and Rcv-Octet counters increment on GBIC ports that are showing a “notconnect” status. This problem is resolved in software release 8.4(2). (CSCeg48512)
- With port security, when a port is shut down due to a security violation, the offending MAC address is not displayed in the syslog. This problem is resolved in software release 8.4(2). (CSCeg76020)
- Under certain conditions when using PAgP, the EtherChannel might go down resulting in traffic loss. This problem is resolved in software release 8.4(2). (CSCef32238)
- On a switch with a large number of ports, the switch might reset with a “Watchdog Timeout” exception after entering the **set cam notification {added | removed} enable** command on a range of ports that are part of an EtherChannel.

Workaround: Do not enter the command on a range of ports; enter the command on individual ports, one by one. This problem is resolved in software release 8.4(2). (CSCef42167)

- In rare circumstances, a group of four ports (1–4, 5–8, 9–12, or 13–16) on the WS-X6516-GE-TX module may experience connectivity problems. If this problem occurs, the following syslog messages might be seen:

```
%PM_SCP-SP-6-LCP_FW_ERR_INFORM: Module 4 is experiencing the following error:
Pinnacle #0 Frames with Bad Packet CRC Error (PI_CI_S_PKT_CRC_ERR - 0xC7) = 110
```

Workaround: Reset the module (hard reset). This problem is resolved in software release 8.4(2). (CSCef46923)

- When CoS output scheduling is set on an egress WS-X6548-GE-TX module port, the following is seen:
 - 64-byte long CoS 0 traffic is stored in WRR high Q or WRR low Q
 - 65-byte long CoS 0 traffic is stored only in WRR low Q

This problem is resolved in software release 8.4(2). (CSCef47548)

- ARP is not being resolved on the MSFC. The glean adjacency in the supervisor engine hardware is not being forwarded to the MSFC which prevents ARP from being resolved. This problem is seen only when **no ip redirect** and **no ip unreachable** are configured on the MSFC ingress VLAN interface.

Workaround: Configure at least one of the following on the MSFC ingress VLAN interface:

- **ip redirect**
- **ip verify unicast reverse-path**

This problem is resolved in software release 8.4(2). (CSCeg01772)

- An IEEE BPDU may be sent from an 802.1Q trunk port even if the native VLAN is cleared from the trunk. When the native VLAN on a trunk is cleared, the IEEE untagged BPDU should not be sent. If the trunk port reinitializes itself for any reason (such as disabling/enabling, module reset, and switch reset), the trunk port may start to send IEEE untagged BPDUs.

Workaround: Add the native VLAN and clear it again as follows:

- 1) **set trunk** *mod/port NativeVlan_ID*
- 2) **clear trunk** *mod/port NativeVlan_ID*

This problem is resolved in software release 8.4(2). (CSCeg29195)

- A dynamic port in the management VLAN does not pass traffic though the switch after its MAC address ages out. The dynamic port is assigned to the correct VLAN. If there is no traffic during the CAM aging time, the MAC address is removed from the table. After it has been removed, and traffic generated again, the MAC address does not appear in the table and traffic is not passed though the switch from that port.

Workaround: Use a dynamic VLAN that is different from the management VLAN or disable and enable the dynamic port. This problem is resolved in software release 8.4(2). (CSCeg30314)

- WS-X6548-GE-TX module ports that are hard coded to “100-full” speed might show “not-connected” after a reboot either due to a power cycling or upgrade where a reload is required.

Workaround: On the problem port, enter the **set port disable** command followed by the **set port enable** command. You might have to do this more than once. Sometimes rebooting the switch corrects the problem. This problem is resolved in software release 8.4(2). (CSCeg31700)

- After a supervisor engine switchover, if you add a VLAN to a trunk port, the VLAN is not displayed in the “Vlans in spanning tree forwarding state and not pruned” field of the **show trunk** command. This problem is resolved in software release 8.4(2). (CSCeg47658)
- Several different models of IP phones intermittently do not power up when attached to the WS-X6148-45AF module. This problem is seen when the power is set to “auto” and the speed is set to “full.” This problem is resolved in software release 8.4(2). (CSCeg55432)

- The switch may not be able to communicate with a connected device on a secure port in a different VLAN. This problem does not impact the other traffic of the connected devices.
Workaround: Disable port security on desired ports using the **set port security mod/port disable** command. This problem is resolved in software release 8.4(2). (CSCeg71622)
- With a Supervisor Engine 2, packets with an unresolved destination MAC address may be dropped instead of being forwarded to the MSFC for the triggering of ARP requests.
Workarounds: 1) Ping the destination from the supervisor engine or the MSFC. 2) Add a static ARP entry on the MSFC. This problem is resolved in software release 8.4(2). (CSCeg73090)
- If you use the **show trunk [mod[/port]] extended-range** command, the system might display all the ports without releasing the CPU for other processes. During this period, BPDU processing might stop. This problem is resolved in software release 8.4(2). (CSCeg73646)
- With certain topologies where 802.1X is being used and UplinkFast is enabled, you might experience a transient loop that could affect the passing of traffic on 802.1X-enabled ports.
Workaround: Disable UplinkFast. This problem is resolved in software release 8.4(2). (CSCeg75736)
- When a Supervisor Engine 2 has an EtherChannel configured in “desirable mode,” the EtherChannel might randomly unbundle due to PAgP corruption. This problem is seen only when voice ports on the WS-X6608 modules are going up and down.
Workaround: Configure the trunking and EtherChannel modes to “on.” We also recommend that you enable UDLD on all trunks in the EtherChannel on both switches. Doing this allows you to monitor and detect any unidirectional links that “desirable mode” EtherChannel would normally detect and recover from. This problem is resolved in software release 8.4(2). (CSCeg78848)
- With IGMP snooping enabled, the switch might fail to relay the DVMRP messages to the other DVMRP routers in that VLAN.
Workaround: Disable IGMP snooping. This problem is resolved in software release 8.4(2). (CSCin84014)
- With redundant supervisor engines, the status and configuration of port 1/1 and port 2/1 is changed after a switchover. The first supervisor engine port on the newly active supervisor engine gets enabled even if the default is set to disable. This problem is only seen in text configuration mode.
Workaround: Use binary configuration mode. This problem is resolved in software release 8.4(2). (CSCsa42331)
- The MIB object “snmpEngineTime” does not report the correct value if the SNMP engine has been active for more than 496 days. This problem is resolved in software release 8.4(2). (CSCeg61577)
- When a switch running IEEE standard MST is connected to a switch running pre-standard MST, the port on the pre-standard MST switch might occasionally come up as a boundary port even though both switches have the same MST configurations.
Workaround: Redetect the protocol on the port that comes up as the boundary port by entering the **set spantree mst mod/port redetect-protocol** command. This problem is resolved in software release 8.4(2). (CSCeg01881)
- For IDSM and NAM modules, the default behavior of the SPAN destination port was changed in software release 8.4(1). If the SPAN destination port is a trunk, the spanned source VLAN must be in the SPAN destination port’s “trunk allow list.” Note that this behavior is corrected in software release 8.4(2); in software release 8.4(2), the behavior is as it was in software releases prior to release 8.4(1).
Workaround: Specify the VLANs that you are interested in spanning on the IDSM or NAM module trunk port. This problem is resolved in software release 8.4(2). (CSCeh02836)

- With software release 8.4(2) and later releases, a new global CLI command has been introduced to control the use of ACL trust over port trust to mark packets. Prior to software release 8.4(2), there was no way to set DSCP with the **set qos acl** command set. With software release 8.4(2) and later releases, a new CLI command, **set qos acl default-action trust-override [enable | disable]**, is available to toggle the ACL trust to override the port trust. (CSCeh14320)
- You might see ports go into the “notconnect” state after disabling and then enabling the port status.
Workaround: If the port goes into the “notconnect” state after disabling and enabling the port status, you can attempt to get the port back to the “connected” state by entering the **set port negotiation mod/port enable** command followed by the **set port negotiation mod/port disable** command. This problem is resolved in software release 8.4(2). (CSCeh25262)
- With software release 8.4(2) and later releases, support for service modules (CSM, SSL, FWSM, VPN, and so on) has been enhanced as follows:
 - Service modules that pass traffic will now participate in spanning tree.
 - PortFast and TrunkFast are enabled on the service modules by default.
 - All STP parameters are configurable on these service modules.
 - BPDU guard and BPDU filter are set as “default” by default on the service modules and are user-configurable. (CSCed73352)

Open and Resolved Caveats in Software Release 8.4(1)

These sections describe open and resolved caveats in supervisor engine software release 8.4(1):

- Open Caveats in Software Release 8.4(1), page 82
- Resolved Caveats in Software Release 8.4(1), page 85

Open Caveats in Software Release 8.4(1)

This section describes open caveats in supervisor engine software release 8.4(1):

- For IDSM and NAM modules, the default behavior of the SPAN destination port has changed in software release 8.4(1). If the SPAN destination port is a trunk, the spanned source VLAN must be in the SPAN destination port’s “trunk allow list.” Note that this behavior will be corrected in software release 8.4(2); in software release 8.4(2), the behavior will be as it was in software releases prior to release 8.4(1).
Workaround: Specify the VLANs that you are interested in spanning on the IDSM or NAM module trunk port. (CSCeh02836)
- With software release 8.1(1) through software release 8.4(1), if the MSFC on the active supervisor engine is specified as the nondesignated router (NDR) and the MSFC on the standby supervisor engine is specified as the designated router (DR), the MSFC that is specified as the NDR does not take over when the standby supervisor engine is removed.
Workaround: Reset the supervisor engine. (CSCeg09491)
- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.

Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)

- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online. (CSCed79483)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.

Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)

- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- The **show module** command displays the Supervisor Engine 720 firmware version (FW) as version 8.1.3; this is inconsistent with the other FW versions - the version should be 8.1(3). (CSCeg66140)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)

- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x) and 8.4(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.4(1)

This section describes resolved caveats in supervisor engine software release 8.4(1):

- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. This problem is resolved in software release 8.4(1). (CSCee16301) (CSCee16301 was fixed in CSCee89331)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. This problem is resolved in software release 8.4(1). (CSCee02221)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. This problem is resolved in software release 8.4(1). (CSCed70239)
- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.
Workaround: Manually configure the FWSM each time that the system boots. This problem is resolved in software release 8.4(1). (CSCee10706)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)



Note This problem was seen in earlier software releases but is not seen in the 8.4(1) software release.

- With a Supervisor Engine 1, you might see some Layer 3 table parity errors. These are non-fatal errors (packets are still forwarded in software). This problem is resolved in software release 8.4(1). (CSCdy41174)
- With the WS-X6502-10GE module, the **set qos map** command maps CoS values to the WRED thresholds only and not to the tail-drop thresholds. This problem is resolved in software release 8.4(1). (CSCdy79506)
- A VACL filter might not have any effect on spanned traffic. If there is an RSPAN session where the source and destination are present on the same switch, applying a VACL filter to the RSPAN VLAN might not create a filter effect on the spanned traffic. This problem is resolved in software release 8.4(1). (CSCee74248)

- After a non-high availability failover, the non-designated MSFC might repeatedly reset. The system does not display a specific reason for the reset. The following syslog messages are displayed:

```
2004 May 28 23:18:21 %SYS-1-MOD_MINORFAIL:Minor problem in module 15
2004 May 28 23:18:21 %SYS-4-NVLOG:SYNDIAGS:Minor hardware problem in Module #15. Use
'show test 15' to see results of tests.
2004 May 28 23:18:23 %SYS-5-MOD_OK:Module 15 is online
2004 May 28 23:23:48 %SYS-5-MOD_RESET:Module 15 reset from Status Poll
```

Workaround: Reboot the chassis. This problem is resolved in software release 8.4(1). (CSCef24069)

- In software release 8.3(3) with the WS-X6704-10GE module, CoS-to-CoS mapping might not work properly. This problem is resolved in software release 8.4(1). (CSCef54500)
- With software release 8.3(3), the switch might perform a reverse DNS query before each new command in a Telnet or SSH session if DNS lookups are enabled.

Workaround: Disable DNS lookups by entering the **set ip dns disable** command. This problem is resolved in software release 8.4(1). (CSCef61776)

- If you configure a SPAN session on a module and then replace the module with a different type of module, the switch disables the SPAN session because a different type of module was inserted. This is normal behavior. The problem is that if you configure a new SPAN session on the newly installed module and then perform a high-availability switchover, the newly configured SPAN session is lost after the switchover.

Workaround: Reconfigure the SPAN session after the high-availability switchover. This problem is resolved in software release 8.4(1). (CSCef67073)

- With IGMP snooping enabled, PIM hellos might not be going out of the ATM LANE modules.

Workaround: Disable and then reenable IGMP snooping. This problem is resolved in software release 8.4(1). (CSCef81723)

- The **set snmp ifalias** command fails on FlexWAN interfaces. The FlexWAN module does not have any ifIndexes (“0” ports); therefore, you should not be allowed to set the SNMP ifalias on FlexWAN module interfaces. Additionally, the system should not display a FlexWAN module entry when the **show snmp ifalias** command is entered. This problem is resolved in software release 8.4(1). (CSCef82995)

- The **show tech** command should not display password information as this could create a security vulnerability. This problem is resolved in software release 8.4(1). (CSCef86581)
- For a Supervisor Engine 2/MSFC2 with more than 255 VLANs assigned to the same HSRP group ID, the HSRP MAC address may be deleted mistakenly, resulting in Layer 3 packets being forwarded to the MSFC2 for software switching.

Workaround: Limit the number of VLANs with the same HSRP group ID to no more than 255. If necessary, use other HSRP group IDs. This problem is resolved in software release 8.4(1). (CSCef88220)

- When port security is configured with the violation mode set to **restrict**, traffic from insecure addresses is dropped. This behavior is achieved by installing a special “trap” CAM entry in the CAM table. While this special CAM entry is suppressed in the **show cam dynamic** command output, the insecure address is still registered in the CAM notification history and is shown in the **show cam notification history** command output. Functionality is not affected. This problem is resolved in software release 8.4(1). (CSCef98123)

- With software releases 8.1(1) and later releases, the switch might drop tagged packets on the 802.1Q access port. A symptom of this problem is that while the **show cam dynamic** command does show the untagged users MAC address, the command does not show the other tagged VLAN users that are being tagged.

Workaround: Enter the following commands:

```
set port dot1qtunnel mod/port disable
```

```
set port dot1qtunnel mod/port access
```

This problem is resolved in software release 8.4(1). (CSCeg04084)

- When you poll the cpsSecureMacAddrType MIB object, it does not return anything. In software release 8.3(3), the cpsSecureMacAddrType MIB object was deprecated and the replacement was the cpsIfVlanSecureMacAddrType MIB object. The problem is that the cpsIfVlanSecureMacAddrType MIB object output is not the same as the output from the **show port security** command. This problem is resolved in software release 8.4(1). (CSCeg07733)
- With software release 8.3(3) and SSH enabled, the switch might unexpectedly reset. This problem is resolved in software release 8.4(1). (CSCeg00623)
- With software release 8.3(3), when the inband interface is added to the ifTable, the MIB object ifNumber is not incremented. This problem results in the ifNumber being 1 less than the number of instances in the ifIndex. This problem is resolved in software release 8.4(1). (CSCeg26260)
- With VACLs in previous software releases, due to inconsistencies between the hardware configuration and the NVRAM configuration, you might have experienced the following problems when configuring VACLs:
 - ACL name commit failure
 - ACL name commit ok, ACEs commit failure
 - ACL mapping failure

These problems have been resolved by ensuring that the hardware configuration and the NVRAM configuration are consistent. This problem is resolved in software release 8.4(1). (CSCee69181)

Open and Resolved Caveats in Software Release 8.3(7)

These sections describe open and resolved caveats in supervisor engine software release 8.3(7):

- Open Caveats in Software Release 8.3(7), page 87
- Resolved Caveats in Software Release 8.3(7), page 90

Open Caveats in Software Release 8.3(7)

This section describes open caveats in supervisor engine software release 8.3(7):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.

Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)

- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.
Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)
- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)

- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.

Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)

- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)

- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)

- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
 - A 64-byte packet should be counted as 4 but is counted as 3
 - 65- to 79-byte packets are correctly counted as 4
 - An 80-byte packet should be counted as 5 but is counted as 4
 - 81- to 95-byte packets are correctly counted as 5
 - A 96-byte packet should be counted as 6 but is counted as 5

(CSCdr56784)

- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(7)

This section describes resolved caveats in supervisor engine software release 8.3(7):

- In redundant systems running software release 8.3(6), the switch might crash after entering the **switch supervisor** command or during system bootup. This problem affects all supervisor engines supported in software release 8.3(x) when the switch is populated with multiple inline power switching modules that contain the WS-F6K-GE48-AF and WS-F6K-FE48-AF daughter cards.

Workaround: Reset the system or insert the inline power switching modules one by one. This problem is resolved in software release 8.3(7). (CSCeh47719)

Open and Resolved Caveats in Software Release 8.3(6)

These sections describe open and resolved caveats in supervisor engine software release 8.3(6):

- Open Caveats in Software Release 8.3(6), page 91
- Resolved Caveats in Software Release 8.3(6), page 93

Open Caveats in Software Release 8.3(6)

This section describes open caveats in supervisor engine software release 8.3(6):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.
Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)
- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.
Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)
- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)

- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)
- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.

Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)
- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)
- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a

high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)

- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:

- A 64-byte packet should be counted as 4 but is counted as 3
- 65- to 79-byte packets are correctly counted as 4
- An 80-byte packet should be counted as 5 but is counted as 4
- 81- to 95-byte packets are correctly counted as 5
- A 96-byte packet should be counted as 6 but is counted as 5

(CSCdr56784)

- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(6)

This section describes resolved caveats in supervisor engine software release 8.3(6):

- In software release 8.3(6), the number of TCP-established sessions has been increased from the current limit of 64 to 128. (CSCeg85630)

Open and Resolved Caveats in Software Release 8.3(5)

These sections describe open and resolved caveats in supervisor engine software release 8.3(5):

- Open Caveats in Software Release 8.3(5), page 94
- Resolved Caveats in Software Release 8.3(5), page 97

Open Caveats in Software Release 8.3(5)

This section describes open caveats in supervisor engine software release 8.3(5):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.

Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)

- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.

Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)

- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.

Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)

- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)

- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)

- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
 - A 64-byte packet should be counted as 4 but is counted as 3
 - 65- to 79-byte packets are correctly counted as 4
 - An 80-byte packet should be counted as 5 but is counted as 4
 - 81- to 95-byte packets are correctly counted as 5
 - A 96-byte packet should be counted as 6 but is counted as 5
 (CSCdr56784)

- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(5)

This section describes resolved caveats in supervisor engine software release 8.3(5):

- With software release 8.3(3), the switch might perform a reverse DNS query before each new command in a Telnet or SSH session if DNS lookups are enabled.

Workaround: Disable DNS lookups by entering the **set ip dns disable** command. This problem is resolved in software release 8.3(5). (CSCef61776)

Open and Resolved Caveats in Software Release 8.3(4)

These sections describe open and resolved caveats in supervisor engine software release 8.3(4):

- Open Caveats in Software Release 8.3(4), page 97
- Resolved Caveats in Software Release 8.3(4), page 100

Open Caveats in Software Release 8.3(4)

This section describes open caveats in supervisor engine software release 8.3(4):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.

Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)

- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)

- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.

Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)

- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.

Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)

- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)

- The **set mls bridged-flow-statistics enable** *vlanlist* command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)

- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch, and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. The Rapid-PVST+ switches should connect directly to the MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(4)

This section describes resolved caveats in supervisor engine software release 8.3(4):

- In text configuration mode, the SPAN sessions on the NAM, IDS module, and other service modules are not reconfigured after a reset.

Workaround: Manually configure the SPAN sessions on a service module each time that the switch is reset. This problem is resolved in software release 8.3(4). (CSCed65635)

- Disaster recovery cannot be done for CMM modules from the Catalyst operating system because the commands that are documented are not available to end users. Call TAC for further assistance if disaster recovery needs to be performed on a CMM. This problem is resolved in software release 8.3(4). (CSCee06730)
- A FWSM and possibly other service modules may not be able to communicate if the dot1q-all-tagged feature is enabled. You cannot use the dot1q-all-tagged feature if a service module is present in the switch.

Workaround: Enter the **set dot1q-all-tagged disable** command and then reset the switch. This problem is resolved in software release 8.3(4). (CSCed18049)

- When the EOBC out-of-band management bus fault detection code tries to power a module that is in the “power-deny” state, the switch may crash. This problem is resolved in software release 8.3(4). (CSCee59418)
- With a Supervisor Engine 2 or Supervisor Engine 720, traffic might be switched matching a policy map using the hardware CEF table instead of the next hop as set by the policy map. This problem has been observed only when you have a policy map with a large number of sequences and different next hops for each sequence. This problem is resolved in software release 8.3(4). (CSCef38462)
- With redundant supervisor engines/MSFCs, MSFCs configured in DRM with both MSFCs using an administered MAC address on the VLAN interface, and MSFCs configured with HSRP and OSPF, there is no problem as long as both supervisor engines remain in the same chassis. If you remove the standby supervisor engine and install it in another chassis with a link between the two switches, you lose unicast communication between the MSFCs, as evidenced by the following problems:
 - Cannot ping between the physical IP addresses
 - OSPF does not come up
 - Problems with HSRP

When you enter the **show cam system** command on the initial chassis, you can see that the MAC address configured on the removed MSFC still points to port 16/1. As soon as the administered MAC address is removed from the VLAN interfaces on the removed MSFC, communication returns. This problem is resolved in software release 8.3(4). (CSCed20984)

- If a port is moved from VLAN X to VLAN Y, permanent CAM entries might be lost. For example, if you have port group 1/1-8 with port 1/2 and port 1/7 in VLAN 10 and a permanent CAM entry configured on port 1/2, if port 1/7 is moved from VLAN 10 to VLAN 20, the permanent CAM entry on port 1/2 might be deleted.

Workaround: After moving a port to a different VLAN, reconfigure the permanent CAM entry. This problem is resolved in software release 8.3(4). (CSCef66696)

- With **cdpverify** enabled, the auxiliary VLAN might not come up on a Cisco IP conference station 7936 IP phone and the phone might not boot.

Workaround: Disable **cdpverify** on that port using the **set port auxiliaryvlan mod/port cdpverify disable** command. This problem is resolved in software release 8.3(4). (CSCef23681)

- Doing a minimal entry (entering only the first part of a command's syntax) on the following commands: **set errdisable**, **set option**, and **show cdp port mod/port**, results in either a missing key word or no error message. This problem is resolved in software release 8.3(4). (CSCed92864)
- The **show tech-support** command does not display "outband counters." This problem is resolved in software release 8.3(4). (CSCef81144)
- If you set the text configuration autosave interval to greater than 25 days or above 35000 minutes using the **set config mode text auto-save interval interval** command, you might see the following error message: "Failed to start text configuration auto-save timer."

Workaround: Do not set the autosave interval to greater than 25 days or above 35000 minutes. We have stopped supporting timers with intervals greater than 25 days or 35000 minutes in software release 7.6(10) and later releases, 8.3(4) and later releases, and 8.4(1) and later releases. Any commands configured with an interval greater than 35000 minutes (or 25 days) in the configuration file are automatically set to 35000 minutes (or 25 days) when the configuration file is loaded on the switch. The same behavior applies to the **set system info-log interval interval** command and all other commands that support an interval configuration. (CSCee17413)

- After upgrading from software release 8.2(1) to software release 8.3(3) in the text configuration mode, the system incorrectly allows you to enter the **write memory** command during the sync up; the system does not allow you to use other **set** commands during the sync up. This problem results in a configuration loss. This problem is resolved in software release 8.3(4). (CSCef36602)
- If you set the system information logging interval to greater than 25 days or above 35000 minutes using the **set system info-log interval interval** command, you might experience a Breakpoint Exception in the StartupConfig process.

Workaround: Do not set the system information logging interval to greater than 25 days or above 35000 minutes. This problem is resolved in software release 8.3(4). (CSCef36760)

- You might experience a TLB Exception when trying to write the system info-log to an FTP server. This problem is seen when the output of the system information logging feature is transferred using the FTP protocol and no FTP username or password has been configured.

Workaround: Set the FTP username and password before using the FTP protocol. This problem is resolved in software release 8.3(4). (CSCef56255)

- You might experience a TLB Exception when trying to write the system info-log to a TFTP server. This problem is seen when the **show top** commands are included in the system information logging feature. This problem is resolved in software release 8.3(4). (CSCef56408)
- You might experience a TLB Exception when a **show topn** command is configured in the system information logging feature and the system information logging feature is enabled from a TCLSH prompt.

Workaround: Do not enable the system information logging feature from a TCLSH prompt when a **show topn** command is included in the feature. This problem is resolved in software release 8.3(4). (CSCef69100)

- An 802.1X client might time out when attempting to authenticate to a Radius server when a primary and backup Radius server is configured and a Radius server failover occurs. The 802.1X configuration should be able to survive a Radius server failover. This problem is resolved in software release 8.3(4). (CSCef52229)
- The switch might drop all EtherChannels configured to "desirable" mode for approximately 10 minutes. Depending on the topology, connectivity may be affected for the entire period of the outage.

Workaround: Configure EtherChannels to "ON" mode using the **set port channel mod/port mode on** command. This problem is resolved in software release 8.3(4). (CSCef02710)

- After experiencing a fabric sync error (%SYS-3-FAB_SYNCERR), some modules might have problems receiving control traffic such as UDLD packets (there is no problem with transmitting traffic).

Workaround: Reset the switch. This problem is resolved in software release 8.3(4). (CSCef06375)

- In software release 8.3(4), to facilitate the troubleshooting of fabric-related problems, the FPOE mismatch count (error counter) has been added to the **show fabric channel counters** command. Additionally, a syslog has been added to indicate that this error counter is incrementing. (CSCef25518)
- A problem is seen after an IP address is changed on a workstation or server; the address change can happen statically or due to DHCP after a reboot. The problem is that a drop adjacency is created for the IP address with a /32 mask on the switch. It is possible to ping the workstation from the switch but pings from a directly connected redundant switch fail (if Layer 3 CEF is traversed).

Workaround: A ping from the MSFC in the same chassis as the switch with the drop adjacency clears the drop adjacency. This problem is resolved in software release 8.3(4). (CSCec23277)

- With redundant Supervisor Engine 2s/MSFC2s and dual router mode (DRM) enabled, resetting the designated MSFC2 might cause loss of connectivity to/from the MSFC2 when it boots up again. The newly designated MSFC2 is not affected. This problem is seen in the following software releases:
 - 1) If the MLS rate limiter is not enabled, the problem is seen in software releases 7.6(5) through 7.6(8).
 - 2) If the MLS rate limiter is enabled, the problem is seen in software releases up to 8.3(3) in the 8.x software train.

Workaround: There are two ways to restore connectivity to the affected MSFC2: 1) Disable the MLS rate limiter by entering the **set mls rate 0** command. Note that if the problem is seen in software releases 7.6(5) through 7.6(8), even if the MLS rate limiter is not enabled, entering the **set mls rate 0** command restores connectivity. 2) Reset the affected MSFC2. This problem is resolved in software release 8.3(4). (CSCef32204)

- A WS-C6509-NEB-A chassis with only one fan in the chassis reports the second FanStatus as “fail.” This problem is resolved in software release 8.3(4). (CSCef57840)
- A WS-C6513 chassis with fan tray version 1 allocates 126W to the fan tray but does not account for it in the output of the **show environment power** command. Fan tray version 1 should not have the 126W allocated to it. This problem is resolved in software release 8.3(4). (CSCef69633)
- If the switch is peering with a multicast router through an ATM interface (either LANE or RFC 1483 with PVC binding), you might experience high CPU utilization with the multicast receive process.

Workaround: Disable IGMP or enable the multicast rate-limit feature and set the rate to a value that alleviates the problem. This problem is resolved in software release 8.3(4). (CSCef27349)

- The sc1 interface might appear on the same VLAN as the sc0 interface after a software upgrade. This problem is related to upgrading from non-supported sc1 interface trains to sc1 supported trains. This problem is resolved in software release 8.3(4). (CSCef06801)
- The following syslog error message indicates an ASIC error with the WS-X6548-RJ-45 module and the recommended action is to replace the module:

```
SYS-6-SYS_LCPERR6:Module [dec]: Pentamak Ddr Sync Error
```

This message has a logging level of 6 but the severity of the error dictates that the logging level should be a 3. This problem is resolved in software release 8.3(4). (CSCef18763)

- LTL indexes for configured multicast CAM entries that point to an EtherChannel that is configured in desirable mode are lost when the EtherChannel link goes up and down.

Workarounds: 1) Clear the configured CAM table entry and reenter it. 2) Configure the EtherChannel to “ON” mode. This problem is resolved in software release 8.3(4). (CSCef51905)

- If the system banner size is over approximately 3072 characters, the switch might crash when you enter the **show banner** command through a Telnet session. This problem is resolved in software release 8.3(4). (CSCef44617)
- With MISTP enabled and the EtherChannel mode set to “ON,” if you configure more than one EtherChannel and trunk in a short period of time, all of the newly configured channels might not join the trunk. With this configuration scenario, the problem has also been seen after the switch is reset. This problem is resolved in software release 8.3(4). (CSCee95922)
- When a switch running standard MST (software releases 8.3[1] and later) is connected to a switch running pre-standard MST (software releases prior to 8.3[1]), MST might not converge in some instances other than IST.

Workaround: Run either standard MST or pre-standard MST on both switches. This problem is resolved in software release 8.3(4). (CSCef69689)

- With PAGP, it might take an unusually long time for a trunk port to join an EtherChannel. This problem is resolved in software release 8.3(4). (CSCee95479)
- The portSecuritySecureSrcAdd field, defined in the CISCO-STACK-MIB, incorrectly displays 00 00 00 00 00 00 when you enable port security, and the MAC address is learned from the port, instead of being configured manually. The portSecuritySecureSrcAdd field displays the correct information for the configured MAC addresses.

Workaround: Configure the secured MAC address manually using the **set port security mod/port enable mac_addr** command. This problem is resolved in software release 8.3(4). (CSCee56936)

- Enabling and disabling the SPAN feature might generate control characters in your Telnet window during an open Telnet session to the switch. This problem is resolved in software release 8.3(4). (CSCeb62318)
- Gigabit fiber-based modules (and under some conditions, copper-based modules) might experience high latency on ports when a SPAN destination session is configured on the same module. If a SPAN destination port goes up and down, there is the possibility that ports that are connected to the same port ASIC might experience latency (or possibly total lockup) in the receive direction. The latency, if present, is noticeable when low amounts of traffic are being sent through the system and/or if the received packet size on ports adjacent to the SPAN port are small or of average size.

For complete details on this problem and a list of affected modules, refer to the online bug toolkit release notes at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

This problem is resolved in software release 8.3(4). (CSCef39614)

- Spanning tree status information for MST instance 1 might disappear from the **show spantree mod/port** display after a high-availability switchover. Connectivity is not affected.

Workaround: Disable high availability. This problem is resolved in software release 8.3(4). (CSCee34858)

- A switch running rapid spanning tree (the switch is not the root bridge), may log the following events in the syslog if it received a corrupt BPDU:

```
2001 Apr 07 23:40:16 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:28 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
```

```

2001 Apr 07 23:40:28 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:42 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:40:42 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:40:59 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:40:59 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1
2001 Apr 07 23:41:13 %SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 4/2 in
MST instance 1. Moved to loop-inconsistent state
2001 Apr 07 23:41:13 %SPANTREE-2-LOOPGUARDUNBLOCK: Port 4/2 restored in MST instance 1

```

These symptoms are usually seen when there is more than one MST instance configured. This problem is resolved in software release 8.3(4). (CSCee77039)

- With Rapid PVST+ enabled, a port might get stuck in the listening state after STP is enabled on a given VLAN.

Workaround: Disable and then reenablen the affected port. This problem is resolved in software release 8.3(4). (CSCef28337)

- CMM ports might come up disabled and cannot be enabled. This problem usually occurs in text configuration mode with the default port status “disabled.”

Workaround: Enter the **set default portstatus enable** command, the **set config mode binary** command, and then reset the CMM module. This problem is resolved in software release 8.3(4). (CSCee63050)

- After a switchover, the first module/link trap for any module/link might not be sent. This problem is resolved in software release 8.3(4). (CSCef27093)
- The switch does not respond properly when the logout timer is set to 3 (**set logout 3**) if you are accessing the switch through a Telnet session and the screen is either holding the display at the “More” prompt, the “Enter Password” prompt, or the “Username” prompt. The logout timer is ignored during these conditions, allowing the connection to remain open beyond the configured logout timer setting. This problem is resolved in software release 8.3(4). (CSCef15158)
- In rare circumstances, a switch running the K9 software image may crash when an SSH client tries to connect. The problem might be seen when establishing the SSH connection to the client.

Workaround: Use Telnet or SSH version 1. This problem is resolved in software release 8.3(4). (CSCef42764)

- The **help** command for **set trunk all** shows the wrong descriptions for available commands. This problem is resolved in software release 8.3(4). (CSCef61890)
- VTP configuration details can be lost from the configuration when switching from binary to text configuration mode. The details are restored when switching back.

Workaround: Switch to binary mode to store configurations. This problem is resolved in software release 8.3(4). (CSCef64385)

- In rare circumstances, when versioning up or down to a different software release, the switch does not boot with the software that is configured to boot.

Workarounds: 1) Verify the bootstring and reset the system one more time. 2) After the reset, if the switch is booting with the wrong image, break the autoboot process and enter into the ROMMON mode by sending a Break. From ROMMON, execute the **boot** command to boot the switch with the correct image. This problem is resolved in software release 8.3(4). (CSCef43494)

- The switch displays the following syslog message when the system is under a Denial of Service attack:

```
TCP-2-TCP_MAXESTABLISHED:Possible TCP ACK attack. . Maximum established connection
limit 64 reached. Will drop unused connection
```

However, under some circumstances, the syslog might be generated when the system is not under attack. The system functionality is not affected. This problem is resolved in software release 8.3(4). (CSCef77162)

- The dot1dStpPortDesignatedPort MIB might return the wrong value as compared to the **show spantree statistics mod/port** command output. This problem is resolved in software release 8.3(4). (CSCef79667)

Open and Resolved Caveats in Software Release 8.3(3)

These sections describe open and resolved caveats in supervisor engine software release 8.3(3):

- Open Caveats in Software Release 8.3(3), page 105
- Resolved Caveats in Software Release 8.3(3), page 108

Open Caveats in Software Release 8.3(3)

This section describes open caveats in supervisor engine software release 8.3(3):

- With a PFC3, when you have an EtherChannel with ports spread across fabric-enabled modules *and* non-fabric-enabled modules, you might see a traffic drop when traffic enters the EtherChannel on the fabric-enabled module and goes out of the same EtherChannel through the non-fabric-enabled module.
Workaround: Do not configure ports in the EtherChannel across fabric-enabled modules and non-fabric-enabled modules. (CSCef10952)
- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)

- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TI_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.

Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)

- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- In text configuration mode, the SPAN sessions on the NAM, IDS module, and other service modules are not reconfigured after a reset.

Workaround: Manually configure the SPAN sessions on a service module each time that the switch is reset. (CSCed65635)

- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- Disaster recovery cannot be done for CMM modules from the Catalyst operating system because the commands that are documented are not available to end users. Call TAC for further assistance if disaster recovery needs to be performed on a CMM. (CSCee06730)

- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- A FWSM and possibly other service modules may not be able to communicate if the dot1q-all-tagged feature is enabled. You cannot use the dot1q-all-tagged feature if a service module is present in the switch.

Workaround: Enter the **set dot1q-all-tagged disable** command and then reset the switch. (CSCed18049)

- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem occurs only in text configuration mode.

Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)

- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)

- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.

Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)

- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)

- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. Rapid-PVST+ switches should connect directly to MST switches (we recommended this topology). (CSCee02592)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(3)

This section describes resolved caveats in supervisor engine software release 8.3(3):

- There is an inconsistency between the default signaling DSCP value used by the switch and the Cisco CallManager. Cisco CallManager release 4.x uses DSCP 24 by default for IP phone and Cisco Softphone signaling. However, automatic QoS on the switch uses DSCP 26. This situation can cause the IP phone packets to egress the switch with an incorrect DSCP value and the Softphone/Communicator packets not getting the appropriate QoS value. This problem is resolved in software release 8.3(3). (CSCee61555)
- Module boot ROM upgrades fail to download to modules supporting the rapid boot feature. As a result, the rapid boot feature is not supported in software release 8.3(1) or software release 8.3(2). This problem is resolved in software release 8.3(3). (CSCee44205)
- If you enter the **show port** command on a switch with voice modules (such as WS-X6624-FXS and WS-X6608-T1), the **show port** command appears to hang and port information for the voice module is not printed. Sometimes the DSP on the voice module may also reset. We recommend that you do not run the **show port** or **show port status** commands on switches with FXS or T1/E1 ports. This problem is resolved in software release 8.3(3). (CSCed91778, CSCec01126)
- If a service module such as a FWSM or a NAM is configured to boot from a nondefault partition with the supervisor engine in text configuration mode, the service module may fail to come online. In text configuration mode, the boot strings for service modules are not saved correctly at bootup.

Workaround: Manually set the boot string and reset the service module each time that the system is reset. Alternately, you can configure service modules to boot from their default partition. This problem is resolved in software release 8.3(3). (CSCed11214)

- If a multicast entry is configured through the CLI by entering the **set cam** command, it does not get synchronized to the standby supervisor engine in the following cases:
 - When the standby supervisor engine is reloaded after configuring the entry.
 - When high availability is disabled and then reenabled after configuring the entry.

Whenever high availability global synchronization is involved in the presence of the entry, it is not synchronized to the standby supervisor engine. When a switchover occurs, the new active supervisor engine is not aware of the multicast entry and it does not show the entry in the **show cam** command output.

Workaround: Ensure that high availability is enabled and “ON” by entering the **show system highavailability** command before creating any multicast entries using the **set cam** command. This problem is resolved in software release 8.3(3). (CSCee27955)

- In text configuration mode, the auto-mdix disable feature fails to work correctly on some modules. If you enter the **set port auto-mdix m/p disable** command and then reset the switch, the feature will be enabled after the switch comes back online. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time that the system boots. This problem is resolved in software release 8.3(3). (CSCed64515)

- In Rapid-PVST+ mode, the STP runtime timers hello, max_age, and fwd_delay are not set correctly after a high-availability switchover. This problem exists in software releases 8.1(x), 8.2(x), and 7.6(x).

Workaround: Reset the supervisor engine to get newer values. This problem is resolved in software release 8.3(3). (CSCee41527)

- With Supervisor Engine 1A, all copy tasks such as downloads, copying between devices (Flash and PCMCIA), and redundant boot image synchronizations are extremely slow and take approximately 25 minutes for a 10-MB file. This problem is resolved in software release 8.3(3). (CSCee24444)
- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. This problem is resolved in software release 8.3(3). (CSCds12349)
- The switch might reset (%SYS-5-MOD_NOSCPPINGRESPONSE) when getting CBL information through a PERL script. This problem is resolved in software release 8.3(3). (CSCee62021)
- After running the Pseudo-Random Bit Sequence (PRBS) test on the WS-X6704-10GE module (starting and stopping the PRBS test), the module port does not come up.

Workaround: Reset the module. The PRBS test is not supported on this module. The software has been modified to reject the PRBS command if it is run on an unsupported module. This problem is resolved in software release 8.3(3). (CSCee86424)

- The IP phone traffic received on an untrusted port should match the configured QoS ACL but the DSCP that is based on the ACL is not rewritten. This problem is due to the wrong mask being used in the QoS ACL. The CLI asks for the IP mask but it should ask for a wildcard. The problem is resolved by making the CLI consistent with the Cisco IOS CLI:
 - Catalyst operating system CLI:

```
Console> (enable) set qos acl ip ipacl1 dscp 32 ip 10.1.3.0 ?
<ip_addr>                Source IP Mask
Console> (enable)
```

– Cisco IOS CLI:

```
msfc2(config)# access-list 199 permit ip 10.1.3.0 ?
A.B.C.D Source wildcard bits
```

This problem is resolved in software release 8.3(3). (CSCec68825)

- The FWSM ports are not allowed to be configured as SPAN source ports. This problem is resolved in software release 8.3(3). (CSCed81400)
- Spanning tree does not block ports that are looped with a Balun cable. If a port is looped through a Balun cable or a loop-back adapter, spanning tree will initially block the port. If a topology change occurs, the port is put into forwarding state. This problem is resolved in software release 8.3(3). (CSCed84323)
- The EthChnlConfig process might cause high CPU utilization when trunk ports are added or deleted due to a link up/down condition or a reboot. This situation causes a loss of control packets, including VTP joins. This problem is resolved in software release 8.3(3). (CSCdu44453)
- A watchdog timeout might occur when you clear a large ACL (the problem was seen with an ACL that had 2000 ACEs). This problem is resolved in software release 8.3(3). (CSCee88608)
- Disabling or enabling port negotiation does not work correctly if you specify more than a single port or single range of ports. For example, if you enter **set port negotiation 3/1,3/5-6 disable**, ports 1 through 6 are disabled. This problem is resolved in software release 8.3(3). (CSCee52831)
- After upgrading Catalyst software to a version that supports the **set msfcautostate** command from a software version that did not support the command, **set msfcautostate disable** is automatically configured even though the default option for this command is enabled. This problem is resolved in software release 8.3(3). (CSCee62169)
- A UNIX script might get stuck at the Telnet prompt.
Workaround: Press **Enter** when the script gets stuck to start the script again. This problem is resolved in software release 8.3(3). (CSCeb69513)
- You might not be able to save your configuration to a 64-MB ATA Flash card if the filename starts with an upper case “N” and the length is more than eight characters. This problem is resolved in software release 8.3(3). (CSCee47457)
- The **set option** command set was inadvertently removed from software releases 7.6(7) and 8.3(1). The **set option** command set will be available again (engineering mode only) in software releases 7.6(8) and 8.3(3). (CSCee67932)
- The **show image-verification** command should not accept any additional input, but it does accept additional input and ignores it. The correct command response to any additional input for this command is to return a “Usage: Unrecognized command!” message. This problem is resolved in software release 8.3(3). (CSCee68770)
- You cannot use the **set security acl capture-ports mod/port** command for both NAM and IDS modules. You can only add either the NAM port or the IDS port with that command. This problem is resolved in software release 8.3(3). (CSCed83584)
- If you have an EtherChannel configured across modules, the EtherChannel configuration might change after you disable PortFast, BPDU filter, and BPDU guard and then reset the switch. This problem is resolved in software release 8.3(3). (CSCee67595)
- The supervisor engine might fail to power down the SFM after a synchronization error or hardware failure.

Workaround: Remove the defective SFM. This problem is resolved in software release 8.3(3). (CSCee34175)

- There is a vulnerability in the Transmission Control Protocol (TCP) specification (RFC793). All Cisco products that contain TCP stack are susceptible to this vulnerability. This advisory is available at these URLs:

- <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

This URL describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

- <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>

This URL describes this vulnerability for products that do not run Cisco IOS software.

This problem is resolved in software release 8.3(3). (CSCed32349)

- With the **ip verify unicast reverse-path** command configured on an MSFC interface, the interface fails to drop packets when there is a default route without a more specific route.

Workaround: Configure the MSFC interface using the **ip verify unicast source reachable-via rx** command. This problem is resolved in software release 8.3(3). (CSCec50151)

- Ping packets to the MSFC loopback interface are rate limited by the MLS CEF glean rate limiter.

Workarounds:

- 1) Disable the MLS CEF glean rate limiter as follows:

```
Router(config)# no mls rate-limit unicast cef glean
```

One side effect of this workaround is that packets hitting the glean adjacency (destined to an unresolved ARP host of a directly connected network) are not rate limited and are all sent to the MSFC for software processing. In general, the number of packets that are affected is small.

- 2) Set the glean rate limiter to a large number. This workaround retains the rate limiter, and is implemented as follows:

```
Router(config)# mls rate-limit unicast cef glean 10000 255
```

This problem is resolved in software release 8.3(3). (CSCee12132)

- With a Supervisor Engine 2/MSFC2 and port security enabled, the switch might display the following message: “Unable to add entry to earl on port 15/1, rc : -1.” If the MSFC2 in slot 2 is active, the switch might display the following message: “Unable to add entry to earl on port 16/1, rc : -1.” This problem is resolved in software release 8.3(3). (CSCeb86233)
- When upgrading from an earlier software release to release 8.3(x), the switch adds VLAN 1 for the static secure MAC address configuration. The switch should add the port native VLAN instead.

Workaround: Manually reconfigure the static secure MAC address. An example of the problem follows:

The following is the configuration in the earlier software release:

```
set vlan 2 9/48
set port security 9/48 00-e0-18-b4-eb-20
```

After upgrading to software release 8.3(x), VLAN 1 is automatically added to the port security configuration that blocks the original device as shown below:

```
set vlan 2 9/48
set port security 9/48 00-e0-18-b4-eb-20 1 (it should be “set port security 9/48 00-e0-18-b4-eb-20 2”)
```

This problem is resolved in software release 8.3(3). (CSCef01268)

- With a Supervisor Engine 1/MSFC, an input Cisco IOS ACL on the MSFC can cause Layer 2 traffic to be dropped in a VLAN. This problem is seen when no ip unreachable are configured and protocol filtering is enabled.

Workaround: Reset the switch to clear the problem. This problem is resolved in software release 8.3(3). (CSCee69960)

- An SNMP query for cvbStpForwardingMap might return an invalid port state. This problem is not resolved by a power cycle, module reset, disabling and enabling the port, or swapping modules. This problem is resolved in software release 8.3(3). (CSCee58481)
- If the default community strings are cleared, the community strings configured by entering the **set snmp community-ext** command do not work after resetting the switch. This problem is resolved in software release 8.3(3). (CSCee66094)
- In text configuration mode, with the switch configured to send a “cold start” trap when the switch is reloaded, the switch does not send the trap after a reload. This problem is not seen when the configuration mode is set to binary. This problem is resolved in software release 8.3(3). (CSCee81130)
- The value of dot1dStpPortDesignatedPort is not correct when queried from SNMP. This problem is resolved in software release 8.3(3). (CSCee94422)
- With a Supervisor Engine 2, when a redirect error interrupt occurs, the Supervisor Engine 2 might crash. The Supervisor Engine 2 should recover from the interrupt without crashing. This problem is resolved in software release 8.3(3). (CSCee57837)
- The traffic monitor feature is not supported on Supervisor Engine 720. That is, the **set traffic monitor ...** command has no effect. This problem is resolved in software release 8.3(3). (CSCee65262)
- With a Supervisor Engine 720 in a 6-slot chassis, fan detection/status might not be properly indicated. This problem is resolved in software release 8.3(3). (CSCee73822)
- The switch might crash while performing a high-availability task. This problem might happen if the VTP version is version 1 or version 2 and the VTP version was changed from version 3 to version 1 or version 2 in a redundant configuration while the standby supervisor engine was coming online. This problem is resolved in software release 8.3(3). (CSCee41005)
- After booting a switch with the auto-config option, the MST region configuration commit fails and the region configuration edit buffer locks with StartUpConfig. Subsequent commits fail too.

Workaround: Downgrade to the previous software release and set and commit the region configuration. This problem is resolved in software release 8.3(3). (CSCee84087)
- A Supervisor Engine 720 might crash when CiscoWorks 2000 LMS is enabled.

Workaround: Do not enable CiscoWorks 2000 LMS. This problem is resolved in software release 8.3(3). (CSCee73017)
- A large number of Watchdog timer interrupt crashes are due to ECC errors. In software release 8.3(3) and later releases, software has been enhanced to better deal with these ECC errors. (CSCed55259)
- You might lose the VLAN configuration when upgrading from a pre-8.3(1) software release to software release 8.3(1) or software release 8.3(2). This problem is only seen in text configuration mode. This problem is resolved in software release 8.3(3). (CSCef20392)

- To enable RSVP with a Supervisor Engine 720 running any 8.3(x) software release, you need to do the following:
 - 1) Disable IGMP snooping.
 - 2) Enable RSVP.
 - 3) Enable IGMP snooping.

If the above steps are not followed, RSVP does not work. With RSVP enabled following the above steps, the IP multicast addresses that map to MAC addresses 01-00-5e-00-00-10 and 01-00-5e-00-00-11 cannot be used. If used, there will be data outages for those groups.

The following symptoms are seen if RSVP is not enabled following the above steps: 1) RSVP does not receive any RSVP packets (no RSVP flows are created). 2) There are data outages to the IP multicast addresses that map to MAC addresses 01-00-5e-00-00-10 and 01-00-5e-00-00-11.

Workaround: For both RSVP and IGMP snooping to function correctly, disable RSVP, disable IGMP snooping, enable RSVP, and then enable IGMP snooping. Even with this workaround, IP multicast addresses that map to MAC addresses 01-00-5e-00-00-10 and 01-00-5e-00-00-11 cannot be used if RSVP is enabled. (CSCee49515)



Note If the intermediate switch for RSVP traffic is a Supervisor Engine 720 running any 8.3(x) software release, for RSVP to function correctly, you must either disable IGMP snooping or enable RSVP on all the transit switches for the RSVP traffic.

- In a redundant system, the standby supervisor engine might crash in syncTask while unpacking data for instance/VLAN 17 (not active) during change mode and the user has changed STP mode from MISTP to MST prior to the current change mode. (That is, the problem is visible in the second change mode.)

Workaround: Reset the standby supervisor engine. This problem is resolved in software release 8.3(3). (CSCef23135)
- After several spanning tree mode changes, you might receive “HADISABLED” syslogs indicating that high availability is being disabled due to a lack of system resources. This problem is resolved in software release 8.3(3). (CSCef25050)

Open and Resolved Caveats in Software Release 8.3(2)

These sections describe open and resolved caveats in supervisor engine software release 8.3(2):

- Open Caveats in Software Release 8.3(2), page 114
- Resolved Caveats in Software Release 8.3(2), page 117

Open Caveats in Software Release 8.3(2)

This section describes open caveats in supervisor engine software release 8.3(2):

- There is an inconsistency between the default signaling DSCP value used by the switch and the Cisco CallManager. Cisco CallManager release 4.x uses DSCP 24 by default for IP phone and Cisco Softphone signaling. However, automatic QoS on the switch uses DSCP 26. This results in IP phone packets egressing the switch with an incorrect DSCP value. This also results in Softphone/Communicator packets not getting the appropriate QoS value. (CSCee61555)
- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as “SP_TL_CFG.” As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes; they seem to be off by one from the specifications. (CSCed70239)
- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.
Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)
- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)

- In text configuration mode, the SPAN sessions on the NAM, IDS module, and other service modules are not reconfigured after a reset.

Workaround: Manually configure the SPAN sessions on a service module each time that the switch is reset. (CSCed65635)

- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- Disaster recovery cannot be done for CMM modules from the Catalyst operating system because the commands that are documented are not available to end users. Call TAC for further assistance if disaster recovery needs to be performed on a CMM. (CSCee06730)
- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)
- Module boot ROM upgrades fail to download to modules supporting the rapid boot feature. As a result, the rapid boot feature is not supported in software release 8.3(1). (CSCee44205)
- If you enter the **show port** command on a switch with voice modules (such as WS-X6624-FXS and WS-X6608-T1), the **show port** command appears to hang and port information for the voice module is not printed. Sometimes the DSP on the voice module may also reset. We recommend that you do not run the **show port** or **show port status** commands on switches with FXS or T1/E1 ports. (CSCed91778, CSCec01126)
- If a service module such as a FWSM or a NAM is configured to boot from a nondefault partition with the supervisor engine in text configuration mode, the service module may fail to come online. In text configuration mode, the boot strings for service modules are not saved correctly at bootup.

Workaround: Manually set the boot string and reset the service module each time that the system is reset. Alternately, you can configure service modules to boot from their default partition. (CSCed11214)

- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.

Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)

- A FWSM and possibly other service modules may not be able to communicate if the dot1q-all-tagged feature is enabled. You cannot use the dot1q-all-tagged feature if a service module is present in the switch.

Workaround: Enter the **set dot1q-all-tagged disable** command and then reset the switch. (CSCed18049)

- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem only happens in text configuration mode.
Workaround: Manually configure the FWSM each time that the system boots. (CSCee10706)
- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- In text configuration mode, the auto-mdix disable feature fails to work correctly on some modules. If you enter the **set port auto-mdix m/p disable** command and then reset the switch, the feature will be enabled after the switch comes back online. Binary configuration mode is not affected.
Workaround: Manually configure the feature each time that the system boots. (CSCed64515)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.
Workaround: Use the binary configuration mode or manually run the command each time that the system boots. (CSCee44285)
- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)
- If a multicast entry is configured through the CLI by entering the **set cam** command, it does not get synchronized to the standby supervisor engine in the following cases:
 - When the standby supervisor engine is reloaded after configuring the entry.
 - When high availability is disabled and then reenabled after configuring the entry.

Whenever high availability global synchronization is involved in the presence of the entry, it is not synchronized to the standby supervisor engine. When a switchover is done, the new active supervisor engine is not aware of the multicast entry and it does not show the entry in the **show cam** command output.
Workaround: Ensure that high availability is enabled and “ON” by entering the **show system highavailability** command before creating any multicast entries using the **set cam** command. (CSCee27955)
- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.
Workaround: Do not connect the leaf switches. Rapid-PVST+ switches should connect directly to MST switches (this is the recommended topology). (CSCee02592)
- In Rapid-PVST+ mode, the STP runtime timers hello, max_age, and fwd_delay are not set correctly after a high-availability switchover. This problem exists in software releases 8.1(x), 8.2(x), and 7.6(x).
Workaround: Reset the supervisor engine to get newer values. (CSCee41527)
- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)

- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.
Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)
- With Supervisor Engine 1A, all copy tasks such as downloads, copying between devices (Flash and PCMCIA), and redundant boot image synchronizations are extremely slow and take approximately 25 minutes for a 10-MB file. (CSCee24444)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(2)

This section describes resolved caveats in supervisor engine software release 8.3(2):

- In a redundant system, after a reset or switchover, you might not be able to view the error log on the standby supervisor engine. Entering the **show log** command results in an error message. This problem is seen only when Network Time Protocol (NTP) is configured.
Workaround: Reset the switch or perform a supervisor engine failover. This problem is resolved in software release 8.3(2). (CSCee54278)
- On a Supervisor Engine 2 with diagnostics set to complete, after a high-availability switchover the following NVLOG is printed on the console for the new standby supervisor engine:

```
2004 Apr 30 09:19:49 %SYS-4-NVLOG:SYNDIAGS:Module 2 detected Local Bus stall. Source:
B/P. Status Register = 0x0
```

This message is harmless and can be ignored (it will be removed in subsequent software releases). This problem is resolved in software release 8.3(2). (CSCin74096)

- WS-X6380-NAM ports do not come online. These ports stay errdisabled. Therefore, the WS-X6380-NAM module is not supported in software release 8.3(1) and software release 7.6(7). This problem is resolved in software release 8.3(2). (CSCee09474)
- The traffic monitor feature is not supported on the Supervisor Engine 720. Entering the **set traffic monitor threshold** command does not have any effect. This problem is resolved in software release 8.3(2). (CSCeb66075)
- Command logs are not updated properly after a software upgrade. This problem is seen only when the following conditions are satisfied: 1) The command log buffer in a pre-8.3 software release wrapped around. 2) The switch is upgraded from a pre-8.3 software release to software release 8.3.

Workaround: Because there are no commands to determine whether the command log buffer has wrapped around, the following workaround is suggested if you are upgrading to software release 8.3. From enable mode, perform the following: 1) Enter the **clear log command** command on the active supervisor engine before beginning the upgrade process. 2) Enter the **clear log command** command on the active supervisor engine immediately after the switch has booted software release 8.3. This problem is resolved in software release 8.3(2). (CSCee42423)

- After performing the following tasks, the standby supervisor engine does not transition to active after a high-availability switchover and both supervisor engines end up in standby mode:
 - Globally disable 802.1X on the switch.
 - Reboot the switch and globally enable 802.1X.
 - Allow at least one port to be “Authenticated” while enabling 802.1X. This could be the port that was “Authenticated” or this could be a port that was moved to a guest VLAN because the PC connected to the port was not 802.1X-capable.
 - Enable high availability.
 - Allow the synchronization to occur and then enter the **show system highavailability** command to verify if high availability is enabled.
 - Enter the **switch supervisor** command to switch over to the standby supervisor engine.

This problem is resolved in software release 8.3(2). (CSCee44569)

- When security and QoS ACLs are mapped together, modifying the security ACL might cause the QoS ACL to be removed from the TCAM. This problem is resolved in software release 8.3(2). (CSCee44654)
- IPX unicast packets may be dropped on the ingress MSFC interface when IP ACLs, VACLs, and no IP redirects are configured. The problem is seen on the Supervisor Engine 720 running software release 8.2(1) with Cisco IOS Release 12.2(17a)SX4 running on the MSFC. The problem only occurs when you have the following three configuration components: An IP ACL configured on a VLAN interface, “no ip redirects” configured on the MSFC, and a VACL configured for the corresponding VLAN on the switch side. The problem is seen once the interface comes up. Only broadcast IPX traffic actually reaches the MSFC. If either the access group is removed or IP redirects are enabled on the VLAN interface on the MSFC, the problem is cleared immediately, but if the configuration is added back and the interface is brought down and then back up by entering the **shutdown** command followed by the **no shutdown** command, the problem returns.

Workaround: Remove one of the three components that causes the problem. This problem is resolved in software release 8.3(2). (CSCee51617)

- When an EtherChannel port is disabled or enabled in MST mode, the LTL is cleared after convergence. The CBL reflects the correct port state.

Workaround: Disable and then reenable all ports of the channel. This problem is resolved in software release 8.3(2). (CSCee19795)

- During a RADIUS request, the switch sends a “NAS-Port” attribute with a length of 5 bytes. According to RFC 2138 and RFC 2865, this attribute should be 6 bytes. Sending 5 bytes triggers a reject on the RADIUS server side. This problem is resolved in software release 8.3(2). (CSCee55667)
- If VTP pruning is disabled, an EtherChannel trunk might show previously pruned VLANs as forwarding but port LTLs do not change to reflect that. As a result, unicast and broadcast traffic for those VLANs on the EtherChannel trunk may not be forwarded.
Workaround: Disable and then reenab the EtherChannel trunk. This problem is resolved in software release 8.3(2). (CSCed95274)
- With redundant Supervisor Engine 2s and high availability enabled, simulated system crashes result in problems with the core-dump and syslog-dump files. With the syslog-dump file, the following printf is displayed on the crashing supervisor engine’s console:

```
Syslog dump: InterruptStatus: 0x0
Opening syslog file bootflash:sysloginfo_040412-074129.
atexit: couldn't allocate exit hook
```


However, the file does seem to be created properly and can be dumped by entering the **show file** [device:]filename [dump] command. With the core-dump file, the same printf is displayed along with this message:

```
ȳeflateInit fail
```


In this case, a zero byte core-dump file is created. This problem is resolved in software release 8.3(2). (CSCee27511)
- The supervisor engine might repeatedly send FIB reload SCP messages. This problem is resolved in software release 8.3(2). (CSCee40322)
- With redundant Supervisor Engine 2s and high availability disabled, the switch can boot up normally. However, when a non-high-availability switchover is performed, the new standby supervisor engine fails to synchronize in local test mode. Several critical failures are then reported and the module fails the boot process and ends up with an error on the console. This problem does not happen when the number of VLAN mappings for a security ACL are reduced to approximately 250 VLANs. This problem is resolved in software release 8.3(2). (CSCee43443)
- After powering down a module, you might see switching bus sequence errors and an RxSBIF_SEQ_NUM_ERROR message. This problem is resolved in software release 8.3(2). (CSCee66999)

Open and Resolved Caveats in Software Release 8.3(1)

These sections describe open and resolved caveats in supervisor engine software release 8.3(1):

- Open Caveats in Software Release 8.3(1), page 120
- Resolved Caveats in Software Release 8.3(1), page 124

Open Caveats in Software Release 8.3(1)

This section describes open caveats in supervisor engine software release 8.3(1):

- On a Supervisor Engine 2 with diagnostics set to complete, after a high-availability switchover the following NVLOG is printed on the console for the new standby supervisor engine:

```
2004 Apr 30 09:19:49 %SYS-4-NVLOG:SYNDIAGS:Module 2 detected Local Bus stall. Source:
B/P. Status Register = 0x0
```

This message is harmless and can be ignored (it will be removed in subsequent software releases). (CSCin74096)

- With redundant Supervisor Engine 2s and high availability disabled, the switch can boot up normally. However, when a non-high-availability switchover is performed, the new standby supervisor engine fails to synchronize in local test mode. Several critical failures are then reported and the module fails the bring-up process and ends up with an error on the console. This problem does not happen when the number of VLAN mappings for a security ACL are reduced to approximately 250 VLANs. (CSCee43443)
- With redundant Supervisor Engine 2s and high availability enabled, simulated system crashes result in problems with the core-dump and syslog-dump files. With the syslog-dump file, the following printf is displayed on the crashing supervisor engine's console:

```
Syslog dump: InterruptStatus: 0x0
Opening syslog file bootflash:sysloginfo_040412-074129.
atexit: couldn't allocate exit hook
```

However, the file does seem to be created properly and can be dumped by entering the **show file [device:]filename [dump]** command. With the core-dump file, the same printf is displayed along with this message:

```
yeflateInit fail
```

In this case, a zero byte core-dump file is created. (CSCee27511)

- With a Supervisor Engine 1, IGMP snooping enabled, a host at port 5/8, a statically configured router at port 5/1, a source at port 5/4, and IGMP querier enabled in the VLAN, when the host sends a report and the source sends traffic, a multicast-configured CAM entry is created with the LTL correctly set sending the traffic to the router and the host. When the user configures a QoS MAC-CoS for the GDA and assigns CoS 7, the source and host are stopped, the GDA is deleted, and the CAM entry changes to user-cgfd with an LTL flood to the VLAN. When the source is started, the traffic floods to all ports in the VLAN (99) and the CoS is correct. However, when the host (port 5/8) starts sending reports again and the CAM entry is changed back to multicast configured, the LTL is not set for any ports (router or host) and the traffic is dropped. (CSCee16301)
- You might not be able to statically configure a multicast router port when the spanning tree mode is set to MST. (CSCee02221)
- With a Supervisor Engine 2 and a FWSM in slot 13 of a 13-slot chassis and with both SFM2s powered down, the FWSM fails online diagnostics (PC loopback) but passes the same tests and comes online if the FWSM is reset after bootup. If the SFM2s are up, the module passes diagnostics and comes online (although if diagnostic traces are set to 1, there are still some failure messages coming out of TestKomodoPlusPorts). (CSCed79483)
- With a Supervisor Engine 720 and a 96-port 10/100BASE-TX RJ-45 module (WS-X6148X2-RJ-45), the **show system health** command displays several nonzero registers for the bus ASIC on the WS-X6148X2-RJ-45. One register displays as "SP_TI_CFG." As a configuration register, it should not be showing in the **show system health** command output. There are also problems in the register decodes, in general, they seem to be off by one from the specifications. (CSCed70239)

- With a Supervisor Engine 2, when you enter the **show system health** command, the output shows nonzero registers for the fabric-bus ASIC on the supervisor engine but the registers being identified are not error counters. (CSCed69903)
- With a Supervisor Engine 2 and a 48-port 10/100BASE-TX RJ-45 module (WS-X6548-RJ-45), when you enter the **show system health** command, there are nonzero counters reported for port ASIC 1 but the values being reported are counters, not error counters. (CSCed62522)
- Port-security learned addresses are seen on ports that are in the STP blocking state. (CSCed64228)
- The T1, E1, and FXS voice modules may not come online in text configuration mode.

Workaround: Manually reset the module after the switch fully boots up. (CSCed12999)

- Supervisor Engine 720 uplink ports may lose their configuration when the switch is in text configuration mode. We recommend that you do not use the Supervisor Engine 720 uplink ports if the system is in text configuration mode. Alternatively, every time that the switch is reset, you can manually configure the uplink ports. Binary configuration mode is not affected. (CSCed20712)
- Occasionally, file system corruption may occur on the compact Flash and ATA drive-based file systems (disk0 on Supervisor Engine 2, disk0/disk1 on Supervisor Engine 720, and disk0 on Supervisor Engine 32). You can use the **fsck** command utility to check for file system errors. If file system corruption occurs again after the **fsck** command utility is run, the file system needs to be reformatted. We recommend that you back up configuration files stored on these file systems to a TFTP server on your network. (CSCed64505)
- In text configuration mode, SPAN sessions on service cards such as a NAM and IDS module are not reconfigured after a reset.

Workaround: Manually configure the SPAN sessions on a NAM or IDS each time that the switch is reset. (CSCed65635)

- If you enter the **set port qos m/p autoqos voip ciscosoftphone** command or the **set port macro m/p ciscosoftphone** command on a group of ports, NVRAM corruption may occur. For example, entering the **set port qos 1/1-48,2/2-48 autoqos voip ciscosoftphone** command may cause NVRAM corruption.

Workaround: Run the command on one port at a time as follows:

```
set port qos 1/1 autoqos voip ciscosoftphone
set port qos 1/2 autoqos voip ciscosoftphone
...
...
...
set port qos 2/48 autoqos voip ciscosoftphone
```

(CSCed95002)

- Disaster recovery cannot be done for CMM modules from the Catalyst operating system because the commands that are documented are not available to end users. Call TAC for further assistance if disaster recovery needs to be performed on a CMM. (CSCee06730)
- WS-X6380-NAM ports do not come online. These ports stay errdisabled. Therefore, the WS-X6380-NAM module is not supported in software release 8.3(1) and software release 7.6(7). (CSCee09474)
- If a high percentage of traffic over 32-Gbps is switched through a 13-slot chassis, protocols such as UDLD, CDP, and STP, may fail and result in network downtime. Both Supervisor Engine 2 and Supervisor Engine 720 systems are affected. This problem affects only the 13-slot chassis. This problem is usually seen when the uplink ports on the supervisor engine are passing traffic but there needs to be traffic on other modules to get to 32 Gbps. (CSCee23154)

- Module boot ROM upgrades fail to download to modules supporting the rapid boot feature. As a result, the rapid boot feature is not supported in software release 8.3(1). (CSCee44205)
- If you enter the **show port** command on a switch with voice modules (such as WS-X6624-FXS and WS-X6608-T1), the **show port** command appears to hang and port information for the voice module is not printed. Sometimes the DSP on the voice module may also reset. We recommend that you do not run the **show port** or **show port status** commands on switches with FXS or T1/E1 ports. (CSCed91778, CSCec01126)
- If a service module such as a FWSM or a NAM is configured to boot from a nondefault partition with the supervisor engine in text configuration mode, the service module may fail to come online. In text configuration mode, the boot strings for service modules are not saved correctly at bootup.
Workaround: Manually set the boot string and reset the service module each time the system is reset. Alternately, you can configure service modules to boot off their default partition. (CSCed11214)
- QoS-bridged microflow policing may not work in text configuration mode. The command to enable QoS-bridge microflow policing intermittently fails to enable the feature. Binary configuration mode is not affected.
Workaround: Manually configure the feature each time after the system is reset. (CSCee44277)
- A FWSM and possibly other service modules may not be able to communicate if the dot1q-all-tagged feature is enabled. You cannot use the dot1q-all-tagged feature if a service module is present in the switch.
Workaround: Enter the **set dot1q-all-tagged disable** command and then reset the switch. (CSCed18049)
- At system bootup, secure VLANs associated with the FWSM may not get secured. This problem only happens in text configuration mode.
Workaround: Manually configure the FWSM each time the system boots. (CSCee10706)
- The traffic monitor feature is not supported on the Supervisor Engine 720. Entering the **set traffic monitor threshold** command does not have any effect. (CSCeb66075)
- 100BASE-T SFPs (GLC-T) do not support features such as UDLD and auto-mdix disable. We recommend that you do not enable UDLD on these SFPs. Auto-mdix is always enabled on these SFPs and cannot be disabled. (CSCec26310)
- In text configuration mode, the auto-mdix disable feature fails to work correctly on some modules. If you enter the **set port auto-mdix m/p disable** command and then reset the switch, the feature will be enabled after the switch comes back online. Binary configuration mode is not affected.
Workaround: Manually configure the feature each time the system boots. (CSCed64515)
- The **set mls bridged-flow-statistics enable vlanlist** command may not work correctly if the system is in text configuration mode. When the command is run in text configuration mode, it fails to enable the feature on all VLANs.
Workaround: Use the binary configuration mode or manually run the command each time the system boots. (CSCee44285)
- With Supervisor Engine 1, the boot string contains several boot images but only one, the first one, actually exists in the file system. When you enter the **show system sanity** command, no boot image is reported as invalid (missing). If the one valid image is cleared from the boot string, then all of the remaining (invalid) images are flagged. If the one valid image is added back to the boot string (at the end, instead of the beginning), the three missing images are flagged. (CSCed56928)

- If a multicast entry is configured through the CLI by entering the **set cam** command, it does not get synchronized to the standby supervisor engine in the following cases:
 - When the standby supervisor engine is reloaded after configuring the entry.
 - When high availability is disabled and then reenabled after configuring the entry.

In general, whenever high availability global synchronization is involved in the presence of the entry, it is not synchronized to the standby supervisor engine. When a switchover is done, the new active supervisor engine is not aware of the multicast entry and it does not show the entry in the **show cam** command output.

Workaround: Ensure that high availability is enabled and “ON” by entering the **show system highavailability** command before creating any multicast entries using the **set cam** command. (CSCee27955)

- When you have a root switch with high availability enabled running MST, additional switches running Rapid-PVST+ connected to the root switch and the switches running Rapid-PVST+ are also connected to each other, the switches running Rapid-PVST+ reconverge when a high-availability switchover occurs on the root switch running MST. This problem occurs only when the Rapid-PVST+ switches are connected with each other (such as in a triangular topology). This problem is known to exist in prior software releases.

Workaround: Do not connect the leaf switches. Rapid-PVST+ switches should connect directly to MST switches (this is the recommended topology). (CSCee02592)

- In Rapid-PVST+ mode, the STP runtime timers hello, max_age, and fwd_delay are not set correctly after a high-availability switchover. This problem exists in software releases 8.1(x), 8.2(x), and 7.6(x).

Workaround: Reset the supervisor engine to get newer values. (CSCee41527)

- Command logs are not updated properly after a software upgrade. This problem is seen only when the following conditions are satisfied: 1) The command log buffer in a pre-8.3 software release wrapped around. 2) The switch is upgraded from a pre-8.3 software release to software release 8.3.

Workaround: Because there are no commands to determine whether the command log buffer has wrapped around, the following workaround is suggested if you are upgrading to software release 8.3. From enable mode, perform the following: 1) Enter the **clear log command** command on the active supervisor engine before beginning the upgrade process. 2) Enter the **clear log command** command on the active supervisor engine immediately after the switch has booted software release 8.3. (CSCee42423)

- Configuring private VLANs for any bidirectional PIM group is not supported in software release 8.3(x). (CSCin64195)
- A bidirectional PIM ACE configured on the MSFC with a mask of 32 bits may result in traffic hitting the resulting (*,G/m) or (*,G). This situation could result in inconsistent forwarding.

Workaround: Configure the ACE with a mask of 31 bits. (CSCin62624)

- With Supervisor Engine 1A, all copy tasks such as downloads, copying between devices (Flash and PCMCIA), and redundant boot image synchronizations are extremely slow and take approximately 25 minutes for a 10-MB file. (CSCee24444)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)

- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.3(1)

This section describes resolved caveats in supervisor engine software release 8.3(1):

- The switch might incorrectly report an STP root change with the following message:


```
2003 Jun 09 11:42:28 EST -04:00 %SPANTREE-5-ROOTCHANGE:Root changed for Vlan Y:New
root port n/m. New Root mac address is XX-XX-XX-XX-XX-XX.
```

This is an informational message only and should not affect the operation of your switch.

Workaround: Change the logging level on the SPANTREE facility down to level 4. This problem is resolved in software release 8.3(1). (CSCeb78548)
- With 802.1X authentication, when a configured supplicant logs off, the supplicant's MAC address is removed from the configured list. This problem is resolved in software release 8.3(1). (CSCin25663)
- Temperature values might not be updating properly as seen in the **show environment temperature** command. This problem is resolved in software release 8.3(1). (CSCdy30696)
- When the cache error handler is called on a Supervisor Engine 2, the status register shows the wrong value (0xfffff83). This behavior hides the real register value and prevents debugging. This problem is resolved in software release 8.3(1). (CSCed79489)
- Booting the MSFC image from slot0: might cause problems with VLANs and trunks. This problem is resolved in software release 8.3(1). (CSCed59675)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. This problem is resolved in software release 8.3(1). (CSCin14627)

- With an IDSM module (WS-X6381-IDS), private VLAN configurations are lost after a reboot. You can add an interface of the IDSM module to a private VLAN but the configuration is lost after the reboot.

Workarounds: 1) Reconfigure the private VLAN after a reboot. 2) Use text configuration mode instead of the default binary configuration mode. This problem is resolved in software release 8.3(1). (CSCee13253)

- The unicast packet count is not shown correctly if a port in an EtherChannel is disabled. After you clear the port counters on two directly connected switches, with traffic still running, shut down one port in the channel connecting the switches. When you enter the **show mac** command on the downed port, the port shows zero packets, although some packets were sent in the period between entering the **clear counters** command and the shutdown. These packets are seen in the Rcv-Unicast statistic on the neighboring port. If you enter the **show mac** command in the period between entering the **clear counters** command and the shutdown, you will see Xmit-Unicast incrementing. After shutting down the port, the count is slightly higher than previously shown but considerably less than the Rcv-Unicast statistic shown on the connecting port. The receive side counters are not incrementing after the port shut down. All the packets that passed across the link between the time the counters were cleared and the time the port was shut down are not seen on the sending side. The sending side still shows zero packets as if the port was shut down when the counters were cleared. The counters were cleared before the port was shut down, so there should be outgoing traffic seen on the port. This problem is resolved in software release 8.3(1). (CSCed46961)
- With a high number of unicast flows and several hundred multicast flows, after inducing a Multicast Source Discovery Protocol (MSDP) failover by shutting down a loopback interface on the MSFC2 in slot 15, the switch might crash with a FIB exception. This problem is triggered by entering the **shutdown** command followed by the **no shutdown** command on the loopback interface tied to the anycast route processor (such as when you are testing the anycast router processor failover). This problem is resolved in software release 8.3(1). (CSCea50206)
- The permanent multicast CAM entries might not work after a high-availability switchover.

Workaround: Clear the permanent multicast CAM entries and then enter the entries manually. This problem is resolved in software release 8.3(1). (CSCed87627)



Note While caveat CSCed87627 is resolved in software release 8.3(1), caveat CSCee27955 is open in software release 8.3(1) and CSCee27955 prevents permanent multicast CAM entries from working after a high-availability switchover. For a description of CSCee27955, see the “Open Caveats in Software Release 8.3(1)” section on page 120. (CSCee27955 is resolved in software release 8.3[3].)

- After a high-availability switchover, when the standby supervisor engine becomes the active supervisor engine, channeling ports may receive different QoS attributes and break the EtherChannel due to timing issues. This problem is resolved in software release 8.3(1). (CSCee02504)
- IP phones might not power up after a switchover. This problem is not seen if high availability is enabled. This problem is resolved in software release 8.3(1). (CSCed93870)
- A cluster leak might result in high-availability toggling between enable and disable states. This problem is resolved in software release 8.3(1). (CSCee06373)
- The IGMP-General Query rate-limit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. This problem is resolved in software release 8.3(1). (CSCin42511)

- After a non-high-availability switchover, you might see an error message similar to the following:
2003 Dec 02 18:43:37 %SYS-2-DTP_MODDOWN:Module Down: cfg port trunk-hw failed 9/2.

Entering the **show port** command for the trunk ports show the ports as connected but the **show spantree** command shows them as not connected.

Workarounds: 1) Disable and then enable the port. 2) Reset the module. 3) Upgrade to software release 8.3(1) or later. This problem is resolved in software release 8.3(1). (CSCed14215)

- Trunking inconsistencies were seen when the following actions were taken on a switch: 1) An EtherChannel was configured using two modules. 2) One of the modules was removed from the switch. 3) An existing VLAN on the switch was added to trunks that were members of the EtherChannel. 4) The removed module was reinserted resulting in trunking inconsistencies. This problem is resolved in software release 8.3(1). (CSCed44129)
- With a Supervisor Engine 1/1A or Supervisor Engine 2, the switch might reload with the following log message:

```
ProcessStatusPing:Module 1 local SCP error detected... resetting module
```

Workaround: Remove the faulty module.



Note The fix for this problem involves running a background task to intelligently detect modules that could be causing the SCP errors. When a faulty module is detected, it is automatically shut down.

This problem is resolved in software release 8.3(1). (CSCea38268)

Open and Resolved Caveats in Software Release 8.2(2)

These sections describe open and resolved caveats in supervisor engine software release 8.2(2):

- Open Caveats in Software Release 8.2(2), page 126
- Resolved Caveats in Software Release 8.2(2), page 127

Open Caveats in Software Release 8.2(2)

This section describes open caveats in supervisor engine software release 8.2(2):

- The IGMP-General Query rate-limit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. (CSCin42511)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. (CSCin14627)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but no MAC address is in the CAM table. (CSCin20244)

- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- With 802.1X authentication, when a configured supplicant logs off, the supplicant's MAC address is removed from the configured list. (CSCin25663)
- After a high-availability switchover, the MSFC2 LTLs are not set when the standby router becomes the designated router. (CSCdy83322)



Note This problem is not seen in subsequent releases.

- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- An IGMP version 3 client may receive traffic from unwanted sources. This problem might occur when the IGMP version 3 client abruptly stops sending the IGMP version 3 report and starts sending the IGMP version 3 report to receive traffic from sources that it does not want to receive (before it abruptly stops sending the IGMP version 3 report). (CSCdx53609)



Note This problem is not seen in subsequent releases.

- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

Resolved Caveats in Software Release 8.2(2)

This section describes resolved caveats in supervisor engine software release 8.2(2):

- When you enter the **show qos info runtime** command on a trust-dscp port, the Rx mapping shows all values mapped to a single queue but the Rx Drop Threshold information is displayed. This problem is resolved in software release 8.2(2). (CSCec02299, CSCeb73117)
- TCP flags are not shared correctly. This problem is resolved in software release 8.2(2). (CSCee12831)
- The **set boot system flash Disk0:** command does not work on Supervisor Engine 720. This problem is resolved in software release 8.2(2). (CSCed56322)
- When the cache error handler is called on a Supervisor Engine 2, the status register shows the wrong value (0xfffff83). This behavior hides the real register value and prevents debugging. This problem is resolved in software release 8.2(2). (CSCed79489)

- When a Catalyst 6506 with a Supervisor Engine 1A running software image cat6000-supk9.7-6-4 on the supervisor engine and an MSFC2 running Cisco IOS image MSFC IOS C6MSFC-PK2SV-M 12.1(20)E2 is connected to an Windows XP host that runs IGMP version 3, the Windows XP host stops receiving traffic after approximately 5 minutes. This problem is resolved in software release 8.2(2). (CSCee08209)
- If high-availability versioning is enabled, the Content Services Gateway (CSG) module and the Content Switching Module (CSM) display as “incompatible” when entering the **show system highavailability** command. This results in these modules being reset when there is a high-availability switchover.
Workaround: Do not enable high-availability versioning and the CSG and CSM will not reset during the high-availability switchover. This problem is resolved in software release 8.2(2). (CSCeb25296)
- A port on the WS-X6748-GE-TX module might take longer to start forwarding than is normal. This problem occurs only on the very first link up event after the switch or WS-X6748-GE-TX module comes up. This problem is not seen with subsequent reconnections to the same port.
Workaround: Disconnect and then reconnect the port. This problem is resolved in software release 8.2(2). (CSCec78431)
- Under rare conditions, when a **show** command being filtered with a pipe (|) is aborted with a **Ctrl-C**, the system will leak 480 bytes of memory. This condition occurs when the screen length is restricted with the **set length** command, and the **show** command output is aborted after the output has started but before the “-More-” prompt appears.
Workaround: Wait for the “-More-” prompt to appear before aborting, and then abort normally by either pressing “q” or **Ctrl-C**. This problem is resolved in software release 8.2(2). (CSCec10277)
- The standby supervisor engine uplink ports are not configured correctly in text configuration mode. The standby supervisor engine uplink ports are not configured correctly because the configuration is applied when the ports are not up. To correct this problem, the execution of the text configuration file was delayed for the standby supervisor engine until the standby supervisor engine uplink ports are up. This problem is resolved in software release 8.2(2). (CSCeb15672)
- A Switch Fabric Module switchover might take 8 seconds when the chassis is populated with fabric-enabled modules. This problem is resolved in software release 8.2(2). (CSCed08827)
- When a FlexWAN interface (such as ATM, HSSI, or any port adapter) is created in a system running single router mode (SRM), and the designated MSFC is reloaded (either using the **reload** command from the MSFC or using the **reset** command from the switch CLI), some of the interface/subinterface IP addresses of the FlexWAN interface are no longer pingable. This results in the MLS receive entry on the switch side missing for the IP address.
Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface/subinterface. This action fixes the problem until the next SRM switchover. This problem is resolved in software release 8.2(2). (CSCed30949)
- Supervisor Engine 1A might reset when entering the **copy config flash** command. This problem is resolved in software release 8.2(2). (CSCdy21260)
- With the Supervisor Engine 720/MSFC3, the IGMP reports might not be sent to the MSFC3 ports when the MSFC3 is down. This problem might occur when the MSFC3 (both MSFC3s in a redundant system) is in ROMMON. When the MSFC3 is in ROMMON, IGMP snooping may not relay the IGMP reports to the external MSFC3 ports. This problem is resolved in software release 8.2(2). (CSCin47303)

- When enabling IGMP version 3 processing in IGMP snooping with IGMP version 3 hosts and routers, when the IGMP version 3 processing is disabled, the corresponding forwarding entries do not clear immediately. The entries clear after a maximum of three general queries occur. As a result, between the time that the IGMP version 3 processing is disabled and the IGMP version 3 forwarding entries are cleared, the forwarded multicast traffic is based on stale IGMP version 3 forwarding entries. This problem also might impact the hardware switching of the corresponding multicast traffic during this interval. This problem is only present in software release 8.2(1). This problem is resolved in software release 8.2(2). (CSCin63429)
- The MST command **set spantree mst config name** does not have a carriage return (\n) if the revision number is set to zero in the **show config** command output. This action causes the next command that you enter to merge with this command. This problem is resolved in software release 8.2(2). (CSCed05362)
- When two trunks are enabled one by one with a small delay in between, and with spanning tree disabled for the VLANs, there could be a race condition between the first port going to forwarding state in a particular VLAN and the second trunk port join the spanning tree. Therefore, when more than one port is established as a trunk in a short time period, several VLANs are not allowed. This problem is resolved in software release 8.2(2). (CSCed12056)
- On a port security enabled port, the auto-learned addresses are displayed in the **show config** output. If you enter the **write memory** command, these addresses should be written to the NVRAM, but the auto-learned addresses are not written to the NVRAM.

Workaround: If you want to retain the auto-learned addresses, enable the **set port security auto-configure** option. This problem is resolved in software release 8.2(2). (CSCed46765)

- After a high-availability switchover, an 802.1X port security-enabled port shuts down due to a security violation. This problem occurs if the supplicant that is connected to a port through an IP phone was previously in a guest VLAN when the port was authenticated. The problem seems to occur only with externally powered IP phones. This problem is resolved in software release 8.2(2). (CSCdz60394)
- When the MSFC is reloaded, some VLANs between the MSFC and the supervisor engine might be pruned. This problem is seen with the MSFC VLAN interfaces in the “up/up” state but the MSFC does not respond to the supervisor engine or clients.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the VLAN interfaces. This problem is resolved in software release 8.2(2). (CSCec43550)

- Under rare conditions, the following modules might reset when a link is rapidly going up and down: WS-6248-RJ45, WS-6248-TEL, WS-6348-RJ45, WS-6348-RJ21, WS-6148-RJ45, WS-6148-RJ21, and WS-6348-100FX. This problem occurs when the link goes from down to up to down within 300 ms.

Workaround: Disable the port that is going up and down, or fix the root cause of the link problem. This problem is resolved in software release 8.2(2). (CSCed17719)

- The WS-X6608-T1 and WS-X6608-E1 voice modules might not get configured correctly if the switch is in text configuration mode; some commands could be missing from the running configuration.

Workaround: Manually configure the voice modules after the switch comes online. This problem is resolved in software release 8.2(2). (CSCec00993)

- The RADIUS NAS-Port attribute for an EAP request is padded at the end with a null character, making the attribute 7 bytes long instead of the normal length of 6 bytes as defined in RFC 2865. This problem is resolved in software release 8.2(2). (CSCed47220)
- A switch might not save the configuration for the IGMP rate limit after a reload. This problem is resolved in software release 8.2(2). (CSCed09426)

- With 802.1X authentication, the authenticated 802.1X-enabled port goes to the connecting state after a high-availability switchover if the nonsupplicant in the guest VLAN behind an IP phone is replaced with a supplicant before the switchover. This problem is resolved in software release 8.2(2). (CSCdz60484)
- HTTP authentication bypasses the IP permit list. If you have the IP permit list configured with the HTTP server enabled on the switch, a user can cause a denial of service attack by repeatedly attempting to open an HTTP session to the switch.
Workaround: Configure access control lists (ACLs) on the supervisor engines that support them. On the switches that do not support ACLs, use an external device for access controlling HTTP traffic to the switch or disable the HTTP server on the switch. This problem is resolved in software release 8.2(2). (CSCdw46637)
- When sending TCP or UDP traffic with a Supervisor Engine 2, the output for the **show mls entry** command might be empty when the MLS flow is set to full. When the flow is set to destination or destination-source, the entries are correct.
Workaround: Use the **show mls entry ip protocol tcp** or **show mls entry ip protocol udp** commands to show the details of the TCP or UDP traffic. This problem is resolved in software release 8.2(2). (CSCin59452)
- The MMLS shortcuts between the supervisor engine and the MSFC might not be consistent. This problem is resolved in software release 8.2(2). (CSCec65498)
- You might receive traps indicating configuration revision errors, and entering the **show vtp statistics** command might show the number of configuration revision errors increasing and the revision number matching for all the switches in the VTP domain. To correct the problem, all the switches in the VTP domain need to be upgraded to software release 8.2(2) and then you need to add and delete a VLAN. This problem is resolved in software release 8.2(2). (CSCdy11099)
- When you start a Telnet session to the Catalyst switch using certain Telnet clients, the Catalyst switch prompt is not displayed until you press the **Enter** (return) key.
Workaround: Press the **Enter** key to get to the Catalyst switch prompt. This problem is resolved in software release 8.2(2). (CSCed45576)
- After performing a software upgrade, the switch might experience an exception and reset. If this problem occurs, the **show log** command displays the following error message:
Error Msg: mfree 2: m=0x8c994080 PID = 0 Kernel an

This problem is resolved in software release 8.2(2). (CSCed48590)
- When you configure a WS-X6548-GE-TX port as a SPAN destination and the aggregate bandwidth of the spanned traffic exceeds the SPAN destination port's capacity, you can see performance issues on other ports within the same group. A group of ports is defined as a group of 8-ports (such as 1-8, 9-16, and 17-24).
Workaround: Disable the destination SPAN to ports on the WS-X6548-GE-TX module or put the SPAN destination port in a group where there is nothing connected. This problem is resolved in software release 8.2(2). (CSCed25278)
- When using Rapid STP/MST, a spanning tree loop might occur when you change the bridge priority at the root bridge. This problem is resolved in software release 8.2(2). (CSCed33849)
- After upgrading from software release 6.4(4a) to software release 8.1(1), several LAN modules on some switches might show up as power-bad or power-deny.
Workaround: Reset the switch. This problem is resolved in software release 8.2(2). (CSCec02255)

- When logging into a switch and with TACACS authentication configured, if the TACACS server is unavailable, the user is still prompted for a username. This condition is confusing to users who are not aware that the TACACS server is unavailable and they might keep trying to enter a valid username/password combination.

Workaround: Enter any value as a username. As long as the switch enable password is used as the password, the authentication will be successful. This problem is resolved in software release 8.2(2). (CSCdz16477)

- With 802.1X authentication, a reauthentication might occur every 30 seconds for the supplicant even if reauthentication is disabled and the reauthentication period is set to a higher value. After the supplicant is authenticated, a manual reauthentication causes the reauthentication to occur every 30 seconds. If no manual reauthentication is done, it works correctly. This problem is resolved in software release 8.2(2). (CSCed29480)
- In software releases 7.6(4), 7.6(5), and 8.2(1) after you successfully enable RMON from either SNMP or the CLI, the **show snmp** command shows RMON as disabled. This problem is resolved in software release 7.6(6) and software release 8.2(2) and later releases. (CSCed77175)
- Attempting to upgrade the EPLDs on a module with a voice daughter card attached fails, as the system is unable to read the SPROM of the module.

Workaround: Run the upgrade on the module with the daughter card removed. This problem is resolved in software release 8.2(2). (CSCed84492)

- A switch equipped with a Supervisor Engine 720 may stop forwarding traffic over a WS-X6548-GE-TX module. If this condition occurs, the **show port** command displays the port as connected, and the **show mac** command does not show any transmitted traffic. This problem is resolved in software release 8.2(2). (CSCed68821)
- The switch has multipath BGP with recursive lookup configured with per-prefix statistics disabled. With this configuration, the hardware counters show an inaccurate number of packets/bytes transmitted through all adjacencies in the TCAM. When traffic is sent through the adjacency, the counters keep showing inaccurate/random numbers. Once traffic stops, the counters return to the initial inaccurate state. This problem is resolved in software release 8.2(2). (CSCea13680)
- The switch might crash with RADIUS authentication enabled. The problem might occur after you do the following:
 - Configure RADIUS authentication with the all option.
 - Set the enable password for console.
 - Enable the local login authentication.
 - Log in to the switch and enter a valid RADIUS username and password at the prompt.

After you do the preceding steps, the switch might respond that the account is disabled for both valid and invalid passwords after you try to enter the enable mode. After repeated attempts, the switch might go into an idle state and then reset. This problem is resolved in software release 8.2(2). (CSCed76069)

- When you enter the **squeeze slot0:** command, the supervisor engine CPU might spike above 95 percent for about 30 seconds. This problem is resolved in software release 8.2(2). (CSCec25582)
- Sometimes, a dynamic VLAN is not assigned on the ports with the configured auxiliary VLAN. Initially, the dynamic VLAN for the port works. After the port link goes up and down 50 times, the port stops working. The port displays as a connected port but the status is inactive. This problem is resolved in software release 8.2(2). (CSCec29415)

- Depending on the location of the **capture** lines in a VACL, the capture function might not work. This problem does not impact VACL filtering. This problem is resolved in software release 8.2(2). (CSCec57893)
- After accessing the switch through a Telnet session and entering the **clear vlan** command to clear a large number of VLANs, if the Telnet session automatically logs you out before all the VLANs are cleared, the VLAN database might be left in an inconsistent state.
Workarounds: 1) Reset the switch. 2) If you need to clear a large number of VLANs, do it through the switch console rather than a Telnet session. 3) If you choose to clear a large number of VLANs through a Telnet session, use the **set logout 0** command, and then clear the VLANs. This problem is resolved in software release 8.2(2). (CSCec19091)
- A TACACS+ server might not record accounting information if you input two consecutive commands by copy and paste. This problem is resolved in software release 8.2(2). (CSCec63892)
- When running MMLS on a Supervisor Engine 1/MSFC with partial-SCs, clearing the mroute table or disabling and then reenabling MLS on the MSFC causes packets to stop getting switched on the partial-SC because no packets are received by the MSFC. After a period of time, the corresponding (S,G) entry times out. This problem seems to affect only partial-SC mroute entries with the no “H” flag set. This problem is resolved in software release 8.2(2). (CSCed41953)
- For Supervisor Engine 1 or Supervisor Engine 2, in a redundant system with DRM on the MSFC and high availability enabled on the supervisor engine, packets may be dropped during an MSFC/supervisor engine switchover until the nondesignated MSFC is up. This problem is resolved in software release 8.2(2). (CSCed91504)
- Auxiliary VLANs and VTP pruning might not work together in all instances. This problem is resolved in software release 8.2(2). (CSCed05516)
- The Network Analysis Module (WS-X6380-NAM) management VLAN does not match the switch sc0 interface VLAN. These VLANs should match.
Workaround: Leave the sc0 interface in VLAN 1. This problem is resolved in software release 8.2(2). (CSCed47510)
- There is a memory leak in the DVLAN_RECONF process when you run a heavy CPU load. This problem is resolved in software release 8.2(2). (CSCeb85102)
- With a Supervisor Engine 2, the high-availability switchover time might be different for the 6-slot and 13-slot chassis. The 13-slot chassis switchover time might be greater than the 6-slot chassis. This problem is resolved in software release 8.2(2). (CSCed68109)
- When you have a VMPS database downloading to the switch (initiated by entering the **download vmps** command), the switch might crash during the “VMPSDownload” process. This problem is due to the vmps-port-group field not being specified in the VMPS configuration file. This problem is resolved in software release 8.2(2). (CSCed43310)
- You might experience a memory leak related to the “Kernel and Idle” process if you enter the **show proc mem** command. This problem is resolved in software release 8.2(2). (CSCed60959)
- With a Supervisor Engine 720/MSFC3, any traffic matching the MLS exclude protocol might be incorrectly sent to the MSFC3 for processing. This problem is resolved in software release 8.2(2). (CSCee09339)
- With Supervisor Engine 1 running software release 8.x, ping packets sent to NDR interfaces that are different from the source VLAN fail after the first packet. This problem is resolved in software release 8.2(2). (CSCed59834)
- On a switch running cryptographic (k9) images, if the value of sshPublicKeySize is nonzero, the SNMP_THREAD process might have a memory leak when sshPublicKeySize is polled. This problem is resolved in software release 8.2(2). (CSCed95950)

Open and Resolved Caveats in Software Release 8.2(1)

These sections describe open and resolved caveats in supervisor engine software release 8.2(1):

- Open Caveats in Software Release 8.2(1), page 133
- Resolved Caveats in Software Release 8.2(1), page 134

Open Caveats in Software Release 8.2(1)

This section describes open caveats in supervisor engine software release 8.2(1):

- When enabling IGMP version 3 processing in IGMP snooping with IGMP version 3 hosts and routers, when the IGMP version 3 processing is disabled, the corresponding forwarding entries do not clear immediately. The entries clear after a maximum of three general queries occur. As a result, between the time that the IGMP version 3 processing is disabled and the IGMP version 3 forwarding entries are cleared, the forwarded multicast traffic is based on stale IGMP version 3 forwarding entries. This problem also might impact the hardware switching of the corresponding multicast traffic during this interval. This problem is only present in software release 8.2(1). (CSCin63429)
- When you enter the **show qos info runtime** command on a trust-dscp port, the Rx mapping shows all values mapped to a single queue but the Rx Drop Threshold information is displayed. (CSCec02299)
- The IGMP-General Query rate-limit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. (CSCin42511)
- With 802.1X authentication, the authenticated 802.1X-enabled port goes to the connecting state after a high-availability switchover if the nonsupplicant in the guest VLAN behind an IP phone is replaced with a supplicant before the switchover. (CSCdz60484)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. (CSCin14627)
- After a high-availability switchover, an 802.1X port security-enabled port will shut down due to a security violation. This problem occurs if the supplicant that is connected to a port through an IP phone was previously in a guest VLAN when the port was authenticated. The problem seems to happen only with externally powered IP phones. (CSCdz60394)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but there is no MAC address in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- With 802.1X authentication, when a configured supplicant logs off, the supplicant's MAC address is removed from the configured list. (CSCin25663)
- After a high-availability switchover, MSFC2 LTLs are not set when the standby router becomes the designated router. (CSCdy83322)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)

- An IGMP version 3 client may receive traffic from unwanted sources. This problem might occur when the IGMP version 3 client abruptly stops sending the IGMP version 3 report and starts sending the IGMP version 3 report to receive traffic from sources that it does not want to receive (before it abruptly stops sending the IGMP version 3 report). (CSCdx53609)
- HTTP authentication bypasses the IP permit list. If you have the IP permit list configured with the HTTP server enabled on the switch, a user can cause a denial of service attack by repeatedly attempting to open an HTTP session to the switch.

Workaround: Configure access control lists (ACLs) on the supervisor engines that support them. On the switches that do not support ACLs, use an external device for access controlling HTTP traffic to the switch or disable the HTTP server on the switch. (CSCdw46637)

- With the Supervisor Engine 720/MSFC3, the IGMP reports might not be sent to the MSFC3 ports when the MSFC3 is down. This problem might occur when the MSFC3 (both MSFC3s in a redundant system) is in ROMMON. When the MSFC3 is in ROMMON, IGMP snooping may not relay the IGMP reports to the external MSFC3 ports. (CSCin47303)
- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

- On a port security enabled port, the auto-learned addresses are displayed in the **show config** output. If you enter the **write memory** command, these addresses should be written to the NVRAM, but the problem is that the auto-learned addresses are not written to the NVRAM.

Workaround: If you want to retain the auto-learned addresses, enable the **set port security auto-configure** option. (CSCed46765)

Resolved Caveats in Software Release 8.2(1)

This section describes resolved caveats in supervisor engine software release 8.2(1):

- When a linkdown trap is sent for a security violation, the value of portSecurityLastSrcAddr might be wrong. If port security is configured using static addresses and a security violation occurs, the configured address is sent in the trap and not the address that actually caused the violation. If port security is configured dynamically and the port is shut down due to a security violation, the linkdown trap contains an invalid MAC address. This problem is resolved in software release 8.2(1). (CSCeb49723)
- When there is an MSFC switchover, it is possible that multicast entries at the supervisor engine will be deleted immediately causing a short disruption in traffic forwarding. This behavior is identical to what happens during a supervisor engine switchover. This problem is resolved in software release 8.2(1). (CSCeb52670)

- With a Supervisor Engine 1/PFC and the following security ACL configured:

```
Cat6k> (enable) show sec acl info ACL_TEST
set security acl ip ACL_TEST
```

```
-----
1. deny icmp any any fragment
2. permit ip any any
```

Both unfragmented and fragmented ICMP packets are denied (the keyword **fragment** is ignored). This problem is not seen with other supervisor engines. This problem is resolved in software release 8.2(1). (CSCea51346)

- A VACL might not filter flows when the UDP source and destination equal 0.
Workaround: Apply an inbound Cisco IOS ACL in hardware. Note that the MSFC must run a recent Cisco IOS Release (Release 12.1(13)E4 was tested and works fine). This problem is resolved in software release 8.2(1). (CSCea65662)
- If you use the maximum character length for a VACL name (31 characters), the switch might reset with a TLB exception after entering the **show config** command. This problem is resolved in software release 8.2(1). (CSCeb37804)
- With software release 8.1(2), command authorization might fail in the TCL shell. This problem is resolved in software release 8.2(1). (CSCec23736)
- When booting a Supervisor Engine 2 or Supervisor Engine 720 with Catalyst software release 8.1(1) in a 6503 chassis with PWR-950-DC power supplies, the system denies power to the remaining slots. The **show env power** command reports PS1 and PS2 at 0 Watts with no available power. This problem is resolved in software release 8.2(1). (CSCec18414)
- With a few hundred secure addresses on a port with a large amount of continuous traffic through the port, and aging enabled, it takes a long time for the addresses to clear out and then be resecured. This problem is resolved in software release 8.2(1). (CSCeb22295)
- With diagnostics set to complete and text configuration mode specified, after a switch over to the redundant supervisor engine, some items in the standby supervisor engine configuration might not be operational. This problem is resolved in software release 8.2(1). (CSCea63643)
- With Supervisor Engine 1, the console might lock up when the switch is reset. This problem has not been seen on switches with redundant Supervisor Engine 1s. This problem is resolved in software release 8.2(1). (CSCea60922)
- When you attempt to establish a console connection and are prompted for the username, if you inadvertently cut and paste a large file (over 100 KB) into the CLI username prompt instead of the correct username, you will see many “%MGMT-5-LOGIN_FAIL:User log” messages. Then after 10 to 14 minutes, the switch will reset with a Breakpoint Exception. This problem is resolved in software release 8.2(1). (CSCea72986)
- After entering the **switch supervisor** command and letting traffic run, when you enter the **show mac** command, the Xmit-Unicast data column is always 0. Additionally, the **show count** command does not display the txHCUnicastPkts data and, the field is always 0. This problem is resolved in software release 8.2(1). (CSCeb60675)
- When a port is configured for a host connection using the **set port host mod/port** command, its CBL should remain in forwarding state when the port is disconnected. This assures that when the link comes up, traffic is switched immediately. When the port is disconnected, spanning tree sends the correct CBL state but dot1x authorization sets the CBL to disable. This problem is resolved in software release 8.2(1). (CSCeb52364)

- When configuring an EtherChannel with ports on separate modules with the jumbo frames and 802.1Q tunneling features configured, the channel configuration may get lost on a member port when using text configuration mode.
Workaround: Use “desirable” mode or binary configuration mode. This problem is resolved in software release 8.2(1). (CSCec06429)
- The WS-X6502-10GE module might form a unidirectional link with the port transmit side functioning but the receive side not functioning.
Workaround: Configure UDLN and/or loop guard to prevent a unidirectional link. This problem is resolved in software release 8.2(1). (CSCeb59325)
- A WS-X6248-TEL module port displays as “connected” when it is manually enabled even though it is connected to a WS-X6248-TEL module port in another switch that is manually disabled.
Workaround: Reset the system. This problem is resolved in software release 8.2(1). (CSCea19802)
- With a Firewall Services Module (FWSM), LTLs might not be set properly if VTP pruning is enabled. This problem is resolved in software release 8.2(1). (CSCea04936)
- With the spanning tree mode set to MISTP-PVST+, when a port leaves or joins a channel, the color blocking logic (CBL) for that port might not be set, resulting in no traffic going through that port. This problem occurs with an 8-port channel that has the channel mode set to on. The ports in the channel were enabled and then disabled, or the module was reset.
Workaround: Disable and then reenables the port (this action might not always work), or change the channel mode to “desirable.” This problem is resolved in software release 8.2(1). (CSCea48516)
- It might not be possible to configure port security on a dot1q tunnel access port. This problem is resolved in software release 8.2(1). (CSCeb54461)
- You should not be able to set ports belonging to the same port ASIC as follows: One port set to trunking mode or a SPAN destination, and another port set to a promiscuous, isolated, or community port. However, on the WS-X6148-GE-TX and WS-X6548-GE-TX modules, you are allowed to set a private VLAN on the same port ASIC where a trunk/SPAN is configured. This problem is resolved in software release 8.2(1). (CSCea77251)
- The maximum burst value that could be configured for a policer was 32,000 kb. The maximum burst rate should have been 256,000 kb. This problem is resolved in software release 8.2(1). (CSCeb22622)
- Configuring trust-cos (for example, **set port qos 3/1 trust trust-cos**) on WS-X6502-10GE ports might result in poor unicast traffic performance. This problem is resolved in software release 8.2(1). (CSCeb30334)
- New vulnerabilities in the OpenSSH implementation for SSH servers have been announced. An affected network device, running an SSH server based on the OpenSSH implementation, may be vulnerable to a Denial of Service (DoS) attack when an exploit script is repeatedly executed against the same device.
Workaround: There are workarounds available to mitigate the effects of these vulnerabilities. Refer to the advisory at this URL:
<http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml>
This problem is resolved in software release 8.2(1). (CSCec33092)
- A Supervisor Engine 1 or 1A may reload with the following log message:

```
ProcessStatusPing:Module 1 local SCP error detected... resetting module
```


Workaround: Remove the faulty module.

- The switch fails to return the complete Fully Qualified Domain Name (FQDN) when polled for the following:

```
sysName
.1.3.6.1.2.1.1.5
```

The switch returns the host name only. This situation is not compliant with the definition of sysName stated in RFC-1907. This problem has a tendency to break NMS applications that expect the switch to respond back with the correct sysName.

Workaround: Specify the complete FQDN on the switch so that sysName returns the complete FQDN:

Enter the following on the switch:

```
nms-6506a> (enable) set system name nms-6506a.sys.etc
System name set.
nms-6506a> (enable) exit
Connection closed by foreign host.
```

Enter the following on the NMS:

```
nms-server2> snmpwalk -c public nms-6506a sysName
SNMPv2-MIB::sysName.0 = STRING: nms-6506a.sys.etc
```

This problem is resolved in software release 8.2(1). (CSCeb37492)

- Different VLANs on a switch might have the same VlanIfIndex. This problem usually occurs after a high-availability switchover that is caused by an exception on the active supervisor engine. This problem is resolved in software release 8.2(1). (CSCeb61525)
- Using the **show snmp ifalias** command might cause a memory leak. This problem is resolved in software release 8.2(1). (CSCeb86760)
- A switch with either a WS-X6K-SUP1A-2GE or WS-X6K-S2U-2GE supervisor engine and a WS-F6K-MSFC2 running boot loader image version 12.1(19)E with the main image on the PCMCIA Flash card in slot0: may not pass traffic to or from the MSFC on VLAN 1 after a reload. This situation affects only traffic that is routed to or from VLAN 1. Traffic being switched within VLAN 1 is not affected by this issue. This issue may be seen when running any version of Catalyst software on the supervisor engine and Cisco IOS boot loader version 12.1(19)E on the MSFC2. Traffic will still pass to and from the MSFC2 for all other VLANs.

Workarounds: 1) Enter the **shutdown** and the **no shutdown** commands on the VLAN 1 virtual interface on the MSFC2. This action will fix the problem until the next reload of the MSFC2 or supervisor engine. 2) If MSFC2 redundancy is not being provided by single router mode (SRM), this issue can be avoided by downgrading only the boot loader image to 12.1(13)E. This problem is resolved in software release 8.2(1). (CSCeb02380)
- A spanning tree loop could be created when you use the **show spantree mst config** or **show spantree mst instance** commands to display a large console output for a MST instance/VLAN mapping.

Workaround: Use the **set length** command to set the screen length to less than 50. This problem is resolved in software release 8.2(1). (CSCec16775)
- Polarization occurs when a switch and its downstream switch have an even number of paths for a prefix. Traffic received on the downstream switch may not be distributed across all paths. This problem is resolved in software release 8.1(2). (CSCeb40304)
- The switch might crash in the getPermTypeValue function. This problem is resolved in software release 8.2(1). (CSCea11480)

- With a WS-X6381-IDS module installed, you might experience a memory leak over a period of weeks.
Workaround: Reload the switch every few weeks to regain lost memory. This problem is resolved in software release 8.2(1). (CSCeb59206)
- When you specify the destination device as slot0:, slot1:, disk0:, or disk1: for the syslog dump feature using the **set system syslog-file device:[filename]** command, the system will hang during the system failure and will not reload. You must power cycle the system. Note that the system will hang only if there is a system failure.
Workaround: Write the file to bootflash. This problem is resolved in software release 8.2(1). (CSCeb51638)
- With MISTP and EtherChannel between switches, when channel ports are disabled and then enabled, some VLANs of the MISTP instance may still show a CBL disable status. This problem is resolved in software release 7.6(3a). (CSCec19186)
- A Supervisor Engine 2 might crash after “%ACL-3-TCAMFULL:Ac1 engine TCAM table is full” messages are seen during the updating of large Cisco IOS ACLs. This problem is resolved in software release 8.2(1). (CSCec04515)
- With software release 7.6(3a) and later releases, the NVRAM monitor is disabled by default at bootup. This feature should be enabled by default. This problem is resolved in software release 8.2(1). (CSCec62324)
- LTLs for multicast and broadcast might not be set after a MST topology change. This problem is resolved in software release 8.2(1). (CSCec23939)
- The 12.1(19)E boot loader on an MSFC fails to work correctly if the MSFC runtime image is on sup-slot0: and text configuration mode is configured. This problem is resolved in software release 8.2(1). (CSCeb36759)
- When two MST switches are connected and if one of the switch ports goes into root inconsistent state, the port does not transmit BPDUs. This problem can cause a loop in the network.
Workaround: Clear the root inconsistency. This problem is resolved in software release 8.2(1). (CSCec67810)
- The port ifIndex on a Supervisor Engine 1 might become 0 after a high-availability switchover. This problem is resolved in software release 8.2(1). (CSCec44842)
- In rare circumstances, upgrading a supervisor engine or switching module EPLD may fail with the message: “Error: Programming EPLD. Error code = 16.” This problem may leave the supervisor engine or switching module inoperable. This problem is resolved in software release 8.2(1). (CSCec77150)
- In a redundant system with WS-X6516 modules configured for channel mode, a reset of one of the modules might cause traffic forwarded through the channel to be dropped. This problem is resolved in software release 8.2(1). (CSCec18911)
- The maximum number of 128 permanent CAM entries needs to be increased. With software release 8.2(1), the number of permanent CAM entries has been increased to 256. (CSCdz35901)
- This problem was seen on a switch running software release 6.4(4a) on a Supervisor Engine 2 and Cisco IOS Release 12.1(13)E19 on the MSFC2. MLS entries in the supervisor engine forwarding information base are not updated after a server failover although the ARP entry is correct. This problem is resolved in software release 8.2(1). (CSCec27027)
- Disabling and enabling ports that belong to two channels may cause ports in one channel to remain in spanning tree blocking state and traffic going through the channel to be dropped.
Workaround: Enable and disable the ports again. This problem is resolved in software release 8.2(1). (CSCec63559)

- The **show version** command does not display the correct memory (DRAM) usage if the supervisor engine (Supervisor Engine 2 and Supervisor Engine 720) has more than 256-MB DRAM. This problem is resolved in software release 8.2(1). (CSCdz46084)
- With Supervisor Engine 720s, the second uplink ports of the active and standby Supervisor Engine 720s might not link up the first time you boot the switch and change the media type to RJ-45.
Workaround: Disable and enable the ports to bring the link up. This problem is resolved in software release 8.2(1). (CSCeb48056)
- When you enter the **clear cam static** command, the following message is displayed:
%EARL-3-LTL:Failure to set LTL for module *n*

The message is printed only when the EARL logging level is set to 3 or higher. This problem is resolved in software release 8.2(1). (CSCed05566)
- The MLS table is empty when using SRM with a Supervisor Engine 1/MSFC with the c6msfc image. This problem is seen only when booting from sup-slot0:, there is no problem when booting from bootflash:. You see this problem because the ROMMON of the MSFC (as opposed to the ROMMON of the MSFC2) does not support TFTP which is required to boot from sup-slot0: The boot image is loaded first and the boot image is not SRM enabled. You end up with one MSFC running in SRM mode and other running in DRM mode.
Workaround: Use an image that supports SRM (such as c6msfc-isv-mz or c6msfc-is-mz) as the boot image in the bootflash when booting an image from sup-slot0:. This problem is resolved in software release 8.2(1). (CSCec38119)
- MLS IP fast-aging time might not work correctly. This problem is resolved in software release 8.2(1). (CSCec70012)
- When there is a high-availability switchover with the spanning-tree mode set to MSTP or MISTP, and there are at least 50,000 instances, it is possible for the switch to experience flooding of multicast control packets. This problem results in IGMP snooping experiencing a lot of port/VLAN up/down events and IGMP control packets causing CPU utilization to go up. Whenever this happens, IGMP snooping gets disabled for a period of 5 minutes and gets reenabled again automatically. Therefore, IGMP snooping will not be usable for 5 minutes and states are started afresh when it is reenabled. This problem is resolved in software release 8.2(1). (CSCec69290)
- ARP requests or responses with a length of 60 bytes that are received by the switch and sent to the CPU of the switch for ARP inspection are padded by the switch with an additional 8 bytes, causing 68-byte ARPs. This problem is resolved in software release 8.2(1). (CSCec65991)
- Microsoft has released KB article 826942 to allow VLAN assignment with DHCP interoperability. Assuming proper VLAN assignment, the code sends three ICMP echos to the current default gateway. If the echoes are not answered, a broadcast is renewed for the DHCP address. The result is that the pings are answered and the tested end point does not request a new IP address. This problem is resolved in software release 8.2(1). (CSCec70893)
- When using SSH to the switch using external authentication, if you enter a blank username (when you press Enter at the username prompt without typing in a username), no matter what password you enter, the session might hang. Additionally, if you enter an incorrect username, you are prompted for the password three times and then the session disconnects. This problem is resolved in software release 8.2(1). (CSCea89170)

- On a Catalyst 6500 series switch or Cisco 7600 series router, an SSH authentication failure may result in 32 bytes of memory leakage. If this condition is repeated it may cause denial of service symptoms on the switch.

Workaround: Permit SSH access only to authorized hosts. An example may look like this display:

```
set ip permit <authorized host #1> ssh
set ip permit <authorized host #2> ssh
set ip permit enable
```

This problem is resolved in software release 8.2(1). (CSCeb49724)

- A vlanTrunkPortDynamicStatus value might not be returned for NAM and IDS module ports. This problem is resolved in software release 8.2(1). (CSCin51922)

Open and Resolved Caveats in Software Release 8.1(3)

These sections describe open and resolved caveats in supervisor engine software release 8.1(3):

- Open Caveats in Software Release 8.1(3), page 140
- Resolved Caveats in Software Release 8.1(3), page 142

Open Caveats in Software Release 8.1(3)

This section describes open caveats in supervisor engine software release 8.1(3):

- When you enter the **show qos info runtime** command on a trust-dscp port, the Rx mapping shows all values mapped to a single queue but the Rx Drop Threshold information is displayed. (CSCec02299)
- The IGMP-General Query rate-limit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. (CSCin42511)
- The **show version** command does not display the correct memory (DRAM) usage if the supervisor engine (Supervisor Engine 2 and Supervisor Engine 720) has more than 256-MB DRAM. (CSCdz46084)
- With 802.1X authentication, the authenticated 802.1X-enabled port goes to the connecting state after a high-availability switchover if the nonsupplicant in the guest VLAN behind an IP phone is replaced with a supplicant before the switchover. (CSCdz60484)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. (CSCin14627)
- After a high-availability switchover, an 802.1X port security-enabled port will shut down due to a security violation. This problem occurs if the supplicant that is connected to a port through an IP phone was previously in a guest VLAN when the port was authenticated. The problem seems to happen only with externally powered IP phones. (CSCdz60394)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but there is no MAC address in the CAM table. (CSCin20244)

- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- With 802.1X authentication, when a configured supplicant logs off, the supplicant's MAC address is removed from the configured list. (CSCin25663)
- After a high-availability switchover, MSFC2 LTLs are not set when the standby router becomes the designated router. (CSCdy83322)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- An IGMP version 3 client may receive traffic from unwanted sources. This problem might occur when the IGMP version 3 client abruptly stops sending the IGMP version 3 report and starts sending the IGMP version 3 report to receive traffic from sources that it does not want to receive (before it abruptly stops sending the IGMP version 3 report). (CSCdx53609)
- HTTP authentication bypasses the IP permit list. If you have the IP permit list configured with the HTTP server enabled on the switch, a user can cause a denial of service attack by repeatedly attempting to open an HTTP session to the switch.

Workaround: Configure access control lists (ACLs) on the supervisor engines that support them. On the switches that do not support ACLs, use an external device for access controlling HTTP traffic to the switch or disable the HTTP server on the switch. (CSCdw46637)

- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

- With Supervisor Engine 720s, the second uplink ports of the active and standby Supervisor Engine 720s might not link up the first time that you boot the switch and change the media-type to RJ-45.

Workaround: Disable and enable the ports to bring the link up. (CSCeb48056)

- With software release 8.1(3), only one MSFC MAC entry is seen in the Layer 2 CAM table with dual-router mode (DRM) high availability enabled at boot time.



Note This problem is not seen in any later software releases.

Workaround: Enter the **shutdown** followed by **no shutdown** commands on the interfaces.

- With the Supervisor Engine 720/MSFC3, IGMP reports might not be sent to the MSFC3 ports when the MSFC3 is down. This problem might occur when the MSFC3 (both MSFC3s in a redundant system) is in ROMMON. When the MSFC3 is in ROMMON, IGMP snooping may not relay the IGMP reports to the external MSFC3 ports. (CSCin47303)

- On a port security enabled port, the auto-learned addresses are displayed in the **show config** output. If you enter the **write memory** command, these addresses should be written to the NVRAM, but the problem is that the auto-learned addresses are not written to the NVRAM.

Workaround: If you want to retain the auto-learned addresses, enable the **set port security auto-configure** option. (CSCed46765)

Resolved Caveats in Software Release 8.1(3)

This section describes resolved caveats in supervisor engine software release 8.1(3):

- An affected network device, running an SSH server based on the OpenSSH implementation, may be vulnerable to a Denial of Service (DoS) attack when an exploit script is repeatedly executed against the same device. There are workarounds available to mitigate the effects of these vulnerabilities. This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml>. This problem is resolved in software release 8.1(3). (CSCec33092)

Open and Resolved Caveats in Software Release 8.1(2)

These sections describe open and resolved caveats in supervisor engine software release 8.1(2):

- Open Caveats in Software Release 8.1(2), page 142
- Resolved Caveats in Software Release 8.1(2), page 144

Open Caveats in Software Release 8.1(2)

This section describes open caveats in supervisor engine software release 8.1(2):

- When you enter the **show qos info runtime** command on a trust-dscp port, the Rx mapping shows all values mapped to a single queue but the Rx Drop Threshold information is displayed. (CSCec02299)
- The IGMP-General Query rate-limit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. (CSCin42511)
- The **show version** command does not display the correct memory (DRAM) usage if the supervisor engine (Supervisor Engine 2 and Supervisor Engine 720) has more than 256-MB DRAM. (CSCdz46084)
- With 802.1X authentication, the authenticated 802.1X-enabled port goes to the connecting state after a high-availability switchover if the nonsupplicant in the guest VLAN behind an IP phone is replaced with a supplicant before the switchover. (CSCdz60484)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. (CSCin14627)
- After a high-availability switchover, an 802.1X port security-enabled port will shut down due to a security violation. This problem occurs if the supplicant that is connected to a port through an IP phone was previously in a guest VLAN when the port was authenticated. The problem seems to happen only with externally powered IP phones. (CSCdz60394)

- With 802.1X authentication, if a high-availability switchover occurs during an authentication after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows that the port MAC address is secured, but there is no MAC address in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- With 802.1X authentication, when a configured supplicant logs off, the supplicant's MAC address is removed from the configured list. (CSCin25663)
- After a high-availability switchover, MSFC2 LTLs are not set when the standby router becomes the designated router. (CSCdy83322)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- An IGMP version 3 client may receive traffic from unwanted sources. This problem might occur when the IGMP version 3 client abruptly stops sending the IGMP version 3 report and starts sending the IGMP version 3 report to receive traffic from sources that it does not want to receive (before it abruptly stops sending the IGMP version 3 report). (CSCdx53609)
- HTTP authentication bypasses the IP permit list. If you have the IP permit list configured with the HTTP server enabled on the switch, a user can cause a denial of service attack by repeatedly attempting to open an HTTP session to the switch.

Workaround: Configure access control lists (ACLs) on the supervisor engines that support them. On the switches that do not support ACLs, use an external device for access controlling HTTP traffic to the switch or disable the HTTP server on the switch. (CSCdw46637)

- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

- With Supervisor Engine 720s, the second uplink ports of the active and standby Supervisor Engine 720s might not link up the first time that you boot the switch and change the media-type to RJ-45.

Workaround: Disable and enable the ports to bring the link up. (CSCeb48056)

- With the Supervisor Engine 720/MSFC3, the IGMP reports might not be sent to the MSFC3 ports when the MSFC3 is down. This problem might occur when the MSFC3 (both MSFC3s in a redundant system) is in ROMMON. When the MSFC3 is in ROMMON, IGMP snooping may not relay the IGMP reports to the external MSFC3 ports. (CSCin47303)

- On a port security enabled port, the auto-learned addresses are displayed in the **show config** output. If you enter the **write memory** command, these addresses should be written to the NVRAM, but the auto-learned addresses are not written to the NVRAM.

Workaround: If you want to retain the auto-learned addresses, enable the **set port security auto-configure** option. (CSCed46765)

Resolved Caveats in Software Release 8.1(2)

This section describes resolved caveats in supervisor engine software release 8.1(2):

- When there is an MSFC switchover, it is possible that multicast entries at the supervisor engine will be deleted immediately causing a short disruption in traffic forwarding. The behavior is identical to what happens during a supervisor engine switchover. This problem is resolved in software release 8.1(2). (CSCeb52670)
- On the WS-X6502-10GE module, the channel mode is automatically configured to “off.” This problem is resolved in software release 8.1(2). (CSCeb24990)
- Packets to be sent out the WS-X6548-GE-TX or WS-X6148-GE-TX modules that are less than 64 bytes are dropped. This occurs when a device forwards a packet that is 60 bytes and the 4-byte dot1q tag is added to create a valid 64-byte packet. When the tag is removed, the packet is 60 bytes. If the destination is out a port on the WS-X6548-GE-TX or WS-X6148-GE-TX modules, the packet is dropped by the module. This problem is resolved in software release 8.1(2). (CSCeb67650)
- With MISTP configured, when a nonroot switch attempts to be the root switch, a TLB exception might occur. This problem is resolved in software release 8.1(2). (CSCeb60477)
- The switch fails to return the complete Fully Qualified Domain Name (FQDN) when polled for the following:

```
sysName
.1.3.6.1.2.1.1.5
```

The switch returns the host name only. This situation is not compliant with the definition of sysName stated in RFC 1907. This problem can break NMS applications that expect the switch to respond back with the correct sysName.

Workaround: Specify the complete FQDN on the switch so that the sysName returns the complete FQDN:

Enter the following on the switch:

```
nms-6506a> (enable) set system name nms-6506a.sys.etc
System name set.
nms-6506a> (enable) exit
Connection closed by foreign host.
```

Enter the following on the NMS:

```
nms-server2> snmpwalk -c public nms-6506a sysName
SNMPv2-MIB::sysName.0 = STRING: nms-6506a.sys.etc
```

This problem is resolved in software release 8.1(2). (CSCeb37492)

- If you use the maximum character length for a VACL name (31 characters), the switch might reset with a TLB exception after entering the **show config** command. This problem is resolved in software release 8.1(2). (CSCeb37804)

- With a Supervisor Engine 720 in flow-through mode and after a high-availability switchover, unicast traffic is restored but multicast traffic stops. This problem only happens when the switch is in flow-through mode.
Workaround: Reset the switch. This problem is resolved in software release 8.1(2). (CSCeb61207)
- Polarization occurs when a switch and its downstream switch have an even number of paths for a prefix. Traffic received on the downstream switch may not be distributed across all paths. This problem is resolved in software release 8.1(2). (CSCeb40304)
- In IGMP fallback mode, the switch might only forward UDP packets destined to address 224.0.0.9 to a multicast router port. This behavior could break the exchange of RIP version 2 update packets between RIP version 2 routers in the VLAN when the IGMP mode goes to fallback.
Workaround: Configure a static multicast MAC entry for 01-00-5e-00-00-09 on ports connected to RIP version 2 routers. This problem is resolved in software release 8.1(2). (CSCeb53428)
- The WS-X6348-RJ-45 module might repeatedly reset. When this particular reset occurs, the logging buffer contains a message indicating that the module is online but *does not* contain a preceding message showing the module resetting. This problem is resolved in software release 8.1(2). (CSCeb35612)
- On a switch with a Supervisor Engine 1, RSPAN source ports might not work in the Rx or TX directions on any port in the switch. RSPAN destination ports work properly. This problem is resolved in software release 8.1(2). (CSCeb80640)
- If an ECC error is detected, you may see more ECC errors generated as a result of the first ECC error. This problem is resolved in software release 8.1(2). (CSCeb72947)

Open and Resolved Caveats in Software Release 8.1(1)

These sections describe open and resolved caveats in supervisor engine software release 8.1(1):

- Open Caveats in Software Release 8.1(1), page 145
- Resolved Caveats in Software Release 8.1(1), page 147

Open Caveats in Software Release 8.1(1)

This section describes open caveats in supervisor engine software release 8.1(1):

- When you enter the **show qos info runtime** command on a trust-dscp port, the Rx mapping shows all values mapped to a single queue but the Rx Drop Threshold information is displayed. (CSCec02299, CSCeb73117)
- The IGMP-General Query ratelimit feature is not supported on Supervisor Engine 720. The feature can cause a high supervisor engine CPU load and can disrupt multicast switching. (CSCin42511)
- When there is an MSFC switchover, it is possible that multicast entries at the supervisor engine will be deleted immediately causing a short disruption in traffic forwarding. The behavior is identical to what happens during a supervisor engine switchover. (CSCeb52670)
- The **show version** command does not display the correct memory (DRAM) usage if the supervisor engine (Supervisor Engine 2 and Supervisor Engine 720) has more than 256-MB DRAM. (CSCdz46084)

- With 802.1X authentication, the authenticated 802.1X-enabled port goes to the connecting state after a high-availability switchover if the nonsupplicant in the guest VLAN behind an IP phone is replaced with a supplicant before the switchover. (CSCdz60484)
- With 802.1X authentication, the authenticator will not be able to communicate through the sc1 interface to the RADIUS server if the authenticator address configured on the RADIUS server is the sc1 interface IP address. (CSCin14627)
- After a high-availability switchover, an 802.1X port security-enabled port will shut down due to a security violation. This problem occurs if the supplicant that is connected to a port through an IP phone was previously in a guest VLAN when the port was authenticated. The problem seems to happen only with externally powered IP phones. (CSCdz60394)
- With 802.1X authentication, if a high-availability switchover occurs during an authentication, after the switchover completes, single authentication and port security are in the authenticated state but the port might not get added to spanning tree. If this situation occurs, then the port would not receive CBL or LTLs. The **show port security** command shows the port MAC address is secured but there is no MAC address in the CAM table. (CSCin20244)
- With high availability enabled, port security is enabled on a port using the **violation restrict** mode. On repeatedly clearing the secured addresses under continuous traffic, the secured port on the standby supervisor engine might shut down. (CSCin25168)
- With 802.1X authentication, when a configured supplicant logs off, their MAC address is removed from the configured list. (CSCin25663)
- After a high-availability switchover, MSFC2 LTLs are not set when the standby router becomes the designated router. (CSCdy83322)
- IGMP version 3 does not support private VLANs. Support for private VLANs will be added in a future release. (CSCdx08912)
- HTTP authentication bypasses the IP permit list. If you have the IP permit list configured with the HTTP server enabled on the switch, a user can cause a denial of service attack by repeatedly attempting to open an HTTP session to the switch.

Workaround: Configure access control lists (ACLs) on the supervisor engines that support them. On the switches that do not support ACLs, use an external device for access controlling HTTP traffic to the switch or disable the HTTP server on the switch. (CSCdw46637)

- Inserting a single-port OC-12 ATM module in a switch where all switching modules are fabric enabled causes the module diagnostics to fail on the ATM module. To put the ATM module into service, enter the **reset slot_number** command. (CSCds12349)
- The ToS byte remains unchanged in bridged multicast packets when you enable Multicast Multilayer Switching (MMLS). The system does not support multiple, different rewrites for a single packet. A Layer 3 rewrite is generated for multicast; there is no rewrite for the Layer 2 forwarding.

For example, you have a multicast source in VLAN 13, a receiver in the same VLAN, and a QoS IP ACL configured and mapped to the source's ingress port that matches the traffic flow and specifies DSCP 31. When you disable the MMLS feature, the IP packets captured on the receiver's port contain a ToS byte of x7C (the expected result). When you enable the MMLS feature and establish a Layer 3 flow, the captured packet's ToS byte is unchanged from the value sent by the source. A ToS rewrite occurs on the replicated packets in the outgoing VLANs (other than VLAN 13). No ToS rewrite occurs for the packets that are bridged in the same incoming VLAN. (CSCdm72364)

- With Supervisor Engine 720s, the second uplink ports of the active and standby Supervisor Engine 720s might not link up the first time that you boot the switch and change the media-type to RJ-45.

Workaround: Disable and enable the ports to bring the link up. (CSCeb48056)

- With the Supervisor Engine 720/MSFC3, the IGMP reports might not be sent to the MSFC3 ports when the MSFC3 is down. This problem might occur when the MSFC3 (both MSFC3s in a redundant system) is in ROMMON. When the MSFC3 is in ROMMON, IGMP snooping may not relay the IGMP reports to the external MSFC3 ports. (CSCin47303)
- On a port security enabled port, the auto-learned addresses are displayed in the **show config** output. If you enter the **write memory** command, these addresses should be written to the NVRAM, but the auto-learned addresses are not written to the NVRAM.

Workaround: If you want to retain the auto-learned addresses, enable the **set port security auto-configure** option. (CSCed46765)

Resolved Caveats in Software Release 8.1(1)

This section describes resolved caveats in supervisor engine software release 8.1(1):

- All VLANs come up in the “down” state after a Supervisor Engine 1 or Supervisor Engine 2 is reset/updated. This problem is seen when the following conditions are present:
 - The MSFC/MSFC2 is loaded from slot0: or disk0:
 - Single router mode (SRM) redundancy is enabled
 - Switches are running software release 7.5(1) or 7.6(1)

Workarounds:

- Load the MSFC/MSFC2 images from the MSFC/MSFC2 bootflash:
- After both MSFCs/MSFC2s come online, reset the active MSFC/MSFC2. The standby MSFC/MSFC2 will come up with the correct VLAN status.
- Do a shut/no shut on each VLAN interface on the active MSFC/MSFC2.

(CSCdy51093, CSCea72554)



Note The problems documented in caveats CSCdy51093 and CSCea72554 require software release 8.1(1) *and* one of the following bootloader images on the MSFC/MSFC2:

MSFC2 boot loader: c6msfc2-boot-mz.121-13.E10

MSFC boot loader: c6msfc-boot-mz.121-13.E10

- Running the TDR test on a 1-Gbps link gives the wrong cable length. This problem is resolved in software release 8.1(1). (CSCeb25429)
- The TDR test gives the wrong result and shows that a shorted cable has a status of “terminated” instead of “shorted.” This problem is resolved in software release 8.1(1). (CSCea90053)
- On a port that has port security enabled, a nonzero age time, a manually configured MAC address, and dynamically learned MAC addresses, when the age time expires, you will lose all the MAC addresses that you manually configured. This problem is resolved in software release 8.1(1). (CSCdy30515)
- A Catalyst 6500 series switch or Cisco 7600 series router, packets that are forwarded in hardware might have an incorrect source MAC or might be forwarded to an incorrect next-hop destination. This problem is resolved in software release 8.1(1). (CSCdy87433)

- The Content Switching Module (CSM) needs online diagnostics support. This problem is resolved in software release 8.1(1). Online diagnostics are available for the CSM but require CSM software release 3.2 and later. (CSCdy80144)
- Support is needed for changing the flow statistics timer for IP multicast. This problem is resolved in software release 8.1(1). (CSCdz71638)
- The TTL of 32 may decrement before the packets exit an MPLS network. This can cause problems with any IP-based application. This problem is resolved in software release 8.1(1). (CSCea48092)
- Some QoS ACL names may cause the system to fail to commit them to run time and will fail to clear them. For example, configuring and committing a QoS ACL named “ipphone” and then, a second ACL named “ipphone17-18” may cause this problem. As a consequence, the ACL named “ipphone17-18” will not be committed to run time and will not be cleared.

Workaround: Clear the first ACL (in the example, “ipphone”), clear the second ACL (in the example, “ipphone17-18”), and then reapply the first ACL (“ipphone”). Also avoid using number 1 after a letter in an ACL names.

This problem is resolved in software release 8.1(1). (CSCea18569)

- In a system with an MSFC2 and Multiple Spanning Tree (MST) configured, when a cable is disconnected and then reconnected, packets are not forwarded over the trunk. Although the output for the **show spantree mst** command may indicate that traffic is being forwarded, the ports remain in blocking mode. This problem is resolved in software release 8.1(1). (CSCea08501)
- When a Catalyst 6500 series switch is functioning as a distribution switch with two uplink ports to the core and UplinkFast is configured on the ports, a timing error may occur after a forwarding port goes down. If the first port goes down, traffic forwarding moves to the second uplink port, but if the second port goes down, the CAM table still points to the second port, which is still in blocking mode. It may take up to 20 seconds for the system to update the CAM table and start forwarding traffic. This problem is resolved in software release 8.1(1). (CSCdx45222)
- Support is needed for flow statistics sent from the route processor in response to the **show mls ip multicast stat group source** command. This problem is resolved in software release 8.1(1). (CSCdz71626)
- A WS-X6348 module port connected to a PC with a 60-meter cable may experience continuous link state changes. These changes occur when a PC has a NIC that does not conform to the IEEE 802.3 pulse shape mask for MLT3. This problem is resolved in software release 8.1(1). (CSCdz46928)
- The ciscoMemoryPoolUsed and ciscoMemoryPoolFree MIB objects report values for the NVRAM that are inconsistent with the **show version** command output. This problem is resolved in software release 8.1(1). (CSCea46369)
- Ports on the WS-X6148-GE-TX modules cannot be configured as VACL capture ports. This problem is resolved in software release 8.1(1). (CSCeb31718)
- In a redundant configuration, you might see the following messages:

```
2001 Nov 06 13:23:59 met +01:00 %SYS-2-MOD_NOINBANDRESPONSE:Module 2 not responding
over inband
```

```
2001 Nov 06 13:24:09 met +01:00%SYS-2-MOD_INBANDOK:Module 2 inband ok
```

These messages indicate that the active supervisor engine is polling the redundant supervisor engine but is not able to get a timely response. This problem may occur when a feature on the switch is incorrectly configured, and the destination host replies with excessive ICMP messages. These ICMP messages may interfere with the supervisor engine inband ping process. This problem is resolved in software release 8.1(1). (CSCdx03048)

Catalyst Software Image Upgrade Procedure

The high-availability image versioning feature allows you to perform a software upgrade with the minimal downtime associated with the high-availability feature. Compatibility between the software images is determined during the procedure in Step 12.

**Note**

Enable high-availability versioning only when upgrading Catalyst software. Implement image synchronization (high-availability versioning is disabled) for normal operating conditions.

Image versioning is supported in supervisor engine software releases 5.4(1) and later. Image versioning is not supported with images prior to release 5.4(1). Therefore, when you enable high-availability versioning, you can have active and standby supervisor engines run different images as long as both images are release 5.4(1) or later.

The high-availability versioning feature and Catalyst software upgrade should only be used when applying a maintenance release of Catalyst software. A maintenance release is a new version of software with incremental feature upgrades and bug fixes such as upgrading from software version 5.5.(1) to 5.5.(2). Major releases might not be high-availability compatible.

Versioning is feature dependent requiring that the high-availability feature is enabled in a dual supervisor engine configuration. Versioning allows different but compatible images to run on the active and standby supervisor engines, disabling the default supervisor engine image synchronization process. Versioning allows you to upgrade the supervisor engine software while the system is running using the stateful supervisor engine switchover of the high-availability feature.

You also have the ability to maintain a previously used and tested version of Catalyst software on the standby supervisor engine as a fallback if anything goes wrong with the software upgrade.

There are no restrictions as to which supervisor engine (active or standby) can be running a newer or older image version allowing you to upgrade or downgrade the Catalyst software images. However, the two versions of Catalyst software must be high-availability compatible to make possible a stateful software upgrade. The active and standby supervisor engines exchange image version information to determine if the two software images are compatible.

Image versions are defined to be one of three options: compatible, incompatible, or upgradable:

- Compatible versions support stateful protocol redundancy between the different images. All configuration settings made to the NVRAM on the active supervisor engine are sent to the standby supervisor engine. Two Catalyst software versions are incompatible if synchronizing the protocol state databases between the two versions is not possible.
- Incompatible software versions impact system operation because they require greater than a one to three second switchover time of a high-availability switchover and no NVRAM configuration changes are synchronized between supervisor engines in the software upgrade process.
- The upgradable option is a special case of incompatible versions. The high-availability supervisor engine switchover is not available, but configuration changes to the NVRAM on the active supervisor engine can be synchronized to the standby supervisor engine. Therefore, the option allows two different software versions to be run with synchronized configurations but without the ability for a high-availability failover.

If the Catalyst software images are not compatible, the high-availability switchover is not possible. The operation status output from the command **show system highavailability** should be monitored to determine the high-availability compatibility of two Catalyst software images. The operational status can either be **ON** or **OFF** (with some system specific status messages). The following shows that high availability is enabled and that the Catalyst software versions are high-availability compatible (**Operational status: ON**).

```
Console-A> (enable) show system highavailability
Highavailability: enabled
Highavailability versioning: enabled
Highavailability Operational-status: ON
```

Refer to Chapter 22, “Configuring Redundancy,” in the *Catalyst 6500 Series Switch Software Configuration Guide*.

**Caution**

You must follow these steps in this section exactly to successfully upgrade your system. Failure to follow these instructions exactly might result in an unusable system.

Perform these steps with the supervisor engine in slot 1 as the active supervisor engine and the supervisor engine in slot 2 in the standby mode:

**Note**

You must have a console connection available for both supervisor engines in this procedure.

Step 1 Disable the high-availability feature on the active supervisor engine:

```
Console_A> (enable) set system highavailability disable
System high availability disabled.
Console _A> (enable)
```



Note The high-availability feature is disabled by default.

Step 2 Load the new Catalyst software image into the bootflash (via slot0, disk0, TFTP, etc.) of the active supervisor engine only.

Note In the following steps, the software versions are shown as a variable (**x**). When performing these procedures, use the image numbers you are using for your system. For available software versions, see the “Orderable Software Images” section on page 24 of these release notes.

```
Console_A> (enable) copy slot0:cat6000-sup2.6-1-X.bin bootflash:cat6000-sup2.6-1-X.bin
5786532 bytes available on device bootflash, proceed (y/n) [n]? y
... display text truncated
Console_A> (enable)
```

Step 3 Verify that the new image is now located in the bootflash of the active supervisor engine.

```
Console_A> (enable) dir bootflash:
```

Step 4 Set the boot variable to boot the new image.

```
Console_A> (enable) set boot system flash bootflash:cat6000-sup2.6-1-X.bin prepend
```

Step 5 Synchronize the configuration files automatically to the standby supervisor engine.

```
Console_A> (enable) set boot sync now
```

Step 6 Verify that the new image is located on the standby supervisor engine and the boot variable is properly set.

```
Console_A> (enable) dir 2/bootflash:
Console_A> (enable) show boot 2
```

The new Catalyst software image is on both supervisor engines.

Step 7 Enable high-availability versioning on the active supervisor engine.

```
Console_A> (enable) set system highavailability versioning enable
```

Before the standby supervisor engine becomes active running the new software, you must enable high-availability versioning to allow the standby supervisor engine to reboot under the new version of Catalyst software while remaining the standby supervisor engine.



Note These upgrade procedures allow for a fallback plan using the old Catalyst software image if problems occur. The now-active supervisor engine must maintain that older image (even after an accidental reboot).

Step 8 Enable high-availability on the active supervisor engine.

```
Console_A> (enable) set system highavailability enable
```

Step 9 Change the boot variable on the active supervisor engine back to its original setting (this setting should still be stored in the bootflash):

```
Console_A> (enable) set boot system flash bootflash:cat6000-sup2.old.bin prepend
```



Note Because high-availability versioning is enabled, setting the boot variable on the active supervisor engine does not cause an image synchronization.

Step 10 Reset the standby supervisor engine.

```
Console_A> (enable) reset 2
This command will reset the system.
Do you want to continue (y/n) [n]? y
```

```
... display text truncated
Console_A> (enable)
```

The standby supervisor engine reboots with the new Catalyst software image. The standby supervisor engine remains the standby supervisor engine and does not affect the operation of the active supervisor engine.

Step 11 After the standby supervisor engine reboots, verify that the standby supervisor engine is running the new Catalyst software image.

```
Console_A> (enable) show module
```

The standby supervisor engine should show that the new software version is different from the active supervisor engine's software version.

Step 12 Verify that the two different Catalyst software images are high-availability compatible.

```
Console_A> (enable) show system highavailability
```

For the high-availability switchover to occur, it is critical that the operational status of high-availability is **ON**. If not, the system will be upgraded with a fast switchover (non-stateful) and the protocols will need to be restarted. This is the “Go, No-Go” decision point for continuing the upgrade.

If the Catalyst software images are not high-availability compatible, you cannot proceed with the upgrade. Individual modules might be compatible or incompatible and get reset (even during an otherwise high-availability switchover).

Step 13 Reset the active supervisor engine. Change the console connection to the supervisor engine in slot 2 (Sup-B) to maintain command line operation.

```
Console_A> (enable) reset 1
```

The standby supervisor engine takes over as the active supervisor engine (running the new software). The previously active supervisor engine is now rebooted as the new standby supervisor engine. The switchover should take under 3 seconds.

Step 14 Verify that the system is performing as expected. The supervisor engine in slot 2 is now the active supervisor engine running the new version of Catalyst software. The supervisor engine in slot 1 is now the standby supervisor engine running the old software version. The standby supervisor engine can be used as a fallback to revert to the old version of Catalyst software.

Step 15 If the system is operating as expected, then you must update the boot configuration on the standby supervisor engine (now, supervisor engine B) by disabling high-availability versioning on the new active supervisor engine, which automatically enables the image synchronization feature.

```
Console_B> (enable) set system highavailability versioning disable
```

Wait for the sync to occur before you reset.

```
Console_B> (enable) reset 1
```

This completes the Catalyst software upgrade procedure.

Troubleshooting

This section describes troubleshooting guidelines for the Catalyst 6500 series switch configuration and is divided into the following subsections:

- System Troubleshooting, page 153
- Module Troubleshooting, page 153
- VLAN Troubleshooting, page 154
- STP Troubleshooting, page 155



Note

Refer to the *Release Notes for Catalyst 6500 Series Switch Multilayer Switch Feature Card—Cisco IOS Release 12.0(3)XE* publication for information about how caveat CSCdm83559 affects the MLS feature. CSCdm83559 is resolved in Release 12.1(2)E.

System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the standby supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.
- After you download a new Flash image, the next reboot might take longer than normal if Erasable Programmable Logic Devices (EPLDs) on the supervisor engine need to be reprogrammed. Whether this happens depends on which software version was running on the supervisor engine before the download and which software version is downloaded. This can add up to 15 minutes to the normal reboot time.
- If you have a port whose port speed is set to **auto** connected to another port whose speed is set to a fixed value, configure the port whose speed is set to a fixed value for half duplex. Alternately, you can configure both ports to a fixed-value port speed and full duplex.

Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module, be sure to 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 6500 Series Switch Module Installation Guide*.
- The Catalyst 6500 series chassis has an EMI gasket on top of the frame member above the power supply, and each module has an EMI gasket on the top of its faceplate. (Blank slot covers also have EMI gaskets.) These EMI gaskets must contact the adjacent module to be effective. The EMI gasket is made from a flat spring material, folded and cut so that it looks like many parallel strips across the top of the faceplate.

When you insert a module, it must compress its own EMI gasket and the EMI gasket on the module below it. Some force is required to compress each EMI gasket. When a majority of the slots in any chassis are filled, the pressure from the EMI gaskets forces the modules toward empty slots, making insertion of the last module difficult. This effect can also cause the top of the faceplate to interfere slightly with the module above.

When assembling a system, use Solution 1. When replacing a module on an active system, use Solution 2.



Note In all cases, use proper ESD protection.

- Solution 1, when assembling a system:

Start from the top of the chassis and work toward the bottom. When inserting the last module, press the faceplate down approximately 1 mm (~.040”) when interference is encountered. Tighten all the thumb screws after the last card is inserted.

- Solution 2, when replacing or troubleshooting a module on an active switch:
 1. First, before removing any module, make sure the thumbscrews on all modules in the chassis are tight. This action will assure that the space for the module that is removed will be maintained. If the thumbscrews are not tightened, the EMI gaskets on the remaining modules will push them toward the open space created by removing the module, reducing the size of the space needed for the replacement module.
 2. Next, loosen the thumbscrews on the module to be removed and use the extractors to unseat the connectors. Remove the module and put it in an antistatic bag.
 3. Finally, open the extractors and insert the replacement module with a slight downward force against the top edge of the faceplate, deflecting it approximately 1 mm (~.040") when it engages the adjacent module. Once the extractors begin to close, use them to fully engage the connectors.
 4. Tighten the thumbscrews.
- If the switch detects a port-duplex misconfiguration, the misconfigured switch port is disabled and placed in the “errdisable” state. The following syslog message is reported to the console indicating that the misconfigured port has been disabled due to a late collision error:


```
SYS-3-PORT_COLL:Port 8/24 late collision (0) detected
%SYS-3-PORT_COLLDIS:Port 8/24 disabled due to collision
%PAGP-5-PORTFROMSTP:Port 8/24 left bridge port 8/24
```

Reconfigure the port-duplex setting and use the **set port enable** command to reenablen the port.
- Whenever you connect a port that is set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

VLAN Troubleshooting

This section contains troubleshooting guidelines for VLAN problems.



Note

Catalyst 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Catalyst 6500 series switches ship with ports in a nontrunking state and the Dynamic Trunking Protocol (DTP) feature in the **auto** mode. In this mode, if a port sees a DTP **on** or DTP **desired** frame, it transitions into the trunking state. Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For ports connected to non-Catalyst family devices in which trunking is not currently being used, configure Catalyst ports to **off** by entering the **set trunk mod_num/port_num off** command.
- When manually enabling trunking on a link to a Cisco router, use the **set trunk mod_num/port_num nonegotiate** command. The **nonegotiate** keyword transitions a link into trunking mode without sending DTP frames.

STP Troubleshooting

This section contains troubleshooting guidelines for spanning tree problems:

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



Note

With Supervisor Engine 720, spanning tree supports up to 2000 BPDUs per second. If that rate is exceeded, spanning tree starts dropping BPDUs which causes a reconvergence. In your network topology, you should make sure that a switch does not receive more than 2000 BPDUs per second (from all the links). Use the **show spantree statistics bpd** command to display all transmitted, received, processed, and dropped BPDUs. The system also displays the rate of these BPDUs in seconds. All BPDU counters give BPDU statistics from the last time that the counters were cleared or from the time that the system was booted up. Use the **clear spantree statistics bpd** command to clear the counters. After clearing the counters, if you still see the dropped BPDU counter going up, that is an indication of spanning tree instability.

Use the following guidelines to debug STP problems:



Note

For a given topology, MST converges faster than PVST+ and MISTP.

- On a Catalyst 6500 series switch with default STP parameters:
 - With Supervisor Engine 32 (WS-SUP32-GE-3B) configured for MST only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 74,000 (with or without the high-availability feature enabled).
 - With Supervisor Engine 32 (WS-SUP32-GE-3B) configured for MISTP only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 74,000 (with or without the high-availability feature enabled).
 - With Supervisor Engine 32 (WS-SUP32-GE-3B) configured for PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 11,000 (with or without the high-availability feature enabled).
 - With Supervisor Engine 32 (WS-SUP32-GE-3B) configured for Rapid-PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 11,000 (with or without the high-availability feature enabled).
 - With Supervisor Engine 32 (WS-SUP32-GE-3B) configured for MISTP-PVST+ with PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 5,000 (with or without the high-availability feature enabled).
 - With Supervisor Engine 720 configured for MST only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 130,000 (with or without the high-availability feature enabled).

- With Supervisor Engine 720 configured for MISTP only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 130,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 720 configured for PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 14,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 720 configured for Rapid-PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 15,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 2 configured for MST only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 127,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 2 configured for MISTP only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 127,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 2 configured for PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 14,000 (with or without the high-availability feature enabled).
- With Supervisor Engine 2 configured for Rapid-PVST+ only, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 14,000 (with or without the high-availability feature enabled).



Note For Supervisor Engine 2 running Rapid-PVST+ in a combined Catalyst 6000/Catalyst 4000 network with the Catalyst 4000 switch in the leaf, the maximum supported instances is 7,000 instead of 14,000.

- With Supervisor Engine 2 configured for MISTP-PVST+ with PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 8,000 (with or without the high-availability feature enabled).
- With software release 8.x you need 128-MB DRAM for Supervisor Engine 1. For upgrade information, see the “Release 8.x DRAM Memory Requirements” section on page 3.
- With Supervisor Engine 1 configured for MISTP only and with the high-availability feature enabled, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 35,000 (28,000 without high availability).
- With Supervisor Engine 1 configured for MST only and with the high-availability feature enabled, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 40,000 (32,000 without high availability).
- With Supervisor Engine 1 configured for PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 2000 (with or without the high-availability feature enabled).
- With Supervisor Engine 1 configured for MISTP-PVST+ with PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 1600 (with or without the high-availability feature enabled).
- With Supervisor Engine 1 configured for Rapid-PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 2000 (with or without the high-availability feature enabled).

The sum of all logical ports equals the number of trunks on the switch times the number of active VLANs on the trunks, plus the number of nontrunking ports on the switch.



Caution

Lowering the values of any STP timers reduces the number of STP instances that can be supported. When numerous protocol features (such as VTP pruning, Fast EtherChannel, and RMON) are enabled concurrently, the number of supported logical spanning tree ports are reduced. Also, to achieve these numbers, we recommend that you keep switched traffic off the management VLAN.

- After a switchover from the active to the standby supervisor engine, the uplink ports on the standby supervisor engine take longer to come up than other switch ports.
- Keep track of all blocked spanning tree ports in each switch in your network. For each of the blocked spanning tree ports, keep track of the output of the following commands:
 - **show port**—Check to see if the port has registered a lot of alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs.
 - **show mac**—If the Inlost counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.
- On trunk ports, make sure that the trunk configuration is set properly on both sides of the link.
- On trunk ports, make sure that the duplex is set to full on both sides of the link to prevent any collisions under heavy traffic conditions.

Additional Documentation

The following documents are available for the Catalyst 6500 series switches:

- *Catalyst 6500 Series Switch Quick Software Configuration*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series Switch System Message Guide*
- *ATM Configuration Guide and Command Reference*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
 Attn: Customer Document Ordering
 170 West Tasman Drive
 San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “Additional Documentation” section on page 157.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Copyright © 2001–2005, Cisco Systems, Inc.
All rights reserved. Printed in USA.