Release Notes for Catalyst 6000 Family Software Release 6.*x*

Current Release
6.4(21)—February 20, 2006
Previous Releases: 6.4(20), 6.4(19), 6.4(18), 6.4(17), 6.4(16), 6.4(15), 6.4(14), 6.4(13), 6.4(12), 6.4(11), 6.4(10), 6.4(9), 6.4(8), 6.4(7), 6.4(6a), 6.4(6), 6.4(5b), 6.4(5a), 6.4(5), 6.4(4a), 6.4(4), 6.4(3) - GD release, 6.4(2), 6.4(1), 6.3(10), 6.3(9), 6.3(8), 6.3(7), 6.3(6), 6.3(5), 6.3(4a), 6.3(4), 6.3(3)x1, 6.3(3)x, 6.3(3a), 6.3(3), 6.3(2a), 6.3(2), 6.3(1a), 6.3(1), 6.2(3a), 6.2(3), 6.2(2a), 6.2(2), 6.1(4b), 6.1(4), 6.1(3a), 6.1(3), 6.1(2a), 6.1(2), 6.1(1e), 6.1(1d), 6.1(1c), 6.1(1b), 6.1(1a)

Note For information on the latest caveats and updates for the Cisco 7600 series router, refer to the Cisco IOS Release 12.1(7a)E1 or later MSFC release notes at this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm

Note Release notes for prior Catalyst 6000 family software releases were accurate at the time of release. However, for information on the latest caveats and updates to previously released Catalyst 6000 family software releases, refer to the release notes for the latest maintenance release in your software release train. You can access all Catalyst 6000 family release notes at the World Wide Web locations listed in the "Obtaining Documentation" section on page 205.

Contents

This document consists of these sections:

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

Release 6.*x* DRAM Memory Requirements

The Catalyst 6000 family Supervisor Engine 2 ships with 128-MB DRAM, which fully supports software release 6.*x*.

The Catalyst 6000 family Supervisor Engine 1 ships with 64-MB DRAM, which fully supports software release 6.*x*.

Boot ROM 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) and later is 5.2(1). The default (shipping) image for software releases 6.x(x) and later is 5.3(1).

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

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

Upgrading the Boot ROM

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

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

- 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 6000 Family Supervisor Engine NMP Boot ROM Upgrade Installation Note* at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_10142.htm

Flash PC Card Support

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

- MEM-C6K-FLC16M(=)
- MEM-C6K-FLC24M(=)
- MEM-C6K-FLC64M(=)
- 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 release 7.5(1) and later releases, 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.

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 Cisco 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, you can put the MSFC2 bootloader and Cisco IOS image on the MSFC2 bootflash, and the Catalyst image can be put on the 24-MB or 64-MB linear Flash PC cards.

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:

- 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

These configuration requirements apply to all Catalyst 6000 family switches. We do not support configurations that are not identical.

Product and Software Version Matrix

Table 1 lists the minimum supervisor engine version and the current recommended/default supervisor engine software version for Catalyst 6000 family modules and chassis.

Note For information about AC power requirements and heat dissipation, refer to the "Power Requirements" section in Chapter 2, "Preparing for Installation," of the *Catalyst 6000 Family Installation Guide*: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/6000hw/index.htm

For information about power management and determining system power requirements, refer to the "Power Management" section in Chapter 20, "Administering the Switch," of the *Catalyst 6000 Family Software Configuration Guide*: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/index.htm

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.

Table 1 Minimum and Recommended Supervisor Engine Software Versions

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended Supervisor 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 1[1]			
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	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.3(1a)CSX	6.4(11)
WS-X6K-SUP1-2GE	Supervisor Engine 1, dual 1000BASE-X GBIC uplinks QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	6.4(11)
Switch Fabric Module			
WS-C6500-SFM	Switch Fabric Module to support fabric-enabled modules	6.1(1d)	6.4(11)
WS-X6500-SFM 2	Switch Fabric Module version 2	6.2(2)	6.4(11)
Gigabit Ethernet Switching Modules			
WS-X6516-GBIC[2]	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)

Table 1 Minimum and Recommended Supervisor Engine Software Versions (continued)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended Supervisor Software Version
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)
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)
Fast Ethernet Switching Modules			
WS-X6324-100FX-SM WS-X6324-100FX-MM	24-port 100FX 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 100FX Multimode MT-RJ QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	6.4(11)
Ethernet/Fast Ethernet (10/100) Switching Modules			
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**	6.4(1)	6.4(11)
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**	6.4(1)	6.4(11)
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)

Table 1 Minimum and Recommended Supervisor Engine Software Versions (continued)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended Supervisor Software Version
WS-F6K-VPWR	Inline-power field-upgrade module for the 48-port 10/100BASE-TX RJ-45 and RJ-21 modules	5.5(1)	6.4(11)
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			
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			
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)
FlexWan Module[3]			
WS-X6182-2PA	FlexWAN Module	5.4(2)	6.4(11)
Intrusion Detection System Module[4]			
WS-X6381-IDS	Intrusion Detection System Module	6.1(1d)	6.4(11)
Network Analysis Module[5, 6]			
WS-X6380-NAM	Network Analysis Module	5.5(1)	6.4(11)
ATM[7]			
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)
Multilayer Switch Module (MSM)[8]			
WS-X6302-MSM	Multilayer Switch Module	5.2(1)CSX	6.4(11)
Optical Services Module[9]			
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 SONET[10]			
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[11], with 4 Gigabit Ethernet ports	6.1(2)	6.4(11)

Table 1 Minimum and Recommended Supervisor Engine Software Versions (continued)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended Supervisor Software Version
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 SONET[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)
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 SONET[9]			
OSM-1OC48-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-1OC48-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-1OC48-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)
Power Supplies			
WS-CAC-1000W	1000W AC power supply	5.1(1)CSX	6.4(11)
WS-CAC-1300W	1300W AC power supply	5.1(1)CSX	6.4(11)
WS-CDC-1300W	1300W DC power supply	5.1(1)CSX	6.4(11)
WS-CAC-2500W	2500W AC power supply	5.4(2)	6.4(11)
WS-CDC-2500W	2500W DC power supply	5.4(2)	6.4(11)
WS-CAC-4000W	4000W AC power supply	6.1(3)	6.4(11)

Table 1 Minimum and Recommended Supervisor Engine Software Versions (continued)

Product Number append with "=" for spares	Product Description	Minimum Supervisor Software Version	Recommended Supervisor Software Version
Modular Chassis			
WS-C6513	Catalyst 6513 chassis: • 13 slots • 64 chassis MAC addresses • Supported only with Supervisor Engine 2	6.2(2)	6.4(11)
WS-C6509	Catalyst 6509 chassis: • 9 slots • 1024 chassis MAC addresses	5.1(1)CSX	6.4(11)
WS-C6509-NEB	Catalyst 6509-NEB chassis: • 9 vertical slots • 1024 chassis MAC addresses	5.4(2)	6.4(11)
WS-C6009	Catalyst 6009 chassis: • 9 slots • 1024 chassis MAC addresses	5.1(1)CSX	6.4(11)
WS-C6506	Catalyst 6506 chassis: • 6 slots • 1024 chassis MAC addresses	5.2(1)CSX	6.4(11)
WS-C6006	Catalyst 6006 chassis: • 6 slots • 1024 chassis MAC addresses	5.2(1)CSX	6.4(11)
OSR-7609-AC, -DC	Cisco 7609 router chassis: • 9 vertical slots • 1024 chassis MAC addresses • Supported only with Supervisor Engine 2	6.1(1b)	6.4(11)

1. Not supported in the WS-C6513 chassis.
2. The WS-X6516A-GBIC version of this module is not supported in software release 6.x. The WS-X6516A-GBIC version is supported in software release 7.5(1).
3. Refer to the *Catalyst 6000 Family FlexWAN Module Installation and Configuration Note.*
4. Refer to the *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note*.
5. Refer to the *Network Analysis Module Installation and Configuration Note.*
6. 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.
7. Refer to the *ATM Configuration Guide and Command Reference.*
8. Refer to the *Multilayer Switch Module Release Notes.*
9. Refer to the *Optical Services Module Installation and Configuration Note.*
10. Also has four Layer 2 Gigabit Ethernet ports.
11. Single-mode, long reach.

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the Catalyst 6000 family 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.

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

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number[1]
Supervisor Engine 2		
6.4(21) Flash image	cat6000-sup2.6-4-21.bin	SC6K-SUP2-6.4
6.4(21) Flash image (CiscoView)	cat6000-sup2cv.6-4-21.bin	SC6K-SUP2CV-6.4
6.4(21) Flash image (Secure Shell)	cat6000-sup2k9.6-4-21.bin	SC6K-SUP2K9-6.4
6.4(21) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-21.bin	SC6K-SUP2CVK9-6.4
6.4(20) Flash image	cat6000-sup2.6-4-20.bin	SC6K-SUP2-6.4
6.4(20) Flash image (CiscoView)	cat6000-sup2cv.6-4-20.bin	SC6K-SUP2CV-6.4
6.4(20) Flash image (Secure Shell)	cat6000-sup2k9.6-4-20.bin	SC6K-SUP2K9-6.4
6.4(20) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-20.bin	SC6K-SUP2CVK9-6.4
6.4(19) Flash image	cat6000-sup2.6-4-19.bin	SC6K-SUP2-6.4
6.4(19) Flash image (CiscoView)	cat6000-sup2cv.6-4-19.bin	SC6K-SUP2CV-6.4
6.4(19) Flash image (Secure Shell)	cat6000-sup2k9.6-4-19.bin	SC6K-SUP2K9-6.4
6.4(19) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-19.bin	SC6K-SUP2CVK9-6.4
6.4(18) Flash image	cat6000-sup2.6-4-18.bin	SC6K-SUP2-6.4
6.4(18) Flash image (CiscoView)	cat6000-sup2cv.6-4-18.bin	SC6K-SUP2CV-6.4
6.4(18) Flash image (Secure Shell)	cat6000-sup2k9.6-4-18.bin	SC6K-SUP2K9-6.4
6.4(18) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-18.bin	SC6K-SUP2CVK9-6.4
6.4(17) Flash image	cat6000-sup2.6-4-17.bin	SC6K-SUP2-6.4
6.4(17) Flash image (CiscoView)	cat6000-sup2cv.6-4-17.bin	SC6K-SUP2CV-6.4
6.4(17) Flash image (Secure Shell)	cat6000-sup2k9.6-4-17.bin	SC6K-SUP2K9-6.4
6.4(17) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-17.bin	SC6K-SUP2CVK9-6.4
6.4(16) Flash image	cat6000-sup2.6-4-16.bin	SC6K-SUP2-6.4
6.4(16) Flash image (CiscoView)	cat6000-sup2cv.6-4-16.bin	SC6K-SUP2CV-6.4
6.4(16) Flash image (Secure Shell)	cat6000-sup2k9.6-4-16.bin	SC6K-SUP2K9-6.4

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(16) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-16.bin	SC6K-SUP2CVK9-6.4
6.4(15) Flash image	cat6000-sup2.6-4-15.bin	SC6K-SUP2-6.4
6.4(15) Flash image (CiscoView)	cat6000-sup2cv.6-4-15.bin	SC6K-SUP2CV-6.4
6.4(15) Flash image (Secure Shell)	cat6000-sup2k9.6-4-15.bin	SC6K-SUP2K9-6.4
6.4(15) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-15.bin	SC6K-SUP2CVK9-6.4
6.4(14) Flash image	cat6000-sup2.6-4-14.bin	SC6K-SUP2-6.4
6.4(14) Flash image (CiscoView)	cat6000-sup2cv.6-4-14.bin	SC6K-SUP2CV-6.4
6.4(14) Flash image (Secure Shell)	cat6000-sup2k9.6-4-14.bin	SC6K-SUP2K9-6.4
6.4(14) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-14.bin	SC6K-SUP2CVK9-6.4
6.4(13) Flash image	cat6000-sup2.6-4-13.bin	SC6K-SUP2-6.4
6.4(13) Flash image (CiscoView)	cat6000-sup2cv.6-4-13.bin	SC6K-SUP2CV-6.4
6.4(13) Flash image (Secure Shell)	cat6000-sup2k9.6-4-13.bin	SC6K-SUP2K9-6.4
6.4(13) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-13.bin	SC6K-SUP2CVK9-6.4
6.4(12) Flash image	cat6000-sup2.6-4-12.bin	SC6K-SUP2-6.4
6.4(12) Flash image (CiscoView)	cat6000-sup2cv.6-4-12.bin	SC6K-SUP2CV-6.4
6.4(12) Flash image (Secure Shell)	cat6000-sup2k9.6-4-12.bin	SC6K-SUP2K9-6.4
6.4(12) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-12.bin	SC6K-SUP2CVK9-6.4
6.4(11) Flash image	cat6000-sup2.6-4-11.bin	SC6K-SUP2-6.4
6.4(11) Flash image (CiscoView)	cat6000-sup2cv.6-4-11.bin	SC6K-SUP2CV-6.4
6.4(11) Flash image (Secure Shell)	cat6000-sup2k9.6-4-11.bin	SC6K-SUP2K9-6.4
6.4(11) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-11.bin	SC6K-SUP2CVK9-6.4
6.4(10) Flash image	cat6000-sup2.6-4-10.bin	SC6K-SUP2-6.4
6.4(10) Flash image (CiscoView)	cat6000-sup2cv.6-4-10.bin	SC6K-SUP2CV-6.4
6.4(10) Flash image (Secure Shell)	cat6000-sup2k9.6-4-10.bin	SC6K-SUP2K9-6.4
6.4(10) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-10.bin	SC6K-SUP2CVK9-6.4
6.4(9) Flash image	cat6000-sup2.6-4-9.bin	SC6K-SUP2-6.4
6.4(9) Flash image (CiscoView)	cat6000-sup2cv.6-4-9.bin	SC6K-SUP2CV-6.4
6.4(9) Flash image (Secure Shell)	cat6000-sup2k9.6-4-9.bin	SC6K-SUP2K9-6.4
6.4(9) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-9.bin	SC6K-SUP2CVK9-6.4
6.4(8) Flash image	cat6000-sup2.6-4-8.bin	SC6K-SUP2-6.4
6.4(8) Flash image (CiscoView)	cat6000-sup2cv.6-4-8.bin	SC6K-SUP2CV-6.4
6.4(8) Flash image (Secure Shell)	cat6000-sup2k9.6-4-8.bin	SC6K-SUP2K9-6.4
6.4(8) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-8.bin	SC6K-SUP2CVK9-6.4
6.4(7) Flash image	cat6000-sup2.6-4-7.bin	SC6K-SUP2-6.4
6.4(7) Flash image (CiscoView)	cat6000-sup2cv.6-4-7.bin	SC6K-SUP2CV-6.4
6.4(7) Flash image (Secure Shell)	cat6000-sup2k9.6-4-7.bin	SC6K-SUP2K9-6.4

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(7) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-7.bin	SC6K-SUP2CVK9-6.4
6.4(6a) Flash image	cat6000-sup2.6-4-6a.bin	SC6K-SUP2-6.4
6.4(6a) Flash image (CiscoView)	cat6000-sup2cv.6-4-6a.bin	SC6K-SUP2CV-6.4
6.4(6a) Flash image (Secure Shell)	cat6000-sup2k9.6-4-6a.bin	SC6K-SUP2K9-6.4
6.4(6a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-6a.bin	SC6K-SUP2CVK9-6.4
6.4(6) Flash image	cat6000-sup2.6-4-6.bin	SC6K-SUP2-6.4
6.4(6) Flash image (CiscoView)	cat6000-sup2cv.6-4-6.bin	SC6K-SUP2CV-6.4
6.4(6) Flash image (Secure Shell)	cat6000-sup2k9.6-4-6.bin	SC6K-SUP2K9-6.4
6.4(6) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-6.bin	SC6K-SUP2CVK9-6.4
6.4(5b) Flash image	cat6000-sup2.6-4-5b.bin	SC6K-SUP2-6.4
6.4(5b) Flash image (Secure Shell)	cat6000-sup2k9.6-4-5b.bin	SC6K-SUP2K9-6.4
6.4(5a) Flash image	cat6000-sup2.6-4-5a.bin	SC6K-SUP2-6.4
6.4(5a) Flash image (Secure Shell)	cat6000-sup2k9.6-4-5a.bin	SC6K-SUP2K9-6.4
6.4(5) Flash image	cat6000-sup2.6-4-5.bin	SC6K-SUP2-6.4
6.4(5) Flash image (CiscoView)	cat6000-sup2cv.6-4-5.bin	SC6K-SUP2CV-6.4
6.4(5) Flash image (Secure Shell)	cat6000-sup2k9.6-4-5.bin	SC6K-SUP2K9-6.4
6.4(5) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-5.bin	SC6K-SUP2CVK9-6.4
6.4(4a) Flash image	cat6000-sup2.6-4-4a.bin	SC6K-SUP2-6.4.4a
6.4(4a) Flash image (CiscoView)	cat6000-sup2cv.6-4-4a.bin	SC6K-SUP2CV-6.4.4a
6.4(4a) Flash image (Secure Shell)	cat6000-sup2k9.6-4-4a.bin	SC6K-SUP2K9-6.4.4a
6.4(4a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-4a.bin	SC6K-SUP2CVK9-6.4.4a
6.4(4) Flash image	cat6000-sup2.6-4-4.bin	SC6K-SUP2-6.4.4
6.4(4) Flash image (CiscoView)	cat6000-sup2cv.6-4-4.bin	SC6K-SUP2CV-6.4.4
6.4(4) Flash image (Secure Shell)	cat6000-sup2k9.6-4-4.bin	SC6K-SUP2K9-6.4.4
6.4(4) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-4.bin	SC6K-SUP2CVK9-6.4.4
6.4(3) Flash image	cat6000-sup2.6-4-3.bin	SC6K-SUP2-6.4.3
6.4(3) Flash image (CiscoView)	cat6000-sup2cv.6-4-3.bin	SC6K-SUP2CV-6.4.3
6.4(3) Flash image (Secure Shell)	cat6000-sup2k9.6-4-3.bin	SC6K-SUP2K9-6.4.3
6.4(3) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-3.bin	SC6K-SUP2CVK9-6.4.3
6.4(2) Flash image	cat6000-sup2.6-4-2.bin	SC6K-SUP2-6.4.2
6.4(2) Flash image (CiscoView)	cat6000-sup2cv.6-4-2.bin	SC6K-SUP2CV-6.4.2
6.4(2) Flash image (Secure Shell)	cat6000-sup2k9.6-4-2.bin	SC6K-SUP2K9-6.4.2
6.4(2) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-2.bin	SC6K-SUP2CVK9-6.4.2
6.4(1) Flash image	cat6000-sup2.6-4-1.bin	SC6K-SUP2-6.4.1
6.4(1) Flash image (CiscoView)	cat6000-sup2cv.6-4-1.bin	SC6K-SUP2CV-6.4.1
6.4(1) Flash image (Secure Shell)	cat6000-sup2k9.6-4-1.bin	SC6K-SUP2K9-6.4.1

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(1) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-4-1.bin	SC6K-SUP2CVK9-6.4.1
6.3(10) Flash image	cat6000-sup2.6-3-10.bin	SC6K-SUP2-6.3.10
6.3(10) Flash image (CiscoView)	cat6000-sup2cv.6-3-10.bin	SC6K-SUP2CV-6.3.10
6.3(10) Flash image (Secure Shell)	cat6000-sup2k9.6-3-10.bin	SC6K-SUP2K9-6.3.10
6.3(10) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-10.bin	SC6K-SUP2CVK9-6.3.10
6.3(9) Flash image	cat6000-sup2.6-3-9.bin	SC6K-SUP2-6.3.9
6.3(9) Flash image (CiscoView)	cat6000-sup2cv.6-3-9.bin	SC6K-SUP2CV-6.3.9
6.3(9) Flash image (Secure Shell)	cat6000-sup2k9.6-3-9.bin	SC6K-SUP2K9-6.3.9
6.3(9) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-9.bin	SC6K-SUP2CVK9-6.3.9
6.3(8) Flash image	cat6000-sup2.6-3-8.bin	SC6K-SUP2-6.3.8
6.3(8) Flash image (CiscoView)	cat6000-sup2cv.6-3-8.bin	SC6K-SUP2CV-6.3.8
6.3(8) Flash image (Secure Shell)	cat6000-sup2k9.6-3-8.bin	SC6K-SUP2K9-6.3.8
6.3(8) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-8.bin	SC6K-SUP2CVK9-6.3.8
6.3(7) Flash image	cat6000-sup2.6-3-7.bin	SC6K-SUP2-6.3.7
6.3(7) Flash image (CiscoView)	cat6000-sup2cv.6-3-7.bin	SC6K-SUP2CV-6.3.7
6.3(7) Flash image (Secure Shell)	cat6000-sup2k9.6-3-7.bin	SC6K-SUP2K9-6.3.7
6.3(7) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-7.bin	SC6K-SUP2CVK9-6.3.7
6.3(6) Flash image	cat6000-sup2.6-3-6.bin	SC6K-SUP2-6.3.6
6.3(6) Flash image (CiscoView)	cat6000-sup2cv.6-3-6.bin	SC6K-SUP2CV-6.3.6
6.3(6) Flash image (Secure Shell)	cat6000-sup2k9.6-3-6.bin	SC6K-SUP2K9-6.3.6
6.3(6) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-6.bin	SC6K-SUP2CVK9-6.3.6
6.3(5) Flash image	cat6000-sup2.6-3-5.bin	SC6K-SUP2-6.3.5
6.3(5) Flash image (CiscoView)	cat6000-sup2cv.6-3-5.bin	SC6K-SUP2CV-6.3.5
6.3(5) Flash image (Secure Shell)	cat6000-sup2k9.6-3-5.bin	SC6K-SUP2K9-6.3.5
6.3(5) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-5.bin	SC6K-SUP2CVK9-6.3.5
6.3(4a) Flash image	cat6000-sup2.6-3-4a.bin	SC6K-SUP2-6.3.4a
6.3(4a) Flash image (CiscoView)	cat6000-sup2cv.6-3-4a.bin	SC6K-SUP2CV-6.3.4a
6.3(4a) Flash image (Secure Shell)	cat6000-sup2k9.6-3-4a.bin	SC6K-SUP2K9-6.3.4a
6.3(4a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-4a.bin	SC6K-SUP2CVK9-6.3.4a
6.3(4) Flash image	cat6000-sup2.6-3-4.bin	SC6K-SUP2-6.3.4
6.3(4) Flash image (CiscoView)	cat6000-sup2cv.6-3-4.bin	SC6K-SUP2CV-6.3.4
6.3(4) Flash image (Secure Shell)	cat6000-sup2k9.6-3-4.bin	SC6K-SUP2K9-6.3.4
6.3(4) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-4.bin	SC6K-SUP2CVK9-6.3.4
6.3(3)x1 Flash image	cat6000-sup2.6-3-3X1.bin	SC6K-SUP2-6.3.3X1
6.3(3)x Flash image	cat6000-sup2.6-3-3X.bin	SC6K-SUP2-6.3.3X
6.3(3a) Flash image	cat6000-sup2.6-3-3a.bin	SC6K-SUP2-6.3.3a

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.3(3a) Flash image (CiscoView)	cat6000-sup2cv.6-3-3a.bin	SC6K-SUP2CV-6.3.3a
6.3(3a) Flash image (Secure Shell)	cat6000-sup2k9.6-3-3a.bin	SC6K-SUP2K9-6.3.3a
6.3(3a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-3a.bin	SC6K-SUP2CVK9-6.3.3a
6.3(3) Flash image	cat6000-sup2.6-3-3.bin	SC6K-SUP2-6.3.3
6.3(3) Flash image (CiscoView)	cat6000-sup2cv.6-3-3.bin	SC6K-SUP2CV-6.3.3
6.3(3) Flash image (Secure Shell)	cat6000-sup2k9.6-3-3.bin	SC6K-SUP2K9-6.3.3
6.3(3) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-3.bin	SC6K-SUP2CVK9-6.3.3
6.3(2a) Flash image	cat6000-sup2.6-3-2a.bin	SC6K-SUP2-6.3.2a
6.3(2a) Flash image (CiscoView)	cat6000-sup2cv.6-3-2a.bin	SC6K-SUP2CV-6.3.2a
6.3(2a) Flash image (Secure Shell)	cat6000-sup2k9.6-3-2a.bin	SC6K-SUP2K9-6.3.2a
6.3(2a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-2a.bin	SC6K-SUP2CVK9-6.3.2a
6.3(2) Flash image	cat6000-sup2.6-3-2.bin	SC6K-SUP2-6.3.2
6.3(2) Flash image (CiscoView)	cat6000-sup2cv.6-3-2.bin	SC6K-SUP2CV-6.3.2
6.3(2) Flash image (Secure Shell)	cat6000-sup2k9.6-3-2.bin	SC6K-SUP2K9-6.3.2
6.3(2) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-2.bin	SC6K-SUP2CVK9-6.3.2
6.3(1a) Flash image	cat6000-sup2.6-3-1a.bin	SC6K-SUP2-6.3.1a
6.3(1a) Flash image (Secure Shell)	cat6000-sup2k9.6-3-1a.bin	SC6K-SUP2K9-6.3.1a
6.3(1) Flash image	cat6000-sup2.6-3-1.bin	SC6K-SUP2-6.3.1
6.3(1) Flash image (CiscoView)	cat6000-sup2cv.6-3-1.bin	SC6K-SUP2CV-6.3.1
6.3(1) Flash image (Secure Shell)	cat6000-sup2k9.6-3-1.bin	SC6K-SUP2K9-6.3.1
6.3(1) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-3-1.bin	SC6K-SUP2CVK9-6.3.1
6.2(3a) Flash image	cat6000-sup2.6-2-3a.bin	SC6K-SUP2-6.2.3a
6.2(3a) Flash image (Secure Shell)	cat6000-sup2k9.6-2-3a.bin	SC6K-SUP2K9-6.2.3a
6.2(3) Flash image	cat6000-sup2.6-2-3.bin	SC6K-SUP2-6.2.3
6.2(3) Flash image (CiscoView)	cat6000-sup2cv.6-2-3.bin	SC6K-SUP2CV-6.2.3
6.2(3) Flash image (Secure Shell)	cat6000-sup2k9.6-2-3.bin	SC6K-SUP2K9-6.2.3
6.2(3) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-2-3.bin	SC6K-SUP2CVK9-6.2.3
6.2(2a) Flash image	cat6000-sup2.6-2-2a.bin	SC6K-SUP2-6.2.2a
6.2(2a) Flash image (CiscoView)	cat6000-sup2cv.6-2-2a.bin	SC6K-SUP2CV-6.2.2a
6.2(2a) Flash image (Secure Shell)	cat6000-sup2k9.6-2-2a.bin	SC6K-SUP2K9-6.2.2a
6.2(2a) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-2-2a.bin	SC6K-SUP2CVK9-6.2.2a
6.2(2) Flash image	cat6000-sup2.6-2-2.bin	SC6K-SUP2-6.2.2
6.2(2) Flash image (CiscoView)	cat6000-sup2cv.6-2-2.bin	SC6K-SUP2CV-6.2.2
6.2(2) Flash image (Secure Shell)	cat6000-sup2k9.6-2-2.bin	SC6K-SUP2K9-6.1.4
6.2(2) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-2-2.bin	SC6K-SUP2CVK9-6.2.2
6.1(4b) Flash image	cat6000-sup2.6-1-4b.bin	SC6K-SUP2-6.1.4b

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.1(4b) Flash image (Secure Shell)	cat6000-sup2k9.6-1-4b.bin	SC6K-SUP2K9-6.1.4b
6.1(4) Flash image	cat6000-sup2.6-1-4.bin	SC6K-SUP2-6.1.4
6.1(4) Flash image (CiscoView)	cat6000-sup2cv.6-1-4.bin	SC6K-SUP2CV-6.1.4
6.1(4) Flash image (Secure Shell)	cat6000-sup2k9.6-1-4.bin	SC6K-SUP2K9-6.1.4
6.1(4) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-4.bin	SC6K-SUP2CVK9-6.1.4
6.1(3a) Flash image	cat6000-sup2.6-1-3a.bin	SC6K-SUP2-6.1.3a
6.1(3a) Flash image (Secure Shell)	cat6000-sup2k9.6-1-3a.bin	SC6K-SUP2K9-6.1.3a
6.1(3) Flash image	cat6000-sup2.6-1-3.bin	SC6K-SUP2-6.1.3
6.1(3) Flash image (CiscoView)	cat6000-sup2cv.6-1-3.bin	SC6K-SUP2CV-6.1.3
6.1(3) Flash image (Secure Shell)	cat6000-sup2k9.6-1-3.bin	SC6K-SUP2K9-6.1.3
6.1(3) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-3.bin	SC6K-SUP2CVK9-6.1.3
6.1(2a) Flash image	cat6000-sup2.6-1-2a.bin	SC6K-SUP2-6.1.2a
6.1(2a) Flash image (Secure Shell)	cat6000-sup2k9.6-1-2a.bin	SC6K-SUP2K9-6.1.2a
6.1(2) Flash image	cat6000-sup2.6-1-2.bin	SC6K-SUP2-6.1.2
6.1(2) Flash image (CiscoView)	cat6000-sup2cv.6-1-2.bin	SC6K-SUP2CV-6.1.2
6.1(2) Flash image (Secure Shell)	cat6000-sup2k9.6-1-2.bin	SC6K-SUP2K9-6.1.2
6.1(2) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-2.bin	SC6K-SUP2CVK9-6.1.2
6.1(1e) Flash image	cat6000-sup2.6-1-1e.bin	SC6K-SUP2-6.1.1e
6.1(1e) Flash image (Secure Shell)	cat6000-sup2k9.6-1-1e.bin	SC6K-SUP2K9-6.1.1e
6.1(1d) Flash image	cat6000-sup2.6-1-1d.bin	SC6K-SUP2-6.1.1
6.1(1d) Flash image (CiscoView)	cat6000-sup2cv.6-1-1d.bin	SC6K-SUP2CV-6.1.1
6.1(1d) Flash image (Secure Shell)	cat6000-sup2k9.6-1-1d.bin	SC6K-SUP2K9-6.1.1
6.1(1d) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-1d.bin	SC6K-SUP2CVK9-6.1.1
6.1(1c) Flash image (Secure Shell)	cat6000-sup2k9.6-1-1c.bin	not orderable
6.1(1c) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-1c.bin	not orderable
6.1(1b) Flash image	cat6000-sup2.6-1-1b.bin	not orderable
6.1(1b) Flash image (CiscoView)	cat6000-sup2cv.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell)	cat6000-sup2k9.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell and CiscoView)	cat6000-sup2cvk9.6-1-1b.bin	not orderable
6.1(1a) Flash image	cat6000-sup2.6-1-1a.bin	not orderable
6.1(1a) Flash image (CiscoView)	cat6000-sup2cv.6-1-1a.bin	not orderable
Supervisor Engine 1		
6.4(21) Flash image	cat6000-sup.6-4-21.bin	SC6K-SUP-6.4
6.4(21) Flash image (CiscoView)	cat6000-supcv.6-4-21.bin	SC6K-SUPCV-6.4
6.4(21) Flash image (Secure Shell)	cat6000-supk9.6-4-21.bin	SC6K-SUPK9-6.4
6.4(21) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-21.bin	SC6K-SUPCVK9-6.4

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(20) Flash image	cat6000-sup.6-4-20.bin	SC6K-SUP-6.4
6.4(20) Flash image (CiscoView)	cat6000-supcv.6-4-20.bin	SC6K-SUPCV-6.4
6.4(20) Flash image (Secure Shell)	cat6000-supk9.6-4-20.bin	SC6K-SUPK9-6.4
6.4(20) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-20.bin	SC6K-SUPCVK9-6.4
6.4(19) Flash image	cat6000-sup.6-4-19.bin	SC6K-SUP-6.4
6.4(19) Flash image (CiscoView)	cat6000-supcv.6-4-19.bin	SC6K-SUPCV-6.4
6.4(19) Flash image (Secure Shell)	cat6000-supk9.6-4-19.bin	SC6K-SUPK9-6.4
6.4(19) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-19.bin	SC6K-SUPCVK9-6.4
6.4(18) Flash image	cat6000-sup.6-4-18.bin	SC6K-SUP-6.4
6.4(18) Flash image (CiscoView)	cat6000-supcv.6-4-18.bin	SC6K-SUPCV-6.4
6.4(18) Flash image (Secure Shell)	cat6000-supk9.6-4-18.bin	SC6K-SUPK9-6.4
6.4(18) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-18.bin	SC6K-SUPCVK9-6.4
6.4(17) Flash image	cat6000-sup.6-4-17.bin	SC6K-SUP-6.4
6.4(17) Flash image (CiscoView)	cat6000-supcv.6-4-17.bin	SC6K-SUPCV-6.4
6.4(17) Flash image (Secure Shell)	cat6000-supk9.6-4-17.bin	SC6K-SUPK9-6.4
6.4(17) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-17.bin	SC6K-SUPCVK9-6.4
6.4(16) Flash image	cat6000-sup.6-4-16.bin	SC6K-SUP-6.4
6.4(16) Flash image (CiscoView)	cat6000-supcv.6-4-16.bin	SC6K-SUPCV-6.4
6.4(16) Flash image (Secure Shell)	cat6000-supk9.6-4-16.bin	SC6K-SUPK9-6.4
6.4(16) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-16.bin	SC6K-SUPCVK9-6.4
6.4(15) Flash image	cat6000-sup.6-4-15.bin	SC6K-SUP-6.4
6.4(15) Flash image (CiscoView)	cat6000-supcv.6-4-15.bin	SC6K-SUPCV-6.4
6.4(15) Flash image (Secure Shell)	cat6000-supk9.6-4-15.bin	SC6K-SUPK9-6.4
6.4(15) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-15.bin	SC6K-SUPCVK9-6.4
6.4(14) Flash image	cat6000-sup.6-4-14.bin	SC6K-SUP-6.4
6.4(14) Flash image (CiscoView)	cat6000-supcv.6-4-14.bin	SC6K-SUPCV-6.4
6.4(14) Flash image (Secure Shell)	cat6000-supk9.6-4-14.bin	SC6K-SUPK9-6.4
6.4(14) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-14.bin	SC6K-SUPCVK9-6.4
6.4(13) Flash image	cat6000-sup.6-4-13.bin	SC6K-SUP-6.4
6.4(13) Flash image (CiscoView)	cat6000-supcv.6-4-13.bin	SC6K-SUPCV-6.4
6.4(13) Flash image (Secure Shell)	cat6000-supk9.6-4-13.bin	SC6K-SUPK9-6.4
6.4(13) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-13.bin	SC6K-SUPCVK9-6.4
6.4(12) Flash image	cat6000-sup.6-4-12.bin	SC6K-SUP-6.4
6.4(12) Flash image (CiscoView)	cat6000-supcv.6-4-12.bin	SC6K-SUPCV-6.4
6.4(12) Flash image (Secure Shell)	cat6000-supk9.6-4-12.bin	SC6K-SUPK9-6.4
6.4(12) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-12.bin	SC6K-SUPCVK9-6.4

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(11) Flash image	cat6000-sup.6-4-11.bin	SC6K-SUP-6.4
6.4(11) Flash image (CiscoView)	cat6000-supcv.6-4-11.bin	SC6K-SUPCV-6.4
6.4(11) Flash image (Secure Shell)	cat6000-supk9.6-4-11.bin	SC6K-SUPK9-6.4
6.4(11) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-11.bin	SC6K-SUPCVK9-6.4
6.4(10) Flash image	cat6000-sup.6-4-10.bin	SC6K-SUP-6.4
6.4(10) Flash image (CiscoView)	cat6000-supcv.6-4-10.bin	SC6K-SUPCV-6.4
6.4(10) Flash image (Secure Shell)	cat6000-supk9.6-4-10.bin	SC6K-SUPK9-6.4
6.4(10) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-10.bin	SC6K-SUPCVK9-6.4
6.4(9) Flash image	cat6000-sup.6-4-9.bin	SC6K-SUP-6.4
6.4(9) Flash image (CiscoView)	cat6000-supcv.6-4-9.bin	SC6K-SUPCV-6.4
6.4(9) Flash image (Secure Shell)	cat6000-supk9.6-4-9.bin	SC6K-SUPK9-6.4
6.4(9) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-9.bin	SC6K-SUPCVK9-6.4
6.4(8) Flash image	cat6000-sup.6-4-8.bin	SC6K-SUP-6.4
6.4(8) Flash image (CiscoView)	cat6000-supcv.6-4-8.bin	SC6K-SUPCV-6.4
6.4(8) Flash image (Secure Shell)	cat6000-supk9.6-4-8.bin	SC6K-SUPK9-6.4
6.4(8) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-8.bin	SC6K-SUPCVK9-6.4
6.4(7) Flash image	cat6000-sup.6-4-7.bin	SC6K-SUP-6.4
6.4(7) Flash image (CiscoView)	cat6000-supcv.6-4-7.bin	SC6K-SUPCV-6.4
6.4(7) Flash image (Secure Shell)	cat6000-supk9.6-4-7.bin	SC6K-SUPK9-6.4
6.4(7) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-7.bin	SC6K-SUPCVK9-6.4
6.4(6a) Flash image	cat6000-sup.6-4-6a.bin	SC6K-SUP-6.4
6.4(6a) Flash image (CiscoView)	cat6000-supcv.6-4-6a.bin	SC6K-SUPCV-6.4
6.4(6a) Flash image (Secure Shell)	cat6000-supk9.6-4-6a.bin	SC6K-SUPK9-6.4
6.4(6a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-6a.bin	SC6K-SUPCVK9-6.4
6.4(6) Flash image	cat6000-sup.6-4-6.bin	SC6K-SUP-6.4
6.4(6) Flash image (CiscoView)	cat6000-supcv.6-4-6.bin	SC6K-SUPCV-6.4
6.4(6) Flash image (Secure Shell)	cat6000-supk9.6-4-6.bin	SC6K-SUPK9-6.4
6.4(6) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-6.bin	SC6K-SUPCVK9-6.4
6.4(5b) Flash image	cat6000-sup.6-4-5b.bin	SC6K-SUP-6.4
6.4(5b) Flash image (Secure Shell)	cat6000-supk9.6-4-5b.bin	SC6K-SUPK9-6.4
6.4(5a) Flash image	cat6000-sup.6-4-5a.bin	SC6K-SUP-6.4
6.4(5a) Flash image (Secure Shell)	cat6000-supk9.6-4-5a.bin	SC6K-SUPK9-6.4
6.4(5) Flash image	cat6000-sup.6-4-5.bin	SC6K-SUP-6.4
6.4(5) Flash image (CiscoView)	cat6000-supcv.6-4-5.bin	SC6K-SUPCV-6.4
6.4(5) Flash image (Secure Shell)	cat6000-supk9.6-4-5.bin	SC6K-SUPK9-6.4
6.4(5) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-5.bin	SC6K-SUPCVK9-6.4
6.4(4a) Flash image	cat6000-sup.6-4-4a.bin	SC6K-SUP-6.4.4a

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.4(4a) Flash image (CiscoView)	cat6000-supcv.6-4-4a.bin	SC6K-SUPCV-6.4.4a
6.4(4a) Flash image (Secure Shell)	cat6000-supk9.6-4-4a.bin	SC6K-SUPK9-6.4.4a
6.4(4a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-4a.bin	SC6K-SUPCVK9-6.4.4a
6.4(4) Flash image	cat6000-sup.6-4-4.bin	SC6K-SUP-6.4.4
6.4(4) Flash image (CiscoView)	cat6000-supcv.6-4-4.bin	SC6K-SUPCV-6.4.4
6.4(4) Flash image (Secure Shell)	cat6000-supk9.6-4-4.bin	SC6K-SUPK9-6.4.4
6.4(4) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-4.bin	SC6K-SUPCVK9-6.4.4
6.4(3) Flash image	cat6000-sup.6-4-3.bin	SC6K-SUP-6.4.3
6.4(3) Flash image (CiscoView)	cat6000-supcv.6-4-3.bin	SC6K-SUPCV-6.4.3
6.4(3) Flash image (Secure Shell)	cat6000-supk9.6-4-3.bin	SC6K-SUPK9-6.4.3
6.4(3) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-3.bin	SC6K-SUPCVK9-6.4.3
6.4(2) Flash image	cat6000-sup.6-4-2.bin	SC6K-SUP-6.4.2
6.4(2) Flash image (CiscoView)	cat6000-supcv.6-4-2.bin	SC6K-SUPCV-6.4.2
6.4(2) Flash image (Secure Shell)	cat6000-supk9.6-4-2.bin	SC6K-SUPK9-6.4.2
6.4(2) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-2.bin	SC6K-SUPCVK9-6.4.2
6.4(1) Flash image	cat6000-sup.6-4-1.bin	SC6K-SUP-6.4.1
6.4(1) Flash image (CiscoView)	cat6000-supcv.6-4-1.bin	SC6K-SUPCV-6.4.1
6.4(1) Flash image (Secure Shell)	cat6000-supk9.6-4-1.bin	SC6K-SUPK9-6.4.1
6.4(1) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-4-1.bin	SC6K-SUPCVK9-6.4.1
6.3(10) Flash image	cat6000-sup.6-3-10.bin	SC6K-SUP-6.3.10
6.3(10) Flash image (CiscoView)	cat6000-supcv.6-3-10.bin	SC6K-SUPCV-6.3.10
6.3(10) Flash image (Secure Shell)	cat6000-supk9.6-3-10.bin	SC6K-SUPK9-6.3.10
6.3(10) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-10.bin	SC6K-SUPCVK9-6.3.10
6.3(9) Flash image	cat6000-sup.6-3-9.bin	SC6K-SUP-6.3.9
6.3(9) Flash image (CiscoView)	cat6000-supcv.6-3-9.bin	SC6K-SUPCV-6.3.9
6.3(9) Flash image (Secure Shell)	cat6000-supk9.6-3-9.bin	SC6K-SUPK9-6.3.9
6.3(9) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-9.bin	SC6K-SUPCVK9-6.3.9
6.3(8) Flash image	cat6000-sup.6-3-8.bin	SC6K-SUP-6.3.8
6.3(8) Flash image (CiscoView)	cat6000-supcv.6-3-8.bin	SC6K-SUPCV-6.3.8
6.3(8) Flash image (Secure Shell)	cat6000-supk9.6-3-8.bin	SC6K-SUPK9-6.3.8
6.3(8) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-8.bin	SC6K-SUPCVK9-6.3.8
6.3(7) Flash image	cat6000-sup.6-3-7.bin	SC6K-SUP-6.3.7
6.3(7) Flash image (CiscoView)	cat6000-supcv.6-3-7.bin	SC6K-SUPCV-6.3.7
6.3(7) Flash image (Secure Shell)	cat6000-supk9.6-3-7.bin	SC6K-SUPK9-6.3.7
6.3(7) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-7.bin	SC6K-SUPCVK9-6.3.7
6.3(6) Flash image	cat6000-sup.6-3-6.bin	SC6K-SUP-6.3.6

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.3(6) Flash image (CiscoView)	cat6000-supcv.6-3-6.bin	SC6K-SUPCV-6.3.6
6.3(6) Flash image (Secure Shell)	cat6000-supk9.6-3-6.bin	SC6K-SUPK9-6.3.6
6.3(6) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-6.bin	SC6K-SUPCVK9-6.3.6
6.3(5) Flash image	cat6000-sup.6-3-5.bin	SC6K-SUP-6.3.5
6.3(5) Flash image (CiscoView)	cat6000-supcv.6-3-5.bin	SC6K-SUPCV-6.3.5
6.3(5) Flash image (Secure Shell)	cat6000-supk9.6-3-5.bin	SC6K-SUPK9-6.3.5
6.3(5) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-5.bin	SC6K-SUPCVK9-6.3.5
6.3(4a) Flash image	cat6000-sup.6-3-4a.bin	SC6K-SUP-6.3.4a
6.3(4a) Flash image (CiscoView)	cat6000-supcv.6-3-4a.bin	SC6K-SUPCV-6.3.4a
6.3(4a) Flash image (Secure Shell)	cat6000-supk9.6-3-4a.bin	SC6K-SUPK9-6.3.4a
6.3(4a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-4a.bin	SC6K-SUPCVK9-6.3.4a
6.3(4) Flash image	cat6000-sup.6-3-4.bin	SC6K-SUP-6.3.4
6.3(4) Flash image (CiscoView)	cat6000-supcv.6-3-4.bin	SC6K-SUPCV-6.3.4
6.3(4) Flash image (Secure Shell)	cat6000-supk9.6-3-4.bin	SC6K-SUPK9-6.3.4
6.3(4) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-4.bin	SC6K-SUPCVK9-6.3.4
6.3(3)x1 Flash image	cat6000-sup.6-3-3X1.bin	SC6K-SUP-6.3.3X1
6.3(3)x Flash image	cat6000-sup.6-3-3X.bin	SC6K-SUP-6.3.3X
6.3(3a) Flash image	cat6000-sup.6-3-3a.bin	SC6K-SUP-6.3.3a
6.3(3a) Flash image (CiscoView)	cat6000-supcv.6-3-3a.bin	SC6K-SUPCV-6.3.3a
6.3(3a) Flash image (Secure Shell)	cat6000-supk9.6-3-3a.bin	SC6K-SUPK9-6.3.3a
6.3(3a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-3a.bin	SC6K-SUPCVK9-6.3.3a
6.3(3) Flash image	cat6000-sup.6-3-3.bin	SC6K-SUP-6.3.3
6.3(3) Flash image (CiscoView)	cat6000-supcv.6-3-3.bin	SC6K-SUPCV-6.3.3
6.3(3) Flash image (Secure Shell)	cat6000-supk9.6-3-3.bin	SC6K-SUPK9-6.3.3
6.3(3) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-3.bin	SC6K-SUPCVK9-6.3.3
6.3(2a) Flash image	cat6000-sup.6-3-2a.bin	SC6K-SUP-6.3.2a
6.3(2a) Flash image (CiscoView)	cat6000-supcv.6-3-2a.bin	SC6K-SUPCV-6.3.2a
6.3(2a) Flash image (Secure Shell)	cat6000-supk9.6-3-2a.bin	SC6K-SUPK9-6.3.2a
6.3(2a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-2a.bin	SC6K-SUPCVK9-6.3.2a
6.3(2) Flash image	cat6000-sup.6-3-2.bin	SC6K-SUP-6.3.2
6.3(2) Flash image (CiscoView)	cat6000-supcv.6-3-2.bin	SC6K-SUPCV-6.3.2
6.3(2) Flash image (Secure Shell)	cat6000-supk9.6-3-2.bin	SC6K-SUPK9-6.3.2
6.3(2) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-2.bin	SC6K-SUPCVK9-6.3.2
6.3(1a) Flash image	cat6000-sup.6-3-1a.bin	SC6K-SUP-6.3.1a
6.3(1a) Flash image (Secure Shell)	cat6000-supk9.6-3-1a.bin	SC6K-SUPK9-6.3.1a
6.3(1) Flash image[2]	cat6000-sup.6-3-1.bin	SC6K-SUP-6.3.1
6.3(1) Flash image (CiscoView)	cat6000-supcv.6-3-1.bin	SC6K-SUPCV-6.3.1

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.3(1) Flash image (Secure Shell)	cat6000-supk9.6-3-1.bin	SC6K-SUPK9-6.3.1
6.3(1) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-3-1.bin	SC6K-SUPCVK9-6.3.1
6.2(3a) Flash image	cat6000-sup.6-2-3a.bin	SC6K-SUP-6.2.3a
6.2(3a) Flash image (Secure Shell)	cat6000-supk9.6-2-3a.bin	SC6K-SUPK9-6.2.3a
6.2(3) Flash image	cat6000-sup.6-2-3.bin	SC6K-SUP-6.2.3
6.2(3) Flash image (CiscoView)	cat6000-supcv.6-2-3.bin	SC6K-SUPCV-6.2.3
6.2(3) Flash image (Secure Shell)	cat6000-supk9.6-2-3.bin	SC6K-SUPK9-6.2.3
6.2(3) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-2-3.bin	SC6K-SUPCVK9-6.2.3
6.2(2a) Flash image	cat6000-sup.6-2-2a.bin	SC6K-SUP-6.2.2a
6.2(2a) Flash image (CiscoView)	cat6000-supcv.6-2-2a.bin	SC6K-SUPCV-6.2.2a
6.2(2a) Flash image (Secure Shell)	cat6000-supk9.6-2-2a.bin	SC6K-SUPK9-6.2.2a
6.2(2a) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-2-2a.bin	SC6K-SUPCVK9-6.2.2a
6.2(2) Flash image	cat6000-sup.6-2-2.bin	SC6K-SUP-6.2.2
6.2(2) Flash image (CiscoView)	cat6000-supcv.6-2-2.bin	SC6K-SUPCV-6.2.2
6.2(2) Flash image (Secure Shell)	cat6000-supk9.6-2-2.bin	SC6K-SUPK9-6.2.2
6.2(2) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-2-2.bin	SC6K-SUPCVK9-6.2.2
6.1(4b) Flash image	cat6000-sup.6-1-4b.bin	SC6K-SUP-6.1.4b
6.1(4b) Flash image (Secure Shell)	cat6000-supk9.6-1-4b.bin	SC6K-SUPK9-6.1.4b
6.1(4) Flash image	cat6000-sup.6-1-4.bin	SC6K-SUP-6.1.4
6.1(4) Flash image (CiscoView)	cat6000-supcv.6-1-4.bin	SC6K-SUPCV-6.1.4
6.1(4) Flash image (Secure Shell)	cat6000-supk9.6-1-4.bin	SC6K-SUPK9-6.1.4
6.1(4) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-1-4.bin	SC6K-SUPCVK9-6.1.4
6.1(3a) Flash image	cat6000-sup.6-1-3a.bin	SC6K-SUP-6.1.3a
6.1(3a) Flash image (Secure Shell)	cat6000-supk9.6-1-3a.bin	SC6K-SUPK9-6.1.3a
6.1(3) Flash image	cat6000-sup.6-1-3.bin	SC6K-SUP-6.1.3
6.1(3) Flash image (CiscoView)	cat6000-supcv.6-1-3.bin	SC6K-SUPCV-6.1.3
6.1(3) Flash image (Secure Shell)	cat6000-supk9.6-1-3.bin	SC6K-SUPK9-6.1.3
6.1(3) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-1-3.bin	SC6K-SUPCVK9-6.1.3
6.1(2a) Flash image	cat6000-sup.6-1-2a.bin	SC6K-SUP-6.1.2a
6.1(2a) Flash image (Secure Shell)	cat6000-supk9.6-1-2a.bin	SC6K-SUPK9-6.1.2a
6.1(2) Flash image	cat6000-sup.6-1-2.bin	SC6K-SUP-6.1.2
6.1(2) Flash image (CiscoView)	cat6000-supcv.6-1-2.bin	SC6K-SUPCV-6.1.2
6.1(2) Flash image (Secure Shell)	cat6000-supk9.6-1-2.bin	SC6K-SUPK9-6.1.2
6.1(2) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-1-2.bin	SC6K-SUPCVK9-6.1.2
6.1(1e) Flash image	cat6000-sup.6-1-1e.bin	SC6K-SUP-6.1.1e
6.1(1e) Flash image (Secure Shell)	cat6000-supk9.6-1-1e.bin	SC6K-SUPK9-6.1.1e
6.1(1c) Flash image (Secure Shell)	cat6000-supk9.6-1-1c.bin	SC6K-SUPK9-6.1.1

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
6.1(1c) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-1-1c.bin	SC6K-SUPCVK9-6.1.1
6.1(1b) Flash image[3]	cat6000-sup.6-1-1b.bin	not orderable
6.1(1b) Flash image (CiscoView)	cat6000-supcv.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell)	cat6000-supk9.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell and CiscoView)	cat6000-supcvk9.6-1-1b.bin	not orderable
6.1(1a) Flash image	cat6000-sup.6-1-1a.bin	not orderable
6.1(1a) Flash image (CiscoView	cat6000-supcv.6-1-1a.bin	not orderable

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

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:

- 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 6000 Family Features

These sections describe the Catalyst 6000 family features:

Features for Supervisor Engine Software Release 6.4

These sections describe the features in software release 6.4, 21 January, 2003:

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.

Software Release 6.4 Hardware Features

Software release 6.4 provides initial support for these modules:

- 48-port 10/100BASE-TX RJ-45 with 128K per-port packet buffers (WS-X6148-RJ-45V provides inline power to IP telephones)

- 48-port 10/100BASE-TX RJ-21 with 128K per-port packet buffers (WS-X6148-RJ21V provides inline power to IP telephones)

Note Software releases 6.1(1) and later do not support the same Flash PC card format as earlier software releases. To use a Flash PC card with software releases 6.1(1) and later, format the card with software releases 6.1(1) and later.

Software Release 6.4 Software Features

Software release 6.4 provides support for these software features:

- In software release 6.4(11) and later releases, 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.
- NVRAM monitoring

  The NVRAM monitoring feature is a background process that allows the system to recover when data in NVRAM is corrupted.

Features for Supervisor Engine Software Release 6.3

These sections describe the features in software release 6.3:

- Software Release 6.3 Hardware Features, page 25
- Software Release 6.3 Software Features, page 25

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.

Software Release 6.3 Hardware Features

There is no new hardware being introduced in software release 6.3.

Note Software releases 6.1(1) and later do not support the same Flash PC card format as earlier software releases. To use a Flash PC card with software releases 6.1(1) and later, format the card with software releases 6.1(1) and later.

Software Release 6.3 Software Features

Software release 6.3 provides support for these software features:

- Single router mode (SRM) redundancy

  SRM redundancy is an alternative to having both MSFC2s in a chassis active at the same time.

  Note that SRM redundancy requires Cisco IOS Release 12.1(8a)E2 and SRM redundancy configuration information will be available when Release 12.1(8a)E2 is posted to Cisco.com. At that time, refer to the "Configuring Redundancy" chapter of the online version of the *Catalyst 6000 Family Software Configuration Guide*, Release 6.3, for detailed configuration procedures.

- Private VLANs on the sc0 interface

  The sc0 management interface can be assigned to a private VLAN.

- EtherChannel enhancements

  An EtherChannel is preserved even if it contains only one port. In software releases prior to 6.3(1), if you have a 2-port channel and one link is removed, the remaining link is removed and added back to spanning tree, which causes a loss of connection on the channel until the link is forwarding again.

- Text file configuration mode

  When you use text file configuration mode, the system stores its configuration as a text file in nonvolatile storage, either in NVRAM or Flash memory. This text file consists of commands entered by you to configure various features.

- Support for NetFlow version 8
- CDPv2 enhancements
  - Addition of TLVs such as sysName, sysObjectID, management address, and physical location.
  - Support of a new device ID format called the mac-address format in addition to the "old-style" format (as in the device hardware serial number).
  - Display changes corresponding to some parameters such as device ID for the **show cdp** command.
- Increase QoS ACLs

  The maximum number of QoS ACLs that can be stored in NVRAM has been increased from 250 to 500. The maximum number of security ACLs (VACLs) remains the same at 250.

- Ethernet link debounce timer feature

  The debounce time is the time a module's firmware waits before notifying the supervisor engine of a link change at the physical layer when a link goes down. If the link is up and then goes down and remains down for a time interval longer than the debounce time, then the supervisor engine is notified. As soon as the link is up again, the timer is reset. If the link is down and then goes up, the supervisor engine is notified immediately. The debounce timer value is hard-coded in the supervisor engine depending upon the type of module being used. The link debounce feature can be enabled on a per-port basis on Ethernet modules.

- Display SNMPv3 counters using the CLI

  Use the CLI to display SNMPv3 counters for various MIBs.

- Autostate enhancements

  A VLAN interface will not transition to the up state until at least one port in the VLAN is forwarding traffic.

- SNMPv3 enhancements

  The SNMPv3 implementation in software releases prior to 6.3(1) supports RFC 2271 through RFC 2275. RFC 2271 through RFC 2275 were replaced with RFC 2571 through RFC 2576. The SNMPv3 enhancement in software release 6.3(1) implements RFC 2571 through RFC 2576.

- Support for the following MIBs:
  - CISCO-AAA-CLIENT-MIB
  - CISCO-CATOS-ACL-QOS-MIB
  - CISCO-CAT6K-CROSSBAR-MIB
  - CISCO-STP-EXTENSION-MIB
  - CISCO-SWITCH-ENGINE-MIB
  - CISCO-SYSTEM-MIB enhancement

Features for Supervisor Engine Software Release 6.2

These sections describe the features in software release 6.2:

- Software Release 6.2 Hardware Features, page 27
- Software Release 6.2 Software Features, page 28

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.

Software Release 6.2 Hardware Features

Software release 6.2 provides initial support for these modules:

- WS-C6513
  Catalyst 13-slot chassis

  Note The WS-C6513 chassis is supported with Supervisor Engine 2 only.

  Note The WS-C6513 chassis has 64 MAC addresses. The MAC address reduction feature is enabled by default on this chassis.

- WS-X6500-SFM 2
  Switch Fabric Module version 2
- WS-X6516-GE-TX
  16-port 10/100/1000BASE-TX fabric-enabled Ethernet module
- WS-X6548-RJ-45
  48-port 10/100BASE-TX fabric-enabled Ethernet module
- WS-X6548-RJ-21
  48-port 10/100BASE-TX fabric-enabled Ethernet module
- WS-X6348-RJ21V
  48-port 10/100BASE-TX Ethernet module with inline power

Note Software releases 6.1(1) and later do not support the same Flash PC card format as earlier software releases. To use a Flash PC card with software releases 6.1(1) and later, format the card with software releases 6.1(1) and later.

Software Release 6.2 Software Features

Software release 6.2 provides support for these software features:

- QoS minimum threshold for WRED

  Allows you to configure the minimum threshold for WRED.

- QoS queuing for port type 1p1q0t/1p3q1t

  Allows queuing on ports that support 1p1q0t/1p3q1t.

- Non-RPF MFD (Multicast Fast Drop)

  Non-RPF multicast fast drop (MFD) rate limits packets that fail the RPF check (non-RPF packets) and drops the majority of the non-RPF packets in hardware.

- Multicast suppression for Gigabit Ethernet modules

  Suppresses multicast traffic on Gigabit Ethernet ports to prevent the ports from being disrupted by a broadcast storm.

- QoS data export

  The QoS statistics data export feature generates per port and per aggregate policer utilization information and forwards this information in UDP packets to traffic monitoring, planning, or accounting applications.

- VACL logging of access denied

  Allows you to configure a log option on any VACL, so that packets or flows that are access denied by the VACL will be redirected to supervisor engine CPU to generate a report.

- Bidirectional VACLs for Private VLANs

  Lets you create a policy that denies access in or out of a network.

- Per-port utilization of QoS statistics

  Provides the input and output packet rate and input and output byte rate on a per-port basis.

- TCAM test on bootup

  The system performs a TCAM test during bootup.

- Dynamic VLAN support with auxiliary VLANs.

  Prior to software release 6.2(2), dynamic ports could only belong to one VLAN. You could not enable the dynamic port VLAN feature on ports that carried a native VLAN and an auxiliary VLAN. With software releases 6.2(2) and later, the dynamic ports can belong to two VLANs. The switch port configured for connecting an IP phone can have separate VLANs configured for carrying the following traffic:

  - Voice traffic to and from the IP phone (auxiliary VLAN)
  - Data traffic to and from the PC connected to the switch through the access port of the IP phone (native VLAN)

- BPDU packet filtering

  BPDU packet filtering turns off BPDU transmission on PortFast-enabled ports and nontrunking ports.

- IEEE 802.1X

  IEEE 802.1X is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

- BPDU skew detection

  BPDU skew detection allows you to troubleshoot slow network convergence caused by skewing.

- Loop guard

  The loop guard feature checks that a root port or an alternate root port is receiving BPDUs. If a port is not receiving BPDUs, the loop guard feature puts the port into an inconsistent state, isolating the failure and letting spanning tree converge to a stable topology until the port starts receiving BPDUs again.

- Local command accounting

  Local command accounting records the last 100 commands that the user entered into the system.

- MSFC Autostate Disable

  Allows you to disable Autostate. The auto state feature shuts down (or brings up) Layer 3 interfaces/subinterfaces on the MSFC and the Multilayer Switch Module (MSM) when the port configuration changes occur on the switch.

- Redundancy enhancement

  Enhanced redundancy provides more efficient system fault detection and recovery mechanisms.

- Core dump for debugging

  A core dump produces a comprehensive report of images when your system fails due to a software error. The core image is produced in Cisco core file format and is stored in the file system. By examining the core dump file, TAC can analyze the error condition of a terminated process.

- Support for the following MIBs:
  - HC-RMON MIB enhancement
  - Cisco STP-EXTENSIONS-MIB enhancements
  - Cisco PRIVATE-VLAN-MIB
  - Cisco ACL-QoS-MIB
  - Cisco QoS-Policy-MIB

Features for Supervisor Engine Software Release 6.1

These sections describe the features in software release 6.1:

- Software Release 6.1 Hardware Features, page 30
- Software Release 6.1 Software Features, page 30

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.

Software Release 6.1 Hardware Features

Software release 6.1(2) provides initial support for these modules:

- 2- and 4-port OC-12 POS Optical Services Modules
- 8- and 16- port OC-3 POS Optical Services Modules

Software release 6.1 provides initial support for these modules:

- Supervisor Engine 2—Policy Feature Card 2 (PFC2; shipped only on Supervisor Engine 2)
  WS-X6K-S2-MSFC2 or WS-X6K-S2-PFC2
  Dual 1000BASE-X GBIC uplinks, fabric-enabled, Cisco Express Forwarding (CEF), enhanced QoS features, PFC2, and MSFC2
  - The Cisco IOS unicast RPF feature is supported in hardware on the PFC2. For ACL-based RPF checks, traffic that matches the RPF ACL is forwarded to the MSFC2.
  - Supervisor Engine 2 and PFC2 do not support ASLB.
- Switch Fabric Module
  WS-C6500-SFM
  Supports fabric-enabled modules.

  Note The WS-C6500-SFM is not supported in the WS-C6513 chassis.

- Fabric-enabled 16-port Gigabit Ethernet GBIC switching module
  WS-X6516-GBIC
- Intrusion Detection System Module
  WS-X6381-IDS

Note Software releases 6.1(1) and later do not support the same Flash PC card format as earlier software releases. To use a Flash PC card with software releases 6.1(1) and later, format the card with software releases 6.1(1) and later.

Software Release 6.1 Software Features

Software release 6.1 provides support for these software features:

- CEF for PFC2—Supervisor Engine 2 and PFC2 provide IP and IPX unicast and IP multicast Layer 3 switching with Cisco Express Forwarding implemented on the PFC2.
- Jumbo frame feature enhancement—You can configure the jumbo frame feature on any Ethernet port and on EtherChannels and trunk ports.

  Note With Cisco IOS Release 12.1(2)E or later, you can configure support for jumbo frames on MSFC2 VLAN interfaces.

- EtherChannel enhancements with PFC2—On a Supervisor Engine 2 with PFC2, you can configure the EtherChannel feature to distribute IP traffic based on Layer 4 port numbers in addition to Layer 3 addresses. With both Supervisor Engine 1 and 2, you can enter the **show channel traffic** command to display EtherChannel traffic.

- Globally disable EtherChannel—Enter the **set port channel all mode off** command to disable all EtherChannels on the switch.
- Globally disable trunking—Enter the **set trunk all off** command to disable all trunks on the switch.
- VMPS server—The Catalyst 6000 family switch can function as a VMPS server.
- 4096 VLANs—Catalyst 6000 family switches support 4096 VLANs in accordance with the IEEE 802.1Q standard.
- Reduced MAC address usage—The MAC address reduction feature is used to enable extended-range VLAN identification. When MAC address reduction is enabled, it disables the pool of MAC addresses used for the VLAN spanning tree, leaving a single MAC address that identifies the switch.

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).

- Multi-Instance Spanning Tree Protocol (MISTP)—MISTP allows you to group multiple VLANs under a single instance of spanning tree. MISTP combines the Layer 2 load-balancing benefits of PVST+ with the lower CPU load of IEEE 802.1Q.
- Spanning Tree Protocol root guard—The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.
- IEEE 802.1Q tunneling—802.1Q tunneling allows multiple VLANs in other VTP domains to be carried by a single VLAN on the Catalyst 6000 family switch without losing their unique VLAN IDs.
- Enhanced ACL configuration with private VLANs—ACLs can be applied as follows:
  - VACLs can be mapped to secondary VLANs or primary VLANs.
  - Cisco IOS ACLs that are mapped to a primary VLAN will get mapped to the associated secondary VLANs.
  - Cisco IOS ACLs cannot be mapped to secondary VLANs.
  - Dynamic ACEs cannot be mapped to a private VLAN.
  - QoS ACLs can be mapped to secondary VLANs or primary VLANs.
- Secure Shell (SSH) encryption—The SSH feature provides security for Telnet sessions to the switch. SSH encryption supports 3DES encryption and can be used in conjunction with RADIUS and TACACS+ authentication (requires a “k9” image).
- MAC address filtering—You can filter traffic based on a host’s MAC address so that packets that are tagged with that specific source MAC address are discarded. When you specify a MAC address filter, incoming traffic from that host MAC address will be dropped and packets addressed to that host will not be forwarded.

- Ability to limit console and Telnet login attempts—You can specify how many console and Telnet login attempts to allow and the duration of the lockout after the switch has denied a login attempt.
- Cisco IOS-like ping—The **-s** argument in the Cisco IOS-like **ping** command allows you to configure the number of packets to ping, the packet size, and the wait time before timing out a response. The wait time can be set as low as 0, which would produce a continuous ping.
- Layer 2 Traceroute—The Layer 2 Traceroute utility allows you to identify the physical path that a packet takes when going from a source to a destination. The Layer 2 Traceroute utility determines the path by looking at the forwarding engine tables of the switches in the path.
- **write tech-support** command—The **write tech-support** command allows you to generate a report with status information about your switch. You can upload this report to a TFTP server and send it to Cisco TAC.
- Search on More prompt—At the More prompt during a **show** command, enter a slash character ("/") followed by a text string to search for text.
- Clearing counters on a per-port basis—The **clear counters** command clears MAC and port counters.
- Enhanced support for scripting—The switch assumes a positive ("yes") answer to all the confirmation prompts when configured from a configuration file.
- System warnings and error counters—Selected debug port counters are polled at a fixed interval, and warnings are generated when the count differs from the previous poll.
- SNMP group access context—When defining the access rights of an SNMP group, you can specify a context string and the way to match the context string.

Features for Supervisor Engine Software Release 5.5

These sections describe the new features available in software release 5.5:

- Software Release 5.5 Hardware Features, page 32
- Software Release 5.5 Software Features, page 33

Software Release 5.5 Hardware Features

This section describes the new hardware component available in software release 5.5:

- 24-port FXS analog interface module (WS-X6224-FXS)—Provides a standard RJ-21 Category 5 telco connector to connect directly to standard analog telephones or fax machines. The module interfaces supply ring voltage and dial tone. The module emulates the central office (CO) or private branch exchange (PBX) because it provides a service to an analog telephone or fax machine. The telephone or fax machine connected through the FXS module behaves as if it is connected to a normal CO or PBX line. The module requires an IP address, is registered with Cisco CallManager in its domain, and is managed by Cisco CallManager.
- 8-port T1/E1 PSTN interface modules (WS-X6608-E1, WS-X6608-T1)—High-density, eight port, T1/E1 VoIP module that can support both digital T1/E1 connectivity to the PSTN or transcoding and conferencing. The module requires an IP address, is registered with Cisco CallManager in its domain, and is managed by Cisco CallManager.

  Download the module software from a TFTP server. Depending upon which software you download, the ports can serve as T1/E1 interfaces or the ports will support transcoding and conferencing.

- Network Analysis Module (WS-X6380-NAM)—Monitors and analyzes network traffic for the Catalyst 6000 family switches using RMON, RMON2, and other MIBs. The RMON support that the NAM provides for Ethernet VLANs is an extension of the RMON support provided by the Catalyst 6000 family supervisor engine. The switched port analyzer (SPAN) selects network traffic and directs it to the NAM. TrafficDirector, or any other IETF-compliant RMON application, can analyze link characteristics, packet layers for capacity planning or departmental accounting, differentiated service deployment and policies, and filter/capture packets for debugging.
- Catalyst 6000 Family Inline-Power Patch Panel (WS-PWR-PANEL)—Works with any Cisco 10/100 Mbps switching product capable of supporting IP telephones. The inline-power patch panel eliminates the need for external power sources; it is a standalone chassis that can be colocated with the Catalyst 6000 family switch to provide –48 VDC power directly to the telephone through existing Catalyst family 10/100BASE-TX switching modules. When used with an uninterruptible power supply (UPS), the inline-power patch panel can provide power to the telephone even in a power failure. The inline-power patch panel has 48 RJ-45 input ports and 48 RJ-45 output ports. There are two RJ-45 connectors per port for a total of 48 ports.
- Inline-power field-upgrade module (WS-F6K-VPWR)—Mounts on the 48-port 10/100BASE-TX RJ-45 module (WS-X6348-RJ-45) and provides –48 VDC inline power on all ports.
- 2500W AC-input power supply (WS-CAC-2500W).

Software Release 5.5 Software Features

This section describes the new software features available in software release 5.5:

Numerous software features are introduced in this release to support configuring a voice-over-IP (VoIP) network using the Catalyst 6000 family voice-related hardware described in the previous section.

For detailed information on the Catalyst 6000 family VoIP software, refer to the “Configuring a Voice-over-IP Network” chapter of the *Catalyst 6000 Family Software Configuration Guide* publication.

Features for Supervisor Engine Software Release 5.4

These sections describe the new features available in software release 5.4:

- Software Release 5.4 Hardware Features, page 33
- Software Release 5.4 Software Features, page 34

Software Release 5.4 Hardware Features

This section describes the new hardware component available in software release 5.4.

- 16-port Gigabit Ethernet module (WS-X6416-GBIC)—Provides 16 switched, full-duplex Gigabit Ethernet ports that you can configure with any combination of 1000BASE-SX, LX/LH, and ZX GBICs. Ports have SC-type connectors for MMF and SMF.
- FlexWAN module (WS-X6182-2PA)—Delivers flexible support for a wide range of Cisco 7200/7500 WAN port adapters. Two port adapters per FlexWAN module are supported, scaling from T1/E1 to OC-3 interfaces and including protocol support for Frame Relay, ATM, Packet over SONET, PPP, and HDLC. The FlexWAN module resides in a single slot of any Catalyst 6000 family switch and has no slot dependencies or limitations. The FlexWAN module works in conjunction with the Policy Feature Card (PFC) on the supervisor engine of the Catalyst 6000 family switch to deliver wire-speed security access control, distributed quality of service (QoS), and granular traffic management functionality.

Note To use the FlexWAN module, you must have a supervisor engine with an MSFC and PFC. You configure the FlexWAN module through the MSFC. For information regarding the FlexWan module, refer to the *Catalyst 6000 Family FlexWAN Module Installation and Configuration Note.*

- 48-port 10/100BASE-TX RJ-45 Ethernet module (WS-X6348-RJ-45)—Provides 128K per-port packet buffers and accepts a field-upgradable voice daughter card in a future release to provide inline power to IP telephones.
- 48-port 10/100 telco RJ-21 Ethernet module (WS-X6248A-TEL)—Provides 128K per-port packet buffers.
- 8-port Gigabit Ethernet module (WS-X6408A-GBIC)—Provides enhanced QoS features.
- 24-port 100FX multimode MT-RJ Ethernet module (WS-X6324-100FX-MT)—Provides 128K per-port packet buffers.
- 16-port 1000BASE-TX RJ-45 Gigabit Ethernet module (WS-X6316-GE-TX)—Provides Gigabit connectivity using standard Category 5 UTP cabling.
- Catalyst Web Interface (CWI)—A browser-based tool that you can use to configure the Catalyst 6000, 5000, and 4000 family switches. It consists of a graphical user interface (GUI) that runs on the client (a Catalyst version of CiscoView 5.0) and a Hypertext Transfer Protocol (HTTP) server that runs on the switch. A GUI alternative to the CLI and SNMP interfaces, the CWI provides a real-time graphical representation of the switch and detailed information such as port status, module status, type of chassis, and modules. The CWI uses HTTP to download CiscoView from the server to the client.

Note For information on installing and using the CWI, refer to the *Catalyst 6000, 5000, and 4000 Family Switches Web Interface Installation and Configuration Note* publication.

Software Release 5.4 Software Features

This section describes the new software features available in software release 5.4:

- High availability—Provides improved switchover time from the active supervisor engine to the standby supervisor engine by synchronizing the standby supervisor engine with the active supervisor engine. In the event of a switchover, the standby can take over and continue exactly where the failed supervisor engine left off. The high-availability feature also provides a versioning option. High-availability versioning allows you to 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.
- UDLD enhancements—With supervisor engine software releases 5.4(3) and later, you can specify the message interval between UDLD messages. Previously, the message interval was fixed at 60 seconds. With a configurable message interval, UDLD reacts much faster to link failures.

  Additionally, releases 5.4(3) and later have UDLD aggressive mode. UDLD aggressive mode is disabled by default and its use is recommended only for point-to-point links between Cisco switches running software release 5.4(3) or later. With aggressive mode enabled, when a port on a bidirectional link stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is put into errdisable state.

In order to prevent spanning tree loops, normal UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to forwarding state (when default spanning tree parameters are used).

Enabling UDLD aggressive mode provides additional benefits in the following cases:

- One side of a link has a port stuck (both Tx and Rx)
- One side of a link remains up while the other side of the link has gone down

In these cases, UDLD aggressive mode errdisables one of the ports on the link and stops the blackholing of traffic. Even with aggressive mode disabled, there would have been no risk for a broadcast storm due to a spanning tree loop in this situation, as one port is unable to pass traffic in both directions.

For detailed information on configuring the message interval and UDLD aggressive mode, refer to the online version of the *Catalyst 6000 Family Software Configuration Guide, Release 5.4*.

- RADIUS authorization and accounting—Provides client-server authentication and accounting for users attempting to connect to the switch.
- TACACS+ authorization and accounting—Provides client-server authentication and accounting for access to network devices.
- Generic summertime—Allows you to configure non-US summertime.
- NTP enhancements—Trusted Key and Authorization supports the trusted key option where NTP time updates are only accepted from hosts with the correct key.
- Errdisable timeout—Allows you to automatically enable or reset a port minutes after a port is disabled by the software due to excessive errors.
- Case-sensitive password—Allows you to set case-sensitive passwords.
- IP permit list enhancements—Increases the number of IP entries allowed and provides you with the capability to configure separate permit lists for Telnet and SNMP traffic.
- Banner improvement—Increases the banner string to 3,070 characters long and includes a tab character.
- Scheduled reset—Allows you to reset the switch at a specified date and time.
- Permanent ARP entries—Allows you to save a static ARP entry in the NVRAM (or Flash) configuration file so a reset or power cycle does not clear the entry.
- Private VLANs—Sets of ports that have the features of normal VLANs and also provide some Layer 2 isolation from other ports on the Catalyst 6000 family switch.
- Port security enhancements and single device per port:
  - Increases the number of learned and configurable MAC addresses for port security to 1 MAC address per port and 1024 shared MAC addresses.
  - Supports an option to automatically enable/reset the port N minutes after a port security violation lockdown.
  - Provides an option to allow port security to automatically enable or reset the port on a link down instead of after a timeout. (NOT supported)
  - Supports aging on the learned address to allow a new MAC address to use switch port after a configurable aging time in minutes.
- Kerberos Telnet—Provides support for encrypted Telnet sessions on the switch using Kerberos.

- DHCP client and rcp—Allows the switch to obtain its IP configuration from a DHCP server automatically and provides an alternative method for copying system software image files and configuration files over the network using remote copy (rcp).
- Command completion—Allows you to use the tab key to automatically complete unambiguous commands.
- Show configuration nondefault and default filename for the device configuration file—Allows you to specify nondefault values only in the **show config** command.
- Configure from Flash on startup—Allows the switch to use a configuration file on Flash instead of NVRAM.
- **show tech-support** command—Allows you to capture all of the information and statistics required by Cisco TAC for the entire device.
- **set port host** command—Essentially a CLI macro that executes these commands: **set spantree portfast enable**, **set trunk off**, and **set port channel off**. This new command will provide a quick and convenient way to configure host/access ports to a mode that allows the port to forward traffic in less than one second from link up.
- VLAN 1 disable on trunks—Allows you to disable VLAN 1 on any individual VLAN trunk link.
- PortFast guard—Provides a means to shut the port down when any received BPDUs are detected.
- RGMP support—Allows the switch to forward IP multicast traffic to only those multicast routers that are interested in receiving the traffic, thus offloading the multicast router from unnecessary packet processing and improving the network bandwidth.

Note The MSFC supports RGMP in Release 12.1(1)E or later.

- IGMP fast leave—Provides a mechanism to leave multicast sessions without any latency.
- Disable port startup option—Allows you to specify the default operation for all ports to be shut down, and once set, in the event of a complete configuration erase or a corrupted configuration, no traffic will be transmitted through the switch.
- Diagnostics options on bootup—Provides options to bypass all diagnostics completely, run a minimal set, or run the complete set.
- Capture capability with VACLs—Allows you to capture selective traffic and redirect it to one or multiple ports to which an Intrusion Detection appliance(s) can be connected.
- SNMPv3—Provides security and remote configuration capabilities of SNMPv3.
- Improved SNMP response time—Minimizes the response time for the SNMP subsystem in the Catalyst 6000 family switch.
- External LDA with the internal router—Supports the internal router as the default router.
- QoS ACL and VACL configuration from Flash memory—Configures and stores ACLs in Flash memory instead of NVRAM.
- System log messages for backplane traffic, low memory conditions, memory corruption, NVRAM conditions, inband communication errors, and TCP/UDP errors.

Features for Supervisor Engine Software Release 5.3

This section describes the new features available in software release 5.3:

- UniDirectional Link Detection (UDLD)—Detects unidirectional connections on both copper and fiber-optic links.
- RADIUS authentication—Provides client-server authentication for users attempting to connect to the switch.
- Jumbo frame support for intra-VLAN traffic on Gigabit Ethernet links increases the MTU size to 9216 bytes (note that jumbo frames cannot be routed or fragmented for transmission through slower ports).
- Virtual Management Policy Server (VMPS) client support allows network administrators to define the VLAN membership policies for their network in a central database so that the switch automatically configures user ports to the correct VLAN.
- With the single-port OC-12 ATM Module (SMF or MMF):
  - Reassembly of up to 255 buffers simultaneously (each buffer represents a packet)
  - Support for up to 4096 virtual circuits
  - Support for AAL 5
  - ATM LANE 1.0, including LEC, LES, BUS, and LECS
  - MPOA support
- On switches with a Policy Feature Card (PFC):

Note IPX VACLs, QoS ACLs, COPS-DS, and RSVP for Qualitative Service were introduced in software release 5.3(1a)CSX but were not fully tested; you were instructed not to use them. **These features can be used in software releases 5.3(3)CSX or later as they have been fully tested.**

  - VLAN access control lists (VACLs) using IP, IPX, and MAC ACLs.

    A VACL enhancement in software release 5.3(3)CSX is as follows:

    A VACL redirect ACE allows a unicast flow to be specified.
  - Common Open Policy Service (COPS) for Differentiated Services (DS) allows QoS to be configured from a central policy decision point server.
  - Resource ReSerVation Protocol (RSVP) for Qualitative Service allows hosts to request QoS.
  - Remote SPAN (RSPAN) supports source and destination SPAN ports on other compatible switches.
  - Quality of service (QoS) supports classification, marking, and policing using IP, IPX, and MAC ACLs.
  - Accelerated server load balancing (ASLB) support enables Catalyst 6000 family switches to cache Cisco LocalDirector load-balancing flows, accelerating the performance of the LocalDirector, which is a network appliance with a secure, real-time, embedded operating system that intelligently load balances IP traffic across multiple servers (refer to the *Catalyst 6000 Family Accelerated Server Load Balancing Installation and Configuration Note*).

    ASLB enhancements in software release 5.3(3)CSX are as follows:

    A TCP port can be a wildcard (0).

    Up to 1024 virtual-IP addresses and TCP port pairs are supported.

Note Accelerated server load balancing was previously called LocalDirector Accelerator in these release notes.

- On switches with a Multilayer Switch Feature Card (MSFC):
  - IP Multilayer Switching (MLS) provides high-performance hardware-based Layer 3 switching of IP unicast traffic, offloading processor-intensive IP packet routing from network routers.
  - IP Multicast Multilayer Switching (IP MMLS) provides high-performance hardware-based Layer 3 switching of IP multicast traffic, offloading processor-intensive IP multicast packet routing from network routers.
  - IPX MLS provides high-performance hardware-based Layer 3 switching of IPX unicast traffic, offloading processor-intensive IPX packet routing from network routers. Provides standard and extended Cisco IOS access control lists (ACLs) at wire rate.
  - NetFlow Data Export (NDE) allows a summary of intersubnet Layer 3 traffic statistics for all expired flows to be periodically exported to a network management data collector.

Note Refer to the *Release Notes for Catalyst 6000 Family Multilayer Switch Feature Card* for more information.

Features for Supervisor Engine Software Release 5.2

This section describes the new features available in software release 5.2:

- GARP VLAN Registration Protocol (GVRP; see IEEE 802.1p) provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.
- GARP Multicast Registration Protocol (GMRP; see IEEE 802.1p) maintains Layer 2 multicast groups that determine which switch ports need to participate in multicasts.
- EtherChannel frame distribution is configurable with Layer 2 Switching Feature Card II (WS-F6020A) and can use either Media Access Control (MAC) addresses or IP addresses and either source or destination or both source and destination addresses.

  Enter a **show module** command for the supervisor engine to determine if EtherChannel frame distribution is configurable on your switch. If the display shows the "Sub-Type" to be "L2 Switching Engine I WS-F6020," then EtherChannel frame distribution is not configurable on your switch; it uses source and destination MAC addresses. EtherChannel frame distribution is configurable with any other switching engine and the default is to use source and destination IP addresses.
- The Spanning Tree Protocol can be enabled and disabled on a per-VLAN basis.

Features for Supervisor Engine Software Release 5.1

This section describes the features available in software release 5.1:

- Initial support for the Catalyst 6000 family switches
- Redundant supervisor engines (uplink ports are fully functional on a redundant supervisor engine in standby mode)
- IP supernetting, compatible with classless interdomain routing (CIDR)

- EtherChannel (maximum of eight ports) on all Ethernet ports on all modules, including those on a standby supervisor engine, with no requirement that ports be contiguous or on the same module
- Up to 1024 VLANs
- VLAN Trunk Protocol (VTP)
- Inter-Switch Link (ISL) and 802.1Q VLAN trunking on all Ethernet ports on all modules
- Per-VLAN Spanning Tree Protocol, STP PortFast, STP UplinkFast, and STP BackboneFast
- 802.1Q-to-ISL VLAN mapping of up to eight 802.1Q VLANs numbered above 1005 to ISL VLANs
- Quality of Service (QoS)
- For transmitted traffic, up to four SPAN sessions; for received or both transmitted and received traffic, up to two SPAN sessions
- SNMP, SNMP v2C, SNMP traps, and Remote Monitoring (RMON)
- Switch TopN reports
- Cisco Discovery Protocol (CDP)
- System message logs

Usage Guidelines and Restrictions

These sections provide usage guidelines and restrictions for the Catalyst 6000 family switches:

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:

- With software releases 6.4(11) and later, after a switchover, the newly active supervisor engine might display the following message:

  ```
  Unable to message Standby Supervisor to Disable consistency checker
  ```

  This problem is due to a shortage of memory for setting ROMMON variables.

  Workaround: Either clear some of the ROMMON variables or reduce the boot string to only the essential images using the **set boot system flash** command. (CSCef42081)

- The WS-C6K-9SLOT-FAN2 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.
- MAC addresses—Theoretical and recommended limits for PFC/PFC2: 128K theoretical maximum, 32K recommended.
- 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 the **standby use-bia** option is configured, 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)
- In extremely rare conditions, the following configuration might cause the supervisor engine to reset when the MSFC2 is reloaded:
  - Supervisor Engine 2 (with MSFC2) running supervisor engine software release 6.2(2) or 6.3(1)
  - FlexWAN module with ATM port adapter
  - Unicast RPF enabled on VLAN interfaces

  The workaround is to disable unicast RPF on the VLAN interfaces. (CSCdv20407)
- In a redundant supervisor engine configuration, both supervisors must be running the same boot ROM version. For information on upgrading the boot ROM version, refer to the *Catalyst 6000 Family Supervisor Engine 2 Boot ROM and Bootflash Device Upgrade Installation Note* at this URL:

  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. The workaround is to 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)

- When you reset the supervisor engine from a Telnet connection, the connection will not get dropped and will appear as though Telnet is frozen. To back out from the Telnet session, you need to manually disconnect the Telnet connection using the escape commands of the Telnet program. (CSCdp32220)
- 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. The workaround is to enable the fast UDP aging only when really needed (for example, when load balancing UDP). (CSCdp79475)
- In a system with a Supervisor Engine 2 and WS-X6101 (ATM LANE) modules, ACLs 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 boot up, 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).

Modules and Switch Ports

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

- It is possible to power down a Switch Fabric Module from the CLI before it comes online but we do not support this action. Powering down a Switch Fabric Module while it is coming online can cause conflicting switching mode change operations to occur simultaneously which can result in delays in restoring the data path and unpredictable switch behavior. This Switch Fabric Module behavior is not going to be addressed by any hardware or software modifications. Rather, we are advising you to wait to power down a Switch Fabric Module until it comes online.
- At bootup some non-Ethernet modules (such as MSFC, WAN modules, and service modules) may fail to come online. This problem is seen especially in fully loaded chassis. The workaround is to manually reset each module that fails to come online at bootup. (CSCed24552)
- With software release 6.4(7), 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 err-disable-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 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

  This problem is seen on modules with the four-port Gigabit interface ASIC.

  (CSCdr56784)
- A SPAN session with a 10/100 source port and a Gigabit destination port might result in duplicated packets on the destination port. (CSCea32926)
- 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. The workaround is to 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, as a workaround, 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.
- 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. The workaround is to 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 only on the MSFC. These items are supported on systems running Cisco IOS Release 12.1(5c)EX or later on both the Supervisor Engine 2 and the MSFC2. For more information, refer to the Release Notes for 12.1(5c)EX on Cisco.com:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/ios121_e/78_12505.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 an 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)

EtherChannel

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

- 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. The workaround is to explicitly configure a higher cost for the EtherChannel after enabling UplinkFast. (CSCds22895)
- 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)

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 (kilo-bits-per-second) and Kb (kilo bits). 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
- When you configure standard QoS receive-queue tail-drop thresholds, do not set the threshold 4 value less than 75 percent. Failure to do so might cause packets to be dropped on ports that are associated with the queue. (CSCdu75029)
- The **set port qos** *mod/por*t {**port-based** | **vlan-based**} command configures all ports on switching modules with **1p1q0t/1p3q1t** QoS port architecture.
- In extremely rare circumstances in a Catalyst 6000 family switch with two Supervisor Engine 2s, if you have more than 300 QoS ACLs and each is mapped to a different VLAN, the active supervisor engine might reset after clearing all the QoS ACLs and then committing the change. There is no workaround. (CSCdu85021)
- 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. The workaround is to 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)
- Catalyst 6000 family switches do not support non-zero WRED minimum values. If a COPS QPM server sends down a COPS policy with a non-zero 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)
- COPS and RSVP are not supported in software release 6.2(2).

- On a Catalyst 6000 family 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. The workaround to 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 boot up, 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. The workaround is to 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 6000 family switch cannot support. (CSCds16976)
- Except for ports that support 1p1q0t/1p3q1t, 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.
- 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)

Multicast

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

- 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.
- If a host sends an IGMPv1 report during the max-query-response-interval (the default is 10 seconds) after another host sends an IGMPv2 report, the IGMPv1 report will be suppressed by the supervisor engine and connected routers will not see this report. This situation can result in connected routers not falling back to IGMPv1 compatibility mode. Later, if an IGMPv2 host sends an IGMP Leave, the routers will send IMGPv2 GS queries in response (which IGMPv1 hosts do not understand). If there are no other IGMPv2 hosts for this group on the VLAN, then the router removes this VLAN from its outgoing interface list. (CSCdu83776)
- 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 a router connected to the switch is configured with a "last-member-query-interval" that is greater than the default interval that is defined in RFC 2236, and IGMP snooping is enabled 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. Currently, the supervisor engine software does not modify its behavior based on the last-member-query-interval configured on connected routers. Therefore, there is no benefit to modifying the last-member-query-interval on routers that are connected to the switch if IGMP snooping is enabled. The workaround is to disable IGMP snooping on the switch. (CSCdu72041)
- Bridged IP multicast traffic is not policed if an MSFC2 is installed and the VLAN interface defined on the MSFC2 is in shutdown mode. (CSCdu12731)
- With software releases 6.3(2) and later, the maximum number of Layer 2 multicast entries is 15488.
- If RGMP-enabled routers connected to an RGMP-enabled Catalyst 6000 family 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 6000 family 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.
- The maximum number of supported multicast CAM entries is 124. After adding 124 permanent or static multicast CAM entries the switch produces the error "Failed to add CAM entry." After adding 124 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.
- In extremely rare conditions, multicast traffic might be blocked due to a mismatch between hardware and software entries. (CSCdp81324)
- 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.

Spanning Tree

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

- 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. The only workaround is to 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 access control:

- The packets that are sent to the MSFC as a result of a bridge action from an ACL are not rate limited. Only those packets that are sent to the MSFC from a FIB hit are rate limited. (CSCdr99239)
- Note that VACLs provide access control for **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.

High Availability

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

- In software release 6.4(11) and later releases, 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.

- Prior to enabling Single Router Mode (SRM) on the MSFC, you must enable high availability on the supervisor engine. Currently, no syslog message is generated when SRM is enabled and high availability is disabled on the supervisor engine. In supervisor engine software releases 6.3(2) and later releases, if you enable SRM and high availability is disabled on the supervisor engine, a syslog message displays indicating that you must enable high availability before you enable SRM. Failure to do so could result in unexpected system behavior. (CSCdu78927)
- 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. The workaround is to 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)
- In extremely rare conditions, 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. The workaround is to either reset the individual modules reporting this error or reset the switch. (CSCdv51172, CSCdv50525)

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 6000 family 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 a Catalyst 6000 family switch running supervisor engine software is connected to a switch running Cisco IOS software on the supervisor engine and both switches have VTP enabled, the Cisco IOS VTP might have a higher VTP configuration revision. In this event, the Cisco IOS switch tries to update the VTP on the switch running supervisor engine software. The switch running Cisco IOS has VLAN 1 translated to VLAN 1003 by default (Token Ring type VLAN), and the switch running supervisor engine software does not support this configuration resulting in an undefined VLAN configuration. If you try to configure the affected VLAN (VLAN 1 in this case), the system might reset with a watchdog timeout. This problem was corrected as follows in software releases 6.3(3) and later.

  When the switch running supervisor engine software experiences the problem, it changes to VTP transparent mode and the following message is displayed:

  ```
  VTP-4-UNSUPPORTEDCFGRCVD:Rcvd VTP advert with unsupported vlan config on trunk 3/24 -
  VTP mode changed to transparent
  ```

  (CSCdu32627)

- 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 6000 family 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 6000 family 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. The workaround is to 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 applies 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)

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. In this section when we say auto-MDI/MDIX works with the speed set to auto/1000 Mbps, but not with the speed set to 10Mbps or 100Mbps, 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 10Mbps or 100Mbps 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 10Mbps or 100Mbps.
- WS-X6316-GE-TX

With software release 8.2(1), auto-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 10Mbps or 100Mbps
- WS-X6148X2-RJ-45, WS-X6148X2-RJ-45V

  Auto-MDI/MDIX works with the speed set to auto, but not with the speed set to 10Mbps or 100Mbps.

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

CiscoView Images

This section contains usage guidelines, restrictions, and troubleshooting information that applies to CiscoView (CV) images:

- The supported client platform/browser/plug-in versions to launch embedded CiscoView are as follows:

Client Platform	Web Browser	Java Plug-in
Solaris 2.6/2.7	Netscape Communicator 4.7	Java Plug-in 1.3.0 (JRE 1.3.0)
Windows NT 4.0 and Windows 2000	Internet Explorer 5.5 and Netscape Communicator 4.7	Java Plug-in 1.3.0-C (JRE 1.3.0)

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

Note Java Plug-in versions 1.3.1 is not supported.

- The digital security certificate that is used to sign the Java classes in software release 6.2(2)CV image will be valid until May 19th, 2002. After the expiration date, if embedded CiscoView cannot be launched or an Access Control Error occurs, upgrade to the latest image or upgrade the plug-in/browser on the client machine.
- If CiscoView does not work after resizing the browser window on a Solaris client machine, download and use the Netscape Communicator 4.7 from Sun Microsystems instead of from Netscape.
- The new releases of the Java Plug-in 1.3 (1.3.0_01 and 1.3.0_02) available for download from Sun Microsystem's website do not work with CiscoView versions 5.5(4) and later on the Catalyst 4000 family, Catalyst 5000 family, Catalyst 6000 family, and Catalyst 2900/3500XL switches. The workaround is to install the previous release of the 1.3 Plug-in, 1.3.0-C.

  To determine the version installed on your system, go to the "Start Menu" and select "Settings" then "Control Panel." There is a Java Icon in the Control Panel that displays the version. If it indicates "Java Plug-In" then it is the correct version. The incorrect versions have _01 or _02 next to the name. You can also double click on the Java Icon and then click on the "About" tab to display the version, which should be 1.3.0-C for CiscoView to work properly. (CSCdt96453)
- CiscoView images take approximately 12 minutes to download from a TFTP server to a PCMCIA Flash card. (CSCdr14437)
- You may be unable to delete a primary VLAN after unbinding the secondary VLAN. The workaround is to close and reopen the dialog and try to delete the primary VLAN again.

  If you attempt to bind a secondary VLAN to the primary VLAN and delete the primary VLAN, the following incorrect error message appears:

  ```
  Set failed due to snmpRspGenErr for vtpVlanEditRowStatus.1.199
  ```

  The workaround is to close and reopen the dialog and the correct error message will display. (CSCdt65530)
- 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. The workaround is to delete the policy selection entry that was added. (CSCdu43690)
- 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. The workaround is to 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 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. The workaround is to overwrite the values in the fields if necessary. (CSCdu05678 and CSCdu15066)

- If you select **Configure >Interface**, all fields show either as N/A or with wrong values for the MultiChannel DS3 PA installed on a WS-X6182-PA module. (CSCdr39591)
- The Catalyst 6000 CiscoView (CV) images do not support the Carrier Alarm LED for WAN modules. (CSCdt52011)

Open and Resolved Caveats in Software Release 6.4(21)

These sections describe open and resolved caveats in supervisor engine software release 6.4(21):

- Open Caveats in Software Release 6.4(21), page 54
- Resolved Caveats in Software Release 6.4(21), page 54

Open Caveats in Software Release 6.4(21)

This section describes open caveats in supervisor engine software release 6.4(21):

- 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 that are 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 that is 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 6.4(21)

This section describes resolved caveats in supervisor engine software release 6.4(21):

- After a high-availability switchover, you might experience a MISTP reconvergence on the newly active supervisor engine and the following message may display:

  ```
  2005 Sep 09 16:00:49 JST +09:00 %SPANTREE-2-SWOVER_TOOLONG: switchover took too much
  time. All STP ports restarted.
  ```

  This problem is resolved in software release 6.4(21). (CSCej37841)

Open and Resolved Caveats in Software Release 6.4(20)

These sections describe open and resolved caveats in supervisor engine software release 6.4(20):

- Open Caveats in Software Release 6.4(20), page 55
- Resolved Caveats in Software Release 6.4(20), page 55

Open Caveats in Software Release 6.4(20)

This section describes open caveats in supervisor engine software release 6.4(20):

- 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 that are 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 that is 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 6.4(20)

This section describes resolved caveats in supervisor engine software release 6.4(20):

- 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 6.4(20). (CSCed20984)
- You might experience a TLB exception when committing a VACL with approximately 278 or more lines. This problem is resolved in software release 6.4(20). (CSCej06637)
- After entering the **set ip unreachable disable** command, "destination unreachable" replies continue to be output from the switch. This problem is resolved in software release 6.4(20). (CSCsb56969)

Open and Resolved Caveats in Software Release 6.4(19)

These sections describe open and resolved caveats in supervisor engine software release 6.4(19):

Open Caveats in Software Release 6.4(19)

This section describes open caveats in supervisor engine software release 6.4(19):

- 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 that are 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 that is 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 6.4(19)

This section describes resolved caveats in supervisor engine software release 6.4(19):

- With an EtherChannel formed using ports on both the standby and active supervisor engines, the switchover time might take longer than normal. This problem is resolved in software release 6.4(19).

  Workaround: Use the ports in a module other than the supervisor engine for the EtherChannel. (CSCef00617)

- In rare circumstances with a Supervisor Engine 2 and UDLD and high availability enabled, you might see a unidirectional link after a high-availability switchover. This problem is resolved in software release 6.4(19). (CSCei12152)

- Removing a private VLAN from a promiscuous port using the **clear pvlan mapping** *primary-vlan secondary-vlan mod/port* command breaks connectivity on that promiscuous port for all other mapped secondary VLANs. This problem has been seen with a Supervisor Engine 1A on switches running software release 7.6(11) and later releases with ports configured on the WS-X6148-GE-TX module.

  Workaround: To restore connectivity, add back the VLAN mapping. This problem is resolved in software release 6.4(19). (CSCeh51722)

- When you are running software release 6.4(12) and later releases, the lbusDrops counter is incremented although no traffic is flowing. This is a cosmetic issue. This problem is resolved in software release 6.4(19). (CSCeh66404)

- With software release 6.4(17) and later releases, when the MSFC on the standby supervisor engine exceeds its minor temperature threshold, the module status is displayed as faulty. The module status should be displayed as temp-minor. This problem is resolved in software release 6.4(19). (CSCei55551)
- After a period of time, the Supervisor Engine 1A might drop multicast traffic. This problem is resolved in software release 6.4(19). (CSCsb55180)

Open and Resolved Caveats in Software Release 6.4(18)

These sections describe open and resolved caveats in supervisor engine software release 6.4(18):

Open Caveats in Software Release 6.4(18)

This section describes open caveats in supervisor engine software release 6.4(18):

- 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 that are 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 that is 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 6.4(18)

This section describes resolved caveats in supervisor engine software release 6.4(18):

- The SNMP "snmpdm" process is sleeping after running for a long time. This problem is resolved in software release 6.4(18). (CSCeg64313)
- The WS-X6148-45AF module might reset due to excessive link changes and display the following error message:

  ```
  2005 May 06 13:02:24 %SYS-5-MOD_NOSCPPINGRESPONSE:Module 9 not responding... resetting
  module 2005 May 06 13:02:24 %SYS-5-MOD_RESET:Module 9 reset from Software 2005 May 06
  13:04:07 %SYS-5-MOD_OK:Module 9(WS-X6148-45AF,SAL08175TMG) is online
  ```

  This reset is not related to faulty hardware and is caused when ports go up and down at an abnormally high rate.

  Workaround: Check the linkChange counter in the output of the **show counters** *mod/port* command. A large number of link changes could cause the module to reset. This problem is resolved in software release 6.4(18). (CSCeh84332)

- When the **set errordetection portcounters enable** command is entered, you will see two SCP retries every 30 minutes.

  Workaround: Enter the **set errordetection portcounters disable** command. This problem is resolved in software release 6.4(18). (CSCei08970)

- Netstat TCP displays negative values. This problem is resolved in software release 6.4(18). (CSCei21068)
- You might experience an exception when using CiscoWorks RME4.0 to pull information from the switch. This problem is resolved in software release 6.4(18). (CSCsb18681)
- With a Supervisor Engine 2/MSFC2, Unicast Reverse Path Forwarding (uRPF) may not work properly for multipath routes after RPF is disabled on a specific VLAN while other VLAN(s) still have RPF enabled.

  Workaround: Disable all RPF-enabled VLANs and then enable them again. This problem is resolved in software release 6.4(18). (CSCei06016)

- With a Supervisor Engine 1 or Supervisor Engine 2, the configuration information for SPAN might be lost when the switch is reset after entering the **clear config all** command followed by the **set span** command. This problem has been seen with the following hardware/sofware:
  - WS-X6K-SUP1A-2GE/software release 6.1(2)
  - WS-X6K-SUP1A-2GE/software release 6.2(2)
  - WS-X6K-SUP1A-2GE/software release 6.4(3)
  - WS-X6K-SUP2-2GE/software release 6.1(3)
  - WS-X6K-SUP2-2GE/software release 6.3(1)
  - WS-X6K-SUP2-2GE/software release 6.3(10)
  - WS-X6K-SUP2-2GE/software release 6.4(2)
  - WS-X6K-SUP2-2GE/software release 6.4(17)

  This problem is resolved in software release 6.4(18). (CSCsb40859)

Open and Resolved Caveats in Software Release 6.4(17)

These sections describe open and resolved caveats in supervisor engine software release 6.4(17):

- Open Caveats in Software Release 6.4(17), page 59
- Resolved Caveats in Software Release 6.4(17), page 59

Open Caveats in Software Release 6.4(17)

This section describes open caveats in supervisor engine software release 6.4(17):

- 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 that are 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 that is 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 6.4(17)

This section describes resolved caveats in supervisor engine software release 6.4(17):

- With a Supervisor Engine 1A/MSFC in single router mode redundancy, old MLS entries might not be purged when the active supervisor engine is removed from the switch. This problem is resolved in software release 6.4(17).

  Workaround: Manually clear the old MLS entries. (CSCef29082)

- A switching module's port cost values might not synchronize correctly with the standby supervisor engine after the following configuration steps are performed on the switching module:

  - UplinkFast is enabled.
  - The module's configuration is cleared.

  The problem is seen regardless of the spanning-tree mode. This problem is resolved in software release 6.4(17). (CSCeg78210)

- The switch might not return the values of the cseL2ForwardedLocalOctets MIB counter, although other counters in the cseL2StatsEntry tree are correctly returned. This problem is resolved in software release 6.4(17). (CSCeh16351)
- IEEE BPDUs 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 BPDUs should not be sent. If the trunk port reinitializes itself for any reason (such as disabling/enabling the trunk or doing a module or switch reset), the trunk port may start to send IEEE untagged BPDUs.

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

  set trunk *mod/port NativeVlan_ID*

  clear trunk *mod/port NativeVlan_ID*

  This problem is resolved in software release 6.4(17). (CSCeh28209)
- On a Supervisor Engine 2/MSFC2 with PFC hardware version 2.0, you might see high CPU utilization after committing a large VACL that results in spanning tree recalculations. This problem is not seen with PFC hardware version 1.0 or 1.3. This problem is resolved in software release 6.4(17). (CSCeh37782)
- OSPF hello packets are not being forwarded from the switching module to the MSFC on the standby supervisor engine resulting in OSPF adjacencies going down on the MSFC. This problem is observed when the FPOE consistency checker is enabled.

  Workaround: Disable the FPOE consistency checker. This problem is resolved in software release 6.4(17). (CSCeh74503)

Open and Resolved Caveats in Software Release 6.4(16)

These sections describe open and resolved caveats in supervisor engine software release 6.4(16):

- Open Caveats in Software Release 6.4(16), page 60
- Resolved Caveats in Software Release 6.4(16), page 61

Open Caveats in Software Release 6.4(16)

This section describes open caveats in supervisor engine software release 6.4(16):

- 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 that are 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 that is 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 6.4(16)

This section describes resolved caveats in supervisor engine software release 6.4(16):

- 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 6.4(16). (CSCef54438)
- 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 6.4(16). (CSCeg29195)
- 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 6.4(16). (CSCeg47658)
- 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 6.4(16). (CSCeg61577)
- Under certain conditions, such as bringing up the standby supervisor engine, the FPOE consistency checker might be disabled even though the active supervisor engine had consistency checking enabled before the switchover. This problem is resolved in software release 6.4(16). (CSCeg64212)
- 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 6.4(16). (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 6.4(16). (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 6.4(16). (CSCeg73646)
- 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 6.4(16). (CSCeg76020)
- In software release 6.4(16), the number of TCP-established sessions has been increased from 64 to 128. (CSCeg85630)

- If you upgrade your switch from any software release 7.x or earlier releases to software release 8.x and later releases with the boot mode set to "text" and spanning tree set to "PVST+," the spanning-tree mode changes to "Rapid PVST+."

  Workaround: Change the boot mode to "binary" before performing the upgrade. This problem is resolved in software release 6.4(16). (CSCin75737)

- During a high availability switchover, the active supervisor engine may incorrectly detect a hardware mismatch during the synchronization process. Possible symptoms of this problem are as follows:
  - Entering the **show module** command displays the standby supervisor engine status as "error"
  - The active standby LED on the supervisor engine is red
  - The **show log** command displays "Active and standby supervisors are of different card types"

  Workaround: Reload the switch. This problem is resolved in software release 6.4(16). (CSCea16228)

- With a Supervisor Engine 2/MSFC2 in truncated mode with SRM configured on the MSFC2, the FPOE for hardware broadcasts is not set properly after resetting the designated MSFC2. When this problem occurs, traffic from fabric-enabled modules to nonfabric enabled modules is dropped.

  Workaround: Change the switching mode to compact or use software release 6.4(13) or earlier releases. This problem is resolved in software release 6.4(16). (CSCeg84506)

- After uploading and downloading both default and nondefault configurations to and from a TFTP server, the "set mmls nonrpf timer 10" entry might mistakenly appear in the **show config all** command output as follows:

```
Console> (enable) show conf all
/snip/
#mmls nonrpf
set mmls nonrpf enable
set mmls nonrpf timer 60
set mmls nonrpf window 10
set mmls nonrpf timer 10   <--- should be interval
```

  The second "set mmls nonrpf timer" entry should be "set mmls nonrpf interval." This problem is resolved in software release 6.4(16). (CSCeh20805)

- 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 6.4(16). (CSCsa42331)

- The **show tech-support** command might display configured passwords in text configuration mode. This problem is resolved in software release 6.4(16). (CSCeg17866)

- The Telnet access denied message includes "retry" timer information. The retry timer information has been removed in software release 6.4(16). (CSCeh18221)

Open and Resolved Caveats in Software Release 6.4(15)

These sections describe open and resolved caveats in supervisor engine software release 6.4(15):

Open Caveats in Software Release 6.4(15)

This section describes open caveats in supervisor engine software release 6.4(15):

- 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 that are 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 that is 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 6.4(15)

This section describes resolved caveats in supervisor engine software release 6.4(15):

- 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 occurs twice).

  Workaround: The problem does not occur if the EtherChannel mode is set to "on." This problem is resolved in software release 6.4(15). (CSCee76807)

- Out-Discard and Rcv-Octet counters increment on GBIC ports that are showing a "notconnect" status. This problem is resolved in software release 6.4(15). (CSCeg48512)

Open and Resolved Caveats in Software Release 6.4(14)

These sections describe open and resolved caveats in supervisor engine software release 6.4(14):

Open Caveats in Software Release 6.4(14)

This section describes open caveats in supervisor engine software release 6.4(14):

- After a high-availability switchover, LTLs might not be set correctly for MSFC ports 15/1 and 16/1. (CSCee03884)

  Note This problem was seen in earlier software releases but is not seen in the 6.4(14) and later software releases.

- 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 that are 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 that is 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 6.4(14)

This section describes resolved caveats in supervisor engine software release 6.4(14):

- 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 6.4(14). (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 6.4(14). (CSCdy79506)
- In text configuration mode, the SPAN sessions on the NAM, IDSM, 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 6.4(14). (CSCed65635)
- With PAgP, it might take an unusually long time for a trunk port to join an EtherChannel. This problem is resolved in software release 6.4(14). (CSCee95479)
- 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 6.4(14). (CSCef15158)
- 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 6.4(14). (CSCef51905)
- 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 6.4(14). (CSCef67073)
- 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 6.4(14). (CSCef77162)
- The **show tech-support** command does not display "outband counters." This problem is resolved in software release 6.4(14). (CSCef81144)
- 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 6.4(14). (CSCef81723)
- The **show tech** command should not display password information because this could create a security vulnerability. This problem is resolved in software release 6.4(14). (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 6.4(14). (CSCef88220)

- 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 6.4(14). (CSCeg05183)

- Manually configured MAC addresses on port security-enabled ports might age out. This problem is resolved in software release 6.4(14). (CSCin83482)

- With dual Supervisor Engine 2s and dual WS-6500-SFM modules running in truncated mode, the WS-X6516-GBIC module might fail to receive multicast traffic. The switch can send multicast traffic and there is no problem with unicast traffic on the problem port.

  Workaround: Force the system to run in bus-only mode, or use a single supervisor engine in the chassis. This problem is resolved in software release 6.4(14). (CSCee13437)

- 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 6.4(14). (CSCef43494)

Open and Resolved Caveats in Software Release 6.4(13)

These sections describe open and resolved caveats in supervisor engine software release 6.4(13):

- Open Caveats in Software Release 6.4(13), page 66
- Resolved Caveats in Software Release 6.4(13), page 67

Open Caveats in Software Release 6.4(13)

This section describes open caveats in supervisor engine software release 6.4(13):

- After a high-availability switchover, LTLs might not be set correctly for MSFC ports 15/1 and 16/1. (CSCee03884)

- 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 that are 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 that is 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 6.4(13)

This section describes resolved caveats in supervisor engine software release 6.4(13):

- 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 6.4(13). (CSCef66696)

- When the EOBC out-of-band management bus fault detection code tries to repower a module that is in the "power-deny" state, the switch may crash. This problem is resolved in software release 6.4(13). (CSCee59418)

- 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 6.4(12) in the 6.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 6.4(13). (CSCef32204)

- There is a vulnerability in the Transmission Control Protocol (TCP) specification (RFC 793). 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 6.4(13). (CSCed32349)

- 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 6.4(13). (CSCef18763)

- 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 6.4(13). (CSCef44617)

- 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 6.4(13). (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 possibilty 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 noticible 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 6.4(13). (CSCef39614)

Open and Resolved Caveats in Software Release 6.4(12)

These sections describe open and resolved caveats in supervisor engine software release 6.4(12):

- Open Caveats in Software Release 6.4(12), page 68
- Resolved Caveats in Software Release 6.4(12), page 68

Open Caveats in Software Release 6.4(12)

This section describes open caveats in supervisor engine software release 6.4(12):

- After a high-availability switchover, LTLs might not be set correctly for MSFC ports 15/1 and 16/1. (CSCee03884)
- 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 that are 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 that is 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 6.4(12)

This section describes resolved caveats in supervisor engine software release 6.4(12):

- 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 6.4(12). (CSCef38462)
- 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 6.4(12). (CSCee95922)

- After a switchover, the first module/link trap for any module/link might not be sent. This problem is resolved in software release 6.4(12). (CSCef27093)
- When running a K9 software image, the switch might crash when the SSH client tries to connect to the switch. This problem is resolved in software release 6.4(12). (CSCdz04272)
- In software release 6.4(12), 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)
- If the switch is peering with a multicast router through an ATM interface (either LANE or RFC1483 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 6.4(12). (CSCef27349)
- The switch might reset (%SYS-5-MOD_NOSCPPINGRESPONSE) when getting CBL information through a PERL script. This problem is resolved in software release 6.4(12). (CSCee62021)
- 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 6.4(12). (CSCee88608)
- 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 6.4(12). (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 6.4(12). (CSCeb69513)
- The switch might drop all EtherChannels configured to “desirable” mode for approximately 10 minutes and 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 6.4(12). (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 6.4(12). (CSCef06375)
- 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 6.4(12). (CSCec23277)
- The switch might crash with crashing function name po_ipu_get_adj_vlan_mac. This problem is resolved in software release 6.4(12). (CSCef00947)
- If port security is enabled on ports that have an auxiliary VLAN configured, no traffic switches on the auxiliary VLAN.

  Workaround: Disable port security. This problem is resolved in software release 6.4(12). (CSCef14201)

- 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 unreachables** are configured and protocol filtering is enabled.

  Workaround: Reset the switch to clear the problem. This problem is resolved in software release 6.4(12). (CSCee69960)

- The value of dot1dStpPortDesignatedPort is not correct when queried from SNMP. This problem is resolved in software release 6.4(12). (CSCee94422)

- With UplinkFast enabled, invalid dummy multicast packets might be sent out from the switch resulting in a communication failure.

  Workaround: Clear the ARP cache. This problem is resolved in software release 6.4(12). (CSCee22626)

Open and Resolved Caveats in Software Release 6.4(11)

These sections describe open and resolved caveats in supervisor engine software release 6.4(11):

- Open Caveats in Software Release 6.4(11), page 70
- Resolved Caveats in Software Release 6.4(11), page 70

Open Caveats in Software Release 6.4(11)

This section describes open caveats in supervisor engine software release 6.4(11):

- After a high-availability switchover, LTLs might not be set correctly for MSFC ports 15/1 and 16/1. (CSCee03884)

- 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 that are 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 that is 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 6.4(11)

This section describes resolved caveats in supervisor engine software release 6.4(11):

- Spanning tree does not block ports 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 6.4(11). (CSCed84323)

- IPX unicast packets may be dropped on the ingress MSFC interface when IP ACLs, VACLs, and no IP redirects are configured. 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 6.4(11). (CSCee51617)

- 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. This problem is resolved in software release 6.4(11). (CSCee27955)

- 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 6.4(11). (CSCed92864)

- 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 6.4(11). (CSCee34175)

- When you enter the **shutdown** command followed by the **no shutdown** command on a loopback interface, and the same loopback interface address is also configured on two or more connected routers, the switch may crash with a FIB exception. This problem is resolved in software release 6.4(11). (CSCea50206)

- When resetting the designated MSFC, you might see “Incorrect_adj_ptr_fib” error messages. The frequency of these messages is proportional to the number of SVIs configured on the MSFC. Approximately two “Incorrect_adj_ptr_fib” messages are likely to be printed for every SVI configured on the MSFC. These messages can be ignored as they are not indications of actual SSRAM FIB errors. This problem is resolved in software release 6.4(11). (CSCed34657)

- When running the **show flash** or **show tech-support** commands, if you interrupt them by pressing **Ctrl-C**, the file system might lock for up to 30 minutes.

  Workarounds: 1) After entering the **show flash** command, do not interrupt it. 2) When you run the **show tech-support** command, interrupt it only after all the **show flash** information is displayed. This problem is resolved in software release 6.4(11). (CSCeb17930)

- Due to alias counters not being cleared, the switch might unnecessarily go into multicast IGMP fall-back mode. If this occurs, you might see multicast packet loss for existing groups as the multicast router ports time out.

  Workaround: Disable IGMP snooping. This problem is resolved in software release 6.4(11). (CSCea08633)

- 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 6.4(11). (CSCee43443)

- 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 6.4(11). (CSCed44129)

- 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 6.4(11). (CSCeb86233)

- With a Supervisor Engine 1 or 1A, the switch might reload with the following log message:

  ```
  ProcessStatusPing:Module 1 local SCP error detected... resetting module
  ```

  Workaround: Remove the faulty module. This problem is resolved in software release 6.4(11). (CSCea38268)

- Setting an existing entry in caqClassifierTable might cause a crash if there is an entry in caqIpAceTable in notInService state. The caqIpAceEntry must be linked to the entry in caqClassifierTable. This problem is resolved in software release 6.4(11). (CSCee27227)

- 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 6.4(11). (CSCee58481)

- The MSFC might not be able to ping the sc0 interface on VLAN 1. This is a reoccurrence of the problem seen in CSCeb02380. This problem is resolved in software release 6.4(11). (CSCee66310)

- In rare circumstances, 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 6.4(11). (CSCds12349)

- 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 6.4(11). (CSCee54278)

- IP phone traffic received on an untrusted port should match the configured QoS ACL but the DSCP based on the ACL is not rewritten. This problem is due to the wrong mask being used in the QoS ACL. The problem is caused by a CLI problem; the CLI asks for the IP mask but it should ask for a wild card. 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 6.4(11). (CSCec68825)
- An MSFC trunk might not be added to the spanning tree after a switchover in DRM. This problem is resolved in software release 6.4(11). (CSCee20623)
- In extremely rare conditions, the standby supervisor engine might not come up after resetting the switch.

  Workaround: Either reset the standby supervisor engine or delay the bootup of the standby supervisor engine. This problem is resolved in software release 6.4(11). (CSCee27392)
- 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 6.4(11). (CSCee57837)
- With a Supervisor Engine 2, when ports are added to an EtherChannel one port at a time, the calculated value of a path cost may be incorrect. In some cases, the path cost value displayed with the **show spantree mistp-instance** command is correct, but the path cost value displayed with the **show spantree statistics** command may be incorrect. Miscalculated path cost values result in ports going into the blocked state and creates spanning tree topology discrepancies. This problem with the MISTP path cost feature is seen in all software releases up to and including release 6.4(10). This problem is resolved in software release 6.4(11). (CSCee82347)
- 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 6.4(11). (CSCec50151)

Open and Resolved Caveats in Software Release 6.4(10)

These sections describe open and resolved caveats in supervisor engine software release 6.4(10):

- Open Caveats in Software Release 6.4(10), page 74
- Resolved Caveats in Software Release 6.4(10), page 75

Open Caveats in Software Release 6.4(10)

This section describes open caveats in supervisor engine software release 6.4(10):

- In extremely rare conditions, the standby supervisor engine might not come up after resetting the switch.

  Workaround: Either reset the standby supervisor engine or delay the bootup of the standby supervisor engine. (CSCee27392)

- After a high-availability switchover, LTLs might not be set correctly for MSFC ports 15/1 and 16/1. (CSCee03884)

- 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)

- 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 that are 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 that is 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 6.4(10)

This section describes resolved caveats in supervisor engine software release 6.4(10):

- TCP flags might not be shared properly. The ACL does not fit into the TCAM on the supervisor engine which results in this error message on the MSFC:

  ```
  %FM-4-TCAM_CAPMAP: Interface Vlan1 hardware TCAM LOU usage capability
  ```

  The problem happens only when you use BDD mode with the ACL. The end result is the allocation of duplicate LOU entries for TCP flags. A large number of ACEs creates a higher probability of allocating more duplicate TCP flags, causing the LOU CAPMAP FULL condition. This problem is resolved in software release 6.4(10). (CSCee12831)

- In rare circumstances, packets that are forwarded in hardware might have an incorrect source MAC address or might be forwarded to an incorrect next-hop destination.

  Workaround: Reset the supervisor engine. This problem is resolved in software release 6.4(10). (CSCdy87433)

- Debug port counters need to be enabled in software release 6.x(x). The debug port counters feature reports critical syslog errors such as the following: 0xC5—Bad Header Checksum on D-Bus, 0xC6—Bad Header Checksum on R-Bus, 0xC7—Bad Packet CRC in D-Bus, 0xC8—Bad Length on D-Bus, and 0x159—Packet CRC on R-Bus. This problem is resolved in software release 6.4(10). (CSCec85662)

- 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 shutdown, so there should be outgoing traffic seen on the port. This problem is resolved in software release 6.4(10). (CSCed46961)

- A TACACS+ server might not record accounting information if you input two consecutive commands by copying and pasting in the commands. This problem is resolved in software release 6.4(10). (CSCec63892)

- When using either 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 6.4(10). (CSCed91504)

- The switch might crash with the crashing function name: no_change. This problem is resolved in software release 6.4(10). (CSCdy54706)

- 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 6.4(10). (CSCee02504)

- On a switch running a cryptographic (k9) image, if the value of sshPublicKeySize is non-zero, the SNMP_THREAD process might have a memory leak when sshPublicKeySize is polled. This problem is resolved in software release 6.4(10). (CSCed95950)
- 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, then 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 6.4(10). (CSCec19091)
- 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 6.4(10). (CSCed87627)

  Note While caveat CSCed87627 is resolved in software release 6.4(10), caveat CSCee27955 is open in software release 6.4(10) 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 6.4(10)" section on page 74.

- When a system with a Supervisor Engine 1A/MSFC or MSFC2 is reset, modules may not come online. Entering the **show module** command shows that the modules are in the "other" state. Supervisor Engine 1A systems without an MSFC/MSFC2 are not affected.

  Workaround: Set the diagnostics level to bypass by entering the **set test diaglevel bypass** command. This problem is resolved in software release 6.4(10). (CSCee15779)
- When running MMLS on a Supervisor Engine 1/MSFC with partial-SCs, clearing the mroute table or disabling and then enabling MLS on the MSFC might cause packets to stop being switched on partial-SCs 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 no "H" flags set.

  Workarounds: 1) Reload the MSFC. 2) Change the incoming interface MTU to match the outgoing interface MTU. When the "H" flag appears in the mroute partial-SC entry, the problem goes away. 3) Disable MMLS on the MSFC using the **no mls ip multicast** command. This problem is resolved in software release 6.4(10). (CSCed41953)

Open and Resolved Caveats in Software Release 6.4(9)

These sections describe open and resolved caveats in supervisor engine software release 6.4(9):

Open Caveats in Software Release 6.4(9)

This section describes open caveats in supervisor engine software release 6.4(9):

- After a high-availability switchover, MSFC ports 15/1 and 16/1 go into the errdisable state. This problem is seen only if you enable inband error detection which is disabled by default.

  Workaround: Reset the MSFC. (CSCed90810)

  Note After further testing, this bug could not be recreated. We believe that the problem is similar to the problem that is causing caveat CSCee03884 which is listed in the "Open Caveats in Software Release 6.4(10)" section on page 74.

- 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 that are 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 that is 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 6.4(9)

This section describes resolved caveats in supervisor engine software release 6.4(9):

- 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. The workaround is to press the **Enter** key to get to the Catalyst switch prompt. This problem is resolved in software release 6.4(9). (CSCed45576)
- Under rare conditions, the following switching modules might reset when a link is rapidly going up and down: WS-X6248-RJ45, WS-X6248-TEL, WS-X6348-RJ45, WS-X6348-RJ21, WS-X6148-RJ45, WS-X6148-RJ21, and WS-X6348-100FX. The link must go from down to up to down within 300 ms. This problem affects all releases of Catalyst software and Cisco IOS software. The workaround is to disable the rapidly flapping port, or fix the root cause of the link flap. This problem is resolved in software release 6.4(9). (CSCed17719)
- In the event of an SRAM failure detection, the process to power cycle the module does not exit after the power cycle is complete. This problem is resolved in software release 6.4(9). (CSCed49629)
- In a redundant system, an MSFC trunk port may go to errdisabled state. This problem has been seen after the standby supervisor engine boots up with a different image than the active supervisor engine. There are two workarounds: 1) Remove and reseat the supervisor engine reporting the errdisabled state. 2) Reset the supervisor engine reporting the errdisabled state using the **reset** command. After the supervisor engine comes up, reset the MSFC. This problem is resolved in software release 6.4(9). (CSCed03243)

- After lowering the number of MAC addresses that can be configured using the **set port security** *mod/port* **maximum** *num_of_mac* command, entering the **clear port security all** command might not clear all the secured addresses from the configuration. This problem might be seen in software release 6.4(8) or earlier releases, software release 7.6(5) or earlier releases, and software release 8.2(1) or earlier releases.

  Workaround: Set the maximum number of MAC addresses allowed to a higher value and then enter the **clear port security all** command. This problem is resolved in software release 6.4(9). (CSCin66276)

- 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 6.4(9). (CSCec00993)

- When logging into a switch 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. The workaround is to 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 6.4(9). (CSCdz16477)

- The switch might not send dummy multicast packets when UplinkFast operates after the **no shutdown** command has been entered from the original root port. This condition results in lost communication because the switch does not clear the older MAC table on the root port. This problem is resolved in software release 6.4(9). (CSCec79652)

- 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 6.4(9). (CSCed43310)

- 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. The workaround is to change the logging level on the SPANTREE facility down to level 4. This problem is resolved in software release 6.4(9). (CSCeb78548)

- When the cache error handler is called on a Supervisor Engine 2, the status register shows the wrong value (0xffffff83). This behavior hides the real register value and hinders debugging. This problem is resolved in software release 6.4(9). (CSCed79489)

- Under rare conditions with SPAN disabled, traffic may not be sent outbound on a port in a fabric-enabled system due to a misprogramming of the ports FPOE (fabric port of exit) on the ingress module. There are three workarounds: 1) Enable SPAN for the egress port (the port should be the source of the SPAN session). 2) Soft reset the egress module. 3) Configure the SPAN destination port to be less than port 33 in the range of ports, the port should be between 1 and 32. This problem is resolved in software release 6.4(9). (CSCed56130)

- 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 6.4(9). (CSCed48590)

- 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.
  - Login 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 6.4(9). (CSCed76069)
- You might receive traps indicating configuration revision errors, and 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 6.4(9) and then you need to add and delete a VLAN. This problem is resolved in software release 6.4(9). (CSCdy11099)
- 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 6.4(9). (CSCec57893)

Open and Resolved Caveats in Software Release 6.4(8)

These sections describe open and resolved caveats in supervisor engine software release 6.4(8):

- Open Caveats in Software Release 6.4(8), page 79
- Resolved Caveats in Software Release 6.4(8), page 80

Open Caveats in Software Release 6.4(8)

This section describes open caveats in supervisor engine software release 6.4(8):

- 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 that are 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 that is 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 6.4(8)

This section describes resolved caveats in supervisor engine software release 6.4(8):

- You can now disable and enable the IGMP rate-limit feature and set the rate limit for IGMP snooping packets by using the **set igmp ratelimit** command as follows:

  set igmp ratelimit {**enable** | **disable**}
  set igmp ratelimit {**dvmrp** | **general-query** | **mospf1** | **mospf2** | **pimv2**} *rate*

  IGMP rate limiting is disabled by default. The default value for each rate-limit counter is 100. This problem is resolved in software release 6.4(8). (CSCin53701)

- 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 6.4(8). (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 6.4(8). (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 situation causes the MLS receive entry to disappear on the switch side 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 6.4(8). (CSCed30949)

- Entering the **copy config flash** command might cause the Supervisor Engine 1A to reset. This problem is resolved in software release 6.4(8). (CSCdy21260)

- A switch running software release 6.4(7) might not save the configuration for the IGMP rate limit after a reload. This problem is resolved in software release 6.4(8). (CSCed09426)

- MLS IP fast aging might not work correctly. This problem is resolved in software release 6.4(8). (CSCec70012)

- The MMLS shortcuts between the supervisor engine and the MSFC might not be consistent. This problem is resolved in software release 6.4(8). (CSCec65498)

- A switch running software release 6.4(2) with the WS-X6K-SUP1-PFC supervisor engine might stop marking the DSCP to incoming packets.

  Workaround: Add a new ACL to trigger a reprogramming in the TCAM. This problem is resolved in software release 6.4(8). (CSCeb32983)

- When using SSH to the switch using external authentication, if you enter a blank username (that is, 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 6.4(8). (CSCea89170)

- A switch running software release 6.4(7) with an EtherChannel connection and with spanning tree PortFast enabled might experience intermittent connectivity when a port in the channel is removed and then added back to the channel. When this problem is seen, the EtherChannel reports an increasing amount of in-discards.

  Workaround: Disable spanning tree PortFast on all ports in the EtherChannel or downgrade to software release 6.4(6) or an earlier release. This problem is resolved in software release 6.4(8). (CSCed08505)

- 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 joining 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 6.4(8). (CSCed12056)

- 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.

  Workarounds: Enter the **shutdown** command followed by the **no shutdown** command on the VLAN interfaces. This problem is resolved in software release 6.4(8). (CSCec43550)

Open and Resolved Caveats in Software Release 6.4(7)

These sections describe open and resolved caveats in supervisor engine software release 6.4(7):

- Open Caveats in Software Release 6.4(7), page 81
- Resolved Caveats in Software Release 6.4(7), page 82

Open Caveats in Software Release 6.4(7)

This section describes open caveats in supervisor engine software release 6.4(7):

- 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 that are 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 that is 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 6.4(7)

This section describes resolved caveats in supervisor engine software release 6.4(7):

- MDIX does not work properly on the WS-X6548-RJ-45 module. If you connect a PC to a port on a WS-X6548-RJ-45 module using a straight-through cable, the port comes online, but if you change the cable to a crossover cable, the port does not come online. This problem is resolved in software release 6.4(7). (CSCec17508)
- When an end station sends PAUSE frames to a switch port that has flow control disabled, the PAUSE frames are sent to the supervisor engine, resulting in high CPU utilization. The workaround is to enable receive flow control on the port receiving the PAUSE frames. This problem is resolved in software release 6.4(7). (CSCec00232)
- When the fabric mode changes from flow-through mode to truncated mode in a switch with redundant Switch Fabric Modules, there will be synchronization errors from the active Switch Fabric Module, resulting in the active Switch Fabric Module being powered down. This problem is resolved in software release 6.4(7). (CSCeb24672)
- 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 6.4(7). (CSCec18911)
- MLS entries in the supervisor engine forwarding information base are not updated after a server failover although the ARP entry is correct. 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. This problem is resolved in software release 6.4(7). (CSCec27027)
- From the active supervisor engine, when you perform a squeeze on the bootflash on the standby supervisor engine using the **squeeze** *mod/bootflash:* command and then abort the command by choosing **no** from the "delete files proceed" option, the standby supervisor engine file system remains locked. The workaround is to reset the switch. This problem is resolved in software release 6.4(7). (CSCec47607)
- With a Firewall Services Module (FWSM), LTLs might not be set properly if VTP pruning is enabled. This problem is resolved in software release 6.4(7). (CSCea04936)
- The following combination of PAgP and DTP results in incorrect forwarding of traffic for Ethernet ports on initial link up: PAgP = Auto, DTP = Off. Specifically, ports with this PAgP/DTP configuration are forwarding traffic prior to the port joining the bridge group. There should be a 10-second delay before traffic gets forwarded. This problem is resolved in software release 6.4(7). (CSCec41056)
- When you enter the **squeeze slot0:** command, the CPU usage will spike above 95 percent for about 30 seconds. The workaround is to use the **squeeze** command during a maintenance window. This problem is resolved in software release 6.4(7). (CSCec25582)
- The port ifIndex on a Supervisor Engine 1 might become 0 after a high-availability switchover. This problem is resolved in software release 6.4(7). (CSCec44842)
- 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 6.4(7). (CSCeb36759)
- 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. The workaround is to enable and disable the ports again. This problem is resolved in software release 6.4(7). (CSCec63559)

- If you enter the **show acl index** command and CPU utilization rises sharply, you may start losing some control packets, such as UDLD, BPDU, MLS, and MMLS. The workaround is to not use the command. This problem is resolved in software release 6.4(7). (CSCec73483)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN that is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate-limit values correctly. To set the IGMP rate-limit values correctly, see the description in these release notes for caveat CSCea44331. Caveat CSCeb21548 is resolved in software release 6.4(7). (CSCeb21548)

Open and Resolved Caveats in Software Release 6.4(6a)

These sections describe open and resolved caveats in supervisor engine software release 6.4(6a):

- Open Caveats in Software Release 6.4(6a), page 83
- Resolved Caveats in Software Release 6.4(6a), page 84

Open Caveats in Software Release 6.4(6a)

This section describes open caveats in supervisor engine software release 6.4(6a):

- With multicast 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 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. (CSCea44331)
- 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 that are 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 that is 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)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries that can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(6a)

This section describes resolved caveats in supervisor engine software release 6.4(6a):

- Under rare conditions, the following switching modules might reset when a link is rapidly going up and down: WS-X6248-RJ45, WS-X6248-TEL, WS-X6348-RJ45, WS-X6348-RJ21, WS-X6148-RJ45, WS-X6148-RJ21, and WS-X6348-100FX. The link must go from down to up to down within 300 ms. This problem affects all releases of Catalyst software and Cisco IOS software. The workaround is to disable the port that is rapidly going up and down, or fix the root cause of this condition. This problem is resolved in software release 6.4(6a). (CSCed17719)

Open and Resolved Caveats in Software Release 6.4(6)

These sections describe open and resolved caveats in supervisor engine software release 6.4(6):

- Open Caveats in Software Release 6.4(6), page 84
- Resolved Caveats in Software Release 6.4(6), page 85

Open Caveats in Software Release 6.4(6)

This section describes open caveats in supervisor engine software release 6.4(6):

- With multicast 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 is to increase the PimV2-hellos ratelimit; 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. (CSCea44331)
- 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 that are 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 that is 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)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(6)

This section describes resolved caveats in supervisor engine software release 6.4(6):

- The **set port disable** and **set port enable** commands might not work correctly if a port list is specified. This problem is resolved in software release 6.4(6). (CSCdw73671)
- 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 6.4(6). (CSCea72986)
- In IGMP fallback mode, the switch might forward only UDP packets that are 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. The workaround is to configure a static multicast MAC entry for 01-00-5e-00-00-09 on ports that are connected to RIP version 2 routers. This problem is resolved in software release 6.4(6). (CSCeb53428)
- The WS-X6348-RJ-45 module might excessively reset. When these resets 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 6.4(6). (CSCeb35612)
- 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. The workaround is to reset the system. This problem is resolved in software release 6.4(6). (CSCea19802)
- With the spanning tree mode is 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. The workaround is to disable and then reenable the port (this might not always work), or change the channel mode to "desirable." This problem is resolved in software release 6.4(6). (CSCea48516)
- 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 6.4(6). (CSCeb61525)
- It is not possible to configure more than 64 non-default trunk ports in the extended VLAN range when using text configuration mode. This problem is resolved in software release 6.4(6). (CSCec22739)
- A switch with either a WS-X6K-SUP1A-2GE or WS-X6K-S2U-2GE supervisor engine and a WS-F6K-MSFC2 running Cisco IOS Release 12.1(19)E boot loader image version 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 that is switched within VLAN 1 is not affected. This problem may occur when running any version of Catalyst software on the supervisor engine and Cisco IOS Release 12.1(19)E boot loader image version on the MSFC2. Traffic will still pass to and from the MSFC2 for all other VLANs. There are two workarounds: 1) Enter the **shutdown** command followed by the **no shutdown** command on the VLAN 1 virtual interface on the MSFC2. This workaround 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), you can avoid this problem by downgrading only the boot loader image to Cisco IOS Release 12.1(13)E. This problem is resolved in software release 6.4(6). (CSCeb02380)

- 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. The workaround is to use “desirable” mode or binary configuration mode. This problem is resolved in software release 6.4(6). (CSCec06429)
- If port security is enabled and in restrictive mode, MAC address movement between secured ports does not cause the ports to shut down. Also, MAC address movement between secured ports clears the MAC address of the ports from the static CAM. The workaround is to configure the port in shutdown mode to shut down the port on detection of MAC address movement (MAC address movement is a security breach). This problem is resolved in software release 6.4(6). (CSCin55891)
- 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 6.4(6). (CSCec19186)

Open and Resolved Caveats in Software Release 6.4(5b)

These sections describe open and resolved caveats in supervisor engine software release 6.4(5b):

- Open Caveats in Software Release 6.4(5b), page 86
- Resolved Caveats in Software Release 6.4(5b), page 87

Open Caveats in Software Release 6.4(5b)

This section describes open caveats in supervisor engine software release 6.4(5b):

- With multicast 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 is to increase the PimV2-hellos ratelimit; 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. (CSCea44331)
- 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 that are 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 that is 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)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(5b)

This section describes resolved caveats in supervisor engine software release 6.4(5b):

- With MISTP configured, when a non-root switch attempts to be the root switch, a TLB exception might occur. These TLB exceptions can occur each time there is a root change, which can trigger a MISTP_VM update on all the non-root switches for the new root. This problem is resolved in software release 6.4(5b). (CSCeb60477)

Open and Resolved Caveats in Software Release 6.4(5a)

These sections describe open and resolved caveats in supervisor engine software release 6.4(5a):

- Open Caveats in Software Release 6.4(5a), page 87
- Resolved Caveats in Software Release 6.4(5a), page 88

Open Caveats in Software Release 6.4(5a)

This section describes open caveats in supervisor engine software release 6.4(5a):

- With multicast 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 is to increase the PimV2-hellos ratelimit; 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. (CSCea44331)
- 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 that are 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 that is 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)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(5a)

This section describes resolved caveats in supervisor engine software release 6.4(5a):

- On WS-X6348 modules, connections between a port connected to a PC with a cable length of 60 meters may continuously go down and back up. This problem occurs when the PC NIC does not conform to the IEEE 802.3 pulse shape mask for MLT3.

  Workaround: Reduce the cable length by about 10 meters or move the cable to another port. This problem is resolved in software release 6.4(5a). (CSCdz46928)

Open and Resolved Caveats in Software Release 6.4(5)

These sections describe open and resolved caveats in supervisor engine software release 6.4(5):

- Open Caveats in Software Release 6.4(5), page 88
- Resolved Caveats in Software Release 6.4(5), page 89

Open Caveats in Software Release 6.4(5)

This section describes open caveats in supervisor engine software release 6.4(5):

- With multicast 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 is to increase the PimV2-hellos ratelimit; 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. (CSCea44331)
- 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 that are 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 that is 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)
- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(5)

This section describes resolved caveats in supervisor engine software release 6.4(5):

- In rare circumstances, IPX traffic may be affected when an IP-input access list is applied. The workaround is to create an IPX access list that permits everything and apply it on the input interface. The IPX access list results in an explicit IPX ACL being programmed into the TCAM.

  To create the IPX access list, do the following in global configuration mode:

  ```
  access-list 800 permit -1 -1
  ```

  On the interface do the following:

  ```
  ipx access-group 800 in
  ```

  Because ACLs are processed in hardware, there is no performance penalty for this workaround. This problem is resolved in software release 6.4(5). (CSCdx17914)

- In text configuration mode, you might see the following message when booting the switch:

  ```
  %SYS-3-PORT_DEVICENOLINK:Device on port <mod>/<port> powered but no link up
  ```

  The ports recover and continue to function normally when you are running the following software releases:

  - 6.3(7) and earlier
  - 7.1(x) and 7.2(x)

  In addition to the above behavior, some ports might be powered down randomly followed by these messages after a reload:

  ```
  %SYS-3-PORT_DEVICENOLINK:Device on port <mod>/<port> powered but no link up
  %SYS-3-PORT_BADPORT:Bad port <mod>/<port> detected, inline power is turned off
  ```

  The messages might display when you are running the following software releases:

  - Software release 6.3(8-10) and later
  - Software release 7.3(2) and 7.4(2-3)

  The workaround is as follows:

  - Run the configuration in binary mode (the default)
  - When it is not possible to run in binary mode (such as when you have a fully loaded Catalyst 6513 switch or heavily configured Catalyst 6509 switch), set the inline power status to automatic after every reload.

  This problem is resolved in software release 6.4(5). (CSCeb43635)

- After a VLAN is cleared from a channeled port by entering the **clear trunk** command, channeled ports disappear from the list of ports when you enter the **show spantree mistp-instance** command. This problem is resolved in software release 6.4(5). (CSCeb13778)

- A WS-X6348-RJ-45 module port might randomly become stuck when connected to other vendor firewalls and DNS servers. The workaround is to disable and then reenable the port using the **set port disable** *mod/port* and **set port enable** *mod/port* commands. This problem is resolved in software release 6.4(5). (CSCdz24626)

- A Supervisor Engine 1A/MSFC running software release 6.4(4) might lose multicast traffic when the incoming interface is a FlexWAN module, the outgoing interface is a VLAN, and IGMP is disabled on the switch. In this situation, the MSFC stops receiving the incoming multicast traffic. This problem is seen when IGMP is enabled and then disabled. If the switch is booted with IGMP disabled, traffic still flows. The workaround is to enable IGMP on the switch. This problem is resolved in software release 6.4(5). (CSCeb48693)
- The system message "Check possible fault in standby supervisor" is misleading because the possible causes might not be related to the standby supervisor engine. This message is part of the inband ping failure message and NVLOGs. This problem is resolved in software release 6.4(5). (CSCeb18736)
- The dot1dBasePortTable of the bridge MIB does not contain all of the ports where VLAN 1 is declared. This problem is resolved in software release 6.4(5). (CSCeb08072)
- The NVRAM log may not completely clear itself after registering an exception (and logging a switching bus timeout). Subsequent exceptions may have truncated stack pointers due to improper clearing of the NVRAM log. The workaround is to manually clear the NVRAM log using the **clear log** command. This problem is resolved in software release 6.4(5). (CSCeb28192)
- 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 only returns the hostname. 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. The workaround is to specify the complete FQDN on the switch so sysName returns the complete FQDN. An example follows:

  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.
  ```

  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 6.4(5). (CSCeb37492)
- Entering the **show rgmp group** command might crash the switch. This problem is resolved in software release 6.4(5). (CSCea84886)
- With a WS-X6381-IDS module installed, you might experience a memory leak over a period of weeks. The workaround is to reload the switch every few weeks to regain lost memory. This problem is resolved in software release 6.4(5). (CSCeb59206)

Open and Resolved Caveats in Software Release 6.4(4a)

These sections describe open and resolved caveats in supervisor engine software release 6.4(4a):

Open Caveats in Software Release 6.4(4a)

This section describes open caveats in supervisor engine software release 6.4(4a):

- 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 that are 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 that is 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)

- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(4a)

This section describes resolved caveats in supervisor engine software release 6.4(4a):

- IGMP multicast entries are not removed from the CAM table. This problems is resolved in software release 6.4(4a).(CSCeb34010)

Open and Resolved Caveats in Software Release 6.4(4)

These sections describe open and resolved caveats in supervisor engine software release 6.4(4):

Open Caveats in Software Release 6.4(4)

This section describes open caveats in supervisor engine software release 6.4(4):

- 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 that are 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 that is 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)

- When IGMP snooping attempts to clear all multicast entries for a given VLAN (as a result of aging out the last multicast router port in the VLAN which is related to caveat CSCea44331), IGMP snooping fails to clear all of the Layer 3 multicast entries corresponding to the VLAN. This problem might leave outdated Layer 3 multicast entries which can cause data disruption of multicast flows. To avoid encountering caveat CSCea44331, you need to set the IGMP rate limit values correctly. To set the IGMP rate limit values correctly, see the description in these release notes for caveat CSCea44331. (CSCeb21548)

Resolved Caveats in Software Release 6.4(4)

This section describes resolved caveats in supervisor engine software release 6.4(4):

- Entering the **ping -s** *ip_address* command (where *ip_address* is an unreachable address) does not display a "ping:Dest Unreachable response from <*default_gateway*>*"* message. This issue is seen only in software release 5.5(3) and later releases, and in software releases 6.x and 7.x. This problem is resolved in software release 6.4(4). (CSCdx03359)

- With a WS-X6348 module, a port might be errdisabled by a late collision and display the following error message:

  ```
  2002 Oct 03 11:09:22 JST +09:00 %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
  2002 Oct 03 11:09:24 JST +09:00 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
  2002 Oct 03 11:10:45 JST +09:00 %SYS-3-PORT_COLL:Port 3/1 late collision (100) detected
  2002 Oct 03 11:10:45 JST +09:00 %SYS-3-PORT_COLLDIS:Port 3/1 disabled due to collision
  2002 Oct 03 11:10:45 JST +09:00 %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
  ```

  This problem is resolved in software release 6.4(4). (CSCdz41466)

- NDE is not exporting statistics for software-installed flows. This problem is resolved in software release 6.4(4). (CSCdz70415)

- In rare circumstances, a Supervisor Engine 1A running software release 6.3(5) might crash with the "getPermTypeValue" function. This problem is resolved in software release 6.4(4). (CSCea11480)

- In rare circumstances, MLS entries might not get aged out. This could hinder hardware switching for new flows. This problem is resolved in software release 6.4(4). (CSCea19439)

- The **set module power down** *mod* command might not work when a faulty module is in the slot. This problem is resolved in software release 6.4(4). (CSCea57097)

- A Supervisor Engine 1 with MSFC running software release 6.3(8) might stop hardware switching multicast flows if the xtag is not set correctly. The workaround is to use the **clear ip mroute** *group-address* command. This problem is resolved in software release 6.4(4). (CSCea58832)
- With RMON enabled, you might see a crash in the mediaIndependentTable when a module is removed and reinserted. This problem is resolved in software release 6.4(4). (CSCea70981)
- A single character tag behaves incorrectly when being configured in snmpCommunityTable and snmpTargetAddrTable. The problem exists in software releases 6.3(x), 6.4(1-3), 7.1(x)-7.5(x), and 7.6(1). This problem is resolved in software release 6.4(4). (CSCea81905)
- A WS-X6101 ATM module running Cisco IOS Release 12.1(14)E1 might be reset by the supervisor engine when high rates of traffic are sent though the module. If this problem occurs, the supervisor engine reports the following error message:

  ```
  %SYS-5-MOD_NOSCPPINGRESPONSE:Module 3 not responding... resetting module
  %SYS-5-MOD_RESET:Module 3 reset from Software
  ```

  This problem occurs when approximately 500 Mbps of traffic is sent through the ATM module over multiple PVCs. The problem is only seen when the ILMI PVC is configured on the WS-X6101 module and ILMI keepalives are enabled. The workaround is to disable ILMI keepalives using the **no atm ilmi-keepalive** interface command or use the **set poll disable** *atm_module_num* command on the supervisor engine. This problem is resolved in software release 6.4(4). (CSCeb11528)
- In a switch with an ATM module, SNMP queries might timeout. This problem is resolved in software release 6.4(4) and ATM software releases 12.0(26)W5(28a) and 12.1(20). (CSCea04300)
- The CISCO-STACK-MIB trap sends an invalid systemGrp. There is no workaround. This problem is resolved in software release 6.4(4). (CSCeb04226)
- The switch might crash with the crashing function name: polarisGetPktByteCount. This crash might happen when recovering from sequence errors. In some cases, reseating the supervisor engine fixes the problem. This problem is resolved in software release 6.4(4). (CSCdy83905)
- With IGMP snooping configured, PIMv2 Hello packets might not be sent to the CPU. With this problem, the multicast traffic reduction features do not work. This problem is resolved in software release 6.4(4). (CSCea63674)

Open and Resolved Caveats in Software Release 6.4(3)

These sections describe open and resolved caveats in supervisor engine software release 6.4(3):

- Open Caveats in Software Release 6.4(3), page 94
- Resolved Caveats in Software Release 6.4(3), page 94

Open Caveats in Software Release 6.4(3)

This section describes open caveats in supervisor engine software release 6.4(3):

- 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 that are 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 that is 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 6.4(3)

This section describes resolved caveats in supervisor engine software release 6.4(3):

- If you repeatedly insert and remove (about 20 times) a 24-MB PCMCIA card, the system may reset. This problem is resolved in Release 6.4(3). (CSCdu58667)
- On a system with a Supervisor Engine I or II running Release 6.3(3) with SPAN configured and a permanent multicast CAM entry configured on the SPAN source port, packets destined to the multicast address are not forwarded on the SPAN destination port. The packets are forwarded on the source port. This problem is resolved in software release 6.4(3). (CSCdw30315)
- In a redundant multicast router configuration where the DR and NDR are both Supervisor Engine 1/MSFC2 and the **mls ip mul stub** command is configured on the NDR VLAN interfaces, the PIM assert mechanism does not work after the DR fails and comes back online. After the DR comes back online, the multicast receiver on each VLAN receives twice as much multicast traffic for about 3 minutes. If IGMP snooping is disabled, the PIM assert mechanism works correctly. This problem is resolved in software release 6.4(3). (CSCdx2137)
- In a redundant configuration, a functional Supervisor Engine 2 may incorrectly switch over to the secondary Supervisor Engine 2. This problem is resolved in software release 6.4(3). (CSCdz57291)
- The system does not synchronize local time through Network Time Protocol (NTP) when summertime is configured or changed. This problem is resolved in software release 6.4(3). (CSCdx42695)
- Testing has shown that for small frames (64 bytes to 86 bytes), the sum of the VLAN Layer 3 receive (Rx) rates is much lower than the configured policer rate. This problem of small packets not being policed at the full rate configured for the aggregate policer is also seen with VLAN and port policers, native VLAN and trunk links, various policer and transmit (Tx) rates, single SA/DA address pairs, and a range of source/destination IP address pairs (512 pairs). For all frame sizes above 86 bytes (various frame size, policer rate, Tx rate), the sum of the VLAN Layer 3 Rx rates was equal to the policer. The smaller the packet size (starting with 64 bytes), the lower the Rx rate. When packets are 86 bytes and larger, the Rx rate possible is 100 percent of the configured rate. This problem is resolved in software release 6.4(3). (CSCdx92093)
- Startup diagnostics may fail when a module fails to boot up. This problem is resolved in software release 6.4(3). (CSCdy03002)

- The NetFlow collector start time and end time are equivalent. This problem will cause inaccuracy of data billing. This problem is resolved in software release 6.4(3). (CSCdy04889)
- If you have two EtherChannels on a switch, after an upgrade, you might see the same ifIndex assigned in the ifTable for the interfaces that represent both channels. This problem is resolved in software release 6.4(3). (CSCdy52937)
- All members of a PAgP port-channel that should be enabled to forward traffic for some multicast groups may not actually be enabled. As a result, traffic for these multicast groups may be intermittently received or not received at all. The workaround is to disable and then enable IGMP snooping. This problem affects both nonredundant and redundant systems (systems with one or two supervisor engines). This problem is resolved in software release 6.4(3). (CSCdz07412)
- A Catalyst 6500 series switch with a Supervisor Engine 1 and no MSFC installed drops multicast packets. When channels go down or ports in a channel go down, a short data outage occurs and shortcut miss counters start to increment. This problem is resolved in software release 6.4(3). (CSCdz83125)
- IGMP snooping in the fallback mode freezes the state of host ports that can lead to the loss of multicast router ports and associated multicast MLS shortcuts on the supervisor engine. When the router port age out timer kicks in, Layer 2 entries get cleared which also causes Layer 3 entries to be cleared. This problem is resolved in software release 6.4(3). (CSCdz89562)
- The IGMP group table is not deleted from the MSFC when the router receives an IGMPv2 leave from the last group member. Additionally, the interface is not removed from the OIL and the MMLS entry is not deleted. This problem is resolved in software release 6.4(3). (CSCea03345)
- Certain QoS ACL names are not read correctly, and the system fails to commit the ACLs to runtime and to clear them. For example, configuring and committing a QoS ACL named “ipphone” and another ACL named “ipphone17-18” will not work. As consequence, the ACL named “ipphone17-18” will not be committed to runtime and will not be cleared. This problem is resolved in software release 6.4(3). (CSCea18569)
- The ciscoMemoryPoolUsed MIB and ciscoMemoryPoolFree MIB report incorrect NVRAM values. SNMP reports more NVRAM used. This problem is resolved in software release 6.4(3). (CSCea46369)
- A TTL of 32 is too low for some implementations. A TTL of 32 may decrement before the packets get out of a MPLS network. This situation can cause problems with any IP-based application. This problem is resolved in software release 6.4(3). (CSCea48092)
- A Catalyst 6500 series switch or Cisco 7600 series router with a redundant supervisor engine configuration might display the following messages:

  ```
  2001 Nov 06 13:23:59 met +01:00 %SYS-2-MOD_NOINBANDRESPONSE:Module 2 notresponding
  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 6.4(3). (CSCdx03048)
- The **show asicreg** *mod/port mii_phy* counters CLI does not work. This problem is resolved in software release 6.4(3). (CSCdz26435)

Open and Resolved Caveats in Software Release 6.4(2)

These sections describe open and resolved caveats in supervisor engine software release 6.4(2):

Open Caveats in Software Release 6.4(2)

This section describes open caveats in supervisor engine software release 6.4(2):

- 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 that are 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 that is 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 6.4(2)

This section describes resolved caveats in supervisor engine software release 6.4(2):

- In a redundant configuration where the active MSFC is the primary HSRP router for a VLAN and an external router is the standby HSRP router for the VLAN, if HSRP preemption is not configured on the VLAN, the standby MSFC will come up as the HSRP standby router for that VLAN after a switchover. However, the CAM table retains the HSRP MAC address of the MSFC that was active before the switchover. As a result, attempts to ping the HSRP IP address on the new active Catalyst 6500 will fail because the old CAM entry will cause packets to be redirected to the inactive MSFC.
  Workaround: Configure HSRP standby preemption on the Catalyst 6500 when you enter the interface configuration for the VLAN. When you configure HSRP standby preemption, after a switchover, the new active MSFC will come up as active HSRP router for that VLAN. This problem is resolved in software release 6.4(2). (CSCdy50639)
- In a redundant Catalyst 6500 configuration with core dump enabled, the uplink ports remain connected after a supervisor engine reset. This behavior causes spanning tree and connectivity problems. These problems continue for the duration of the core dump operation.
  Workaround: Disable the core dump feature on each supervisor engine, or make sure that the uplink ports are not in use when the core dump is enabled. This problem is resolved in software release 6.4(2). (CSCea03215A)
- On a Catalyst 6500 series switch running software release 6.4(1), the WS-X6148 and WS-X6348 modules respond differently to the **set feature agg-link-partner enable** global command. This problem is resolved in software release 6.4(2). (CSCea19099)
- If you have two EtherChannels on a switch, after an upgrade, you might see the same ifIndex assigned in the ifTable for the interfaces that represent both channels. This problem is resolved in software release 6.4(2). (CSCdy52937)

- In rare circumstances, a dynamic CAM entry pointing to port 16/62 can be created when QoS is enabled and multicast data traffic is flowing in the system. This problem could result in connectivity loss when unicast packets are destined to the MAC address shown as part of the CAM entry. The workaround is to clear the CAM entry and disable QoS globally. This problem exists in all 6.x software releases. This problem is resolved in software release 6.4(2). (CSCdz72304, CSCdw36426)
- The integrated CiscoView image sends the wrong user ID to the RADIUS server during authentication. This problem is resolved in software release 6.4(2). (CSCdz18313)
- Prior to software release 6.4(2), two labels were used for every unique VACL that was created and applied to a VLAN. There is support for up to 500 labels system wide that are shared between QoS ACLs, VACLs, and Cisco IOS ACLs. With software release 6.4(2) and later releases, only one label is used per VACL. (CSCdy45904)
- The ifindex field is zero for the corresponding source or destination IP address of the flow if the default route is the forwarding entry for the specific IP address. Using a more specific route results in the correct ifIndex numbers. This problem is resolved in software release 6.4(2). (CSCdz06899)
- The overflow counters in the HC-RMON-MIB may not show correct values. This problem is resolved in software release 6.4(2). (CSCdz70475)
- An SNMP set or get on cseNetflowLSGroup objects might cause memory leaks. This problem is resolved in software release 6.4(2). (CSCdz81270)
- In rare circumstances, when you statically configure a multicast router port on a trunk, some of the VLANs on that trunk might be cleared from the multicast router port list for that port even though they were statically configured. This problem is resolved in software release 6.4(2). (CSCdz89582)
- The switch may crash in the CmpOID function when a connected ATM module runs out of memory. This problem is resolved in software release 6.4(2). (CSCdz50307)
- With a WS-X6148 module, the runtime trust-dscp and trust-ipprec values are reversed in the output of the **show port qos** *mod/port* command for that module. This problem is resolved in software release 6.4(2). (CSCdz88155)
- The switch might crash when there is a high traffic load on the EOBC out-of-band management bus. This problem is resolved in software release 6.4(2). (CSCea16376)

Open and Resolved Caveats in Software Release 6.4(1)

These sections describe open and resolved caveats in supervisor engine software release 6.4(1):

- Open Caveats in Software Release 6.4(1), page 98
- Resolved Caveats in Software Release 6.4(1), page 98

Open Caveats in Software Release 6.4(1)

This section describes open caveats in supervisor engine software release 6.4(1):

- In rare circumstances, a dynamic CAM entry pointing to port 16/62 can be created when QoS is enabled and multicast data traffic is flowing in the system. This problem could result in connectivity loss when unicast packets are destined to the MAC address that is shown as part of the CAM entry. The workaround is to clear the CAM entry and disable QoS globally. This problem exists in all 6.x software releases. (CSCdz72304)
- 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 that are 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 that is 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 6.4(1)

This section describes resolved caveats in supervisor engine software release 6.4(1):

- After a high-availability switchover, the auxiliary VLAN ID and the port VLAN ID are not set for Multiple VLAN Access Ports (MVAPs). With high availability enabled in a redundant system, if some ports are MVAPs, after the high-availability switchover, the auxiliary VLAN ID and the port VLAN ID for those ports are not set. The workaround is to reconfigure the ports. This problem is resolved in software release 6.4(1). (CSCdy30915)
- In rare circumstances, the switch might experience a red status light on the supervisor engine due to an NVRAM checksum error. Under this condition, you will observe the following:
  - The **show version** command shows a checksum failure of some type.
  - The **show test 1** command show an NVRAM failure (NVRAM: F).

  This problem does not have any impact on switch operation as long as you do not make any configuration changes while the switch is in this condition. If the switch is reset while in this condition, some configuration data may be lost. Before the switch is reset, make sure that you have a current copy of your configuration stored on another device. The workaround for this problem is to reset the supervisor engine. This problem is resolved in software release 6.4(1). (CSCdz32620)
- When RGMP is enabled, the switch might reset when you enter the **set igmp disable** command. This problem occurs only when RGMP is enabled.

  Workaround: Disable RGMP before disabling IGMP snooping by issuing the following commands in order:
  - **set rgmp disable**
  - **set igmp disable**

  This problem is resolved in software release 6.4(1). (CSCdy14752, duplicate of CSCdy11713)

- In a redundant configuration, the following messages might display:

```
%SYS-2-MOD_NOINBANDRESPONSE:Module 2 not responding over inband
%SYS-2-MOD_INBANDOK:Module 2 inband ok
```

  These messages indicate that the active supervisor engine is polling the redundant supervisor engine but is unsuccessful in getting a timely response. This problem is resolved in software release 6.4(1). (CSCdx93107)

- The NAM application image release 1.1(1a) is not supported with software releases 6.3(2) and later due to an SCP incompatibility. The workaround is to upgrade the NAM application image to release 1.2(1). The NAM maintenance image also needs to be upgraded from release 1.1(1a)m to release 1.2(1)m. This problem is resolved in software release 6.4(1). (CSCdv81351)
- With high availability enabled, removing and then reinserting the standby supervisor engine might cause it to reset with a TLB exception. This problem is resolved in software release 6.4(1). (CSCdx38593)
- Entering the **set crypto rsa key 2048** command might cause high CPU utilization for a period of up to 18 minutes. There is no workaround other than generating the key at a non-peak traffic period or using a lower bit crypto key. This problem is resolved in software release 6.4(1). (CSCdx76688)
- You might experience a problem with disabling IEEE 802.1Q tunneling on a WS-X6248 or WS-X6348 module port. When you disable 802.1Q tunneling on the port, the port is now an access port but the port still accepts tagged traffic that is for VLANs other than its native VLAN. An access port should only accept untagged traffic or traffic tagged with the port's native VLAN. This problem is resolved in software release 6.4(1). (CSCdy11767)
- With IGMP snooping enabled, a switch running software release 6.3(7) on the supervisor engine and Cisco IOS Release 12.1(8b)E9 on the MSFC might not establish a PIM neighbor relationship with a directly connected router running PIM v1. The workaround is as follows:
  - 1) Use PIM v2 on the directly connected router.
  - 2) Disable IGMP snooping using the **set igmp disable** command.

  This problem is resolved in software release 6.4(1). (CSCdy17806)
- In a redundant configuration running single-router mode (SRM), if the switch is reset or if both MSFCs are reloaded at the same time, all the interfaces on the designated router stay in a down/down state. This problem happens only when both the MSFCs are booting off sup-slot0:. The workaround is to reload the designated router, so that the nondesignated router becomes the designated router, or manually do a shut/no shut on the interfaces on the designated router. This problem is resolved in software release 6.4(1). (CSCdy51093)
- "Group Specific" report statistics might not display using the **show igmp statistics** command. When IGMP packets with group address 01-00-5e-00-00-xx (where xx= 01, 02, 04, 05, 06, 0d) are sent, the group-specific reports field display is empty. Even though report packets are sent, the applicable fields are not incremented in the statistical display. This problem is not seen with other group addresses. This problem is resolved in software release 6.4(1). (CSCdy64989)
- After entering the **set msfcautostate enable** command, OSPF adjacencies for FlexWAN module interfaces are lost. The workaround is to do a shut/no shut on the FlexWAN module interfaces to bring traffic back up. This problem is resolved in software release 6.4(1). (CSCdy74216)
- Under rare conditions, a WS-X6348 module that is installed in a system with a Supervisor Engine 1A might stop forwarding packets due to a synchronization error between the module and the supervisor engine. This problem is resolved in software release 6.4(1). (CSCdz10526)
- After a supervisor engine switchover, the MSFC on the new standby supervisor engine may not come online. The workaround is to reload the MSFC. This problem is resolved in software release 6.4(1). (CSCdz16855)

- With a Supervisor Engine 2 running software release 6.3(9), if spanning tree is disabled and the switch is reset, the destination MAC address assigned for Ethernet pause frames on full-duplex links does not get added to the system CAM (01-80-c2-00-00-01). In networks in which spanning tree is disabled, pause frames sent from an attached workstation will be flooded to all the ports in the VLAN. Other workstations that are connected to the switch that support pause frames will see any pause frames sourced anywhere on the network and will stop transmitting. This problem is resolved in software release 6.4(1). (CSCdz22537)
- The switch might experience a TLB exception when upgrading to software releases 6.3(10), 7.4(2), and 7.4(3). The TLB exception will happen after entering the **show log** or **show tech** commands after upgrading. Some log buffer information related to inband ping failures will trigger this exception. The workaround is to clear the log before upgrading to these releases. Upgrades to software releases 6.4(x) and 7.5(x) are not affected. When upgrading or downgrading from/to software releases 6.3(10), 7.4(2), and 7.4(3), you must use the **clear log** command if you see "INBAND PING FAILURE" messages in the log. This problem is resolved in software release 6.4(1). (CSCdz32730)
- Under rare conditions, the Rx port buffers on a WS-X6548 module can lock up. This problem is resolved in software release 6.4(1). (CSCdz39293)
- With dual MSFC redundancy using Supervisor Engine 1 with the MSFC or MSFC2, you might not be able to boot from sup-slot0:. With Catalyst software release 6.3(6) or later and Cisco IOS Release 12.1(12c)E1 or later bootloader image, fixes were incorporated to allow booting from sup-slot0. There may be a delay in booting the second MSFC/MSFC2 until the first MSFC/MSFC2 finishes booting from sup-slot0:. With Catalyst software releases 6.4(1) and later and Cisco IOS Release 12.1E, the delay has been eliminated and the MSFCs boot from their local supervisor engine sup-slot0: (you must have the MSFC images in sup-slot0: of both supervisor engines). (CSCdy55525)
- Under certain circumstances, the switch might crash due to "fill_mbuf_ids_que" when running software release 6.3(8). This problem is resolved in software release 6.4(1). (CSCdy80039)
- A VACL might not be able to map to a VLAN when you enter the **set security acl map** <*name*> <*vlan*> command. The system responds with this error message:

  ```
  Failed to map VLAN 4 to ACL <name>.
  ```

  This problem is seen when the TCAM is full. The problem is resolved in software release 6.4(1) by displaying an error message that clearly indicates the reason for the failed ACL mapping. The workaround is to use the ODM ACL merge algorithm that released in software release 7.1 (this is an improvement on the BDD ACL merge algorithm). (CSCdz51934)
- You might see outdiscards incrementing on spanning tree blocked ports with the WS-X6408A-GBIC module. This problem does not degrade system performance. This problem is resolved in software release 6.4(1). (CSCdy08649)
- With protocol filtering enabled and IPX on, IP off, and group off, you might not be able to log on through IPX. The workaround is to disable protocol filtering on the switch. This problem is resolved in software release 6.4(1). (CSCdy71775)
- In a redundant configuration with high availability, dual-router mode, and core-dump enabled, if you have a Switch Fabric Module in truncated mode and the standby supervisor engine crashes while the core dump is being written to the standby supervisor engine Flash PC card, the active MSFC will experience EIGRP and HSRP flaps causing connectivity failures. The workaround is to disable core-dump on both supervisor engines. This problem is resolved in software release 6.4(1). (CSCdz71055)

- The WS-X6608-T1 modules may lose part of their configuration when the module is reseated or reset. Specifically, a board configured with a VLAN, IP address, TFTP server, and DNS with DHCP disabled, may lose the DNS entry for each port in its configuration. The workaround is to ensure that the system DNS entries are configured using the following commands:
  - **set ip dns server** *a.b.c.d* **primary**
  - **set ip dns server** *x.y.z.w*
  - **set ip dns enable**
  - **set ip dns domain** *mydomain.com*

  With the DNS entries configured, the voice ports inherit the DNS entries and come online. This problem is resolved in software release 6.4(1). (CSCdz19014)
- In a WS-C6513 chassis, you might be unable to session into MSFC 15 when the WS-X6101-OC12-MMF/SMF module in slot 11 has been reseated or reset through software. Sessioning to MSFC 16 (if present) is not affected. MSFC routing is not affected and the **switch console** 15 or 16 command is not affected. The problem only occurs with the WS-X6101-OC12-MMF/SMF module in slot 11. The workaround is to reset MSFC 15 or reboot the switch. This problem is resolved in software release 6.4(1). (CSCdz36766)
- On an EtherChannel, after a reset or disruption, the CBL on some links of the channel might be incorrectly set for VLANs that have spanning tree disabled. This situation causes connectivity problems. The workaround is to enable the channel and then bring up one port in the channel at a time. The time interval between bringing up the ports should be approximately 30 seconds. This problem is resolved in software release 6.4(1). (CSCdz55426)
- A switch running software release 6.3(10) may crash with the following error:

```
int status = 00000000, 00200000mistral interrupt status register contents: 00000000,
00200000
lo pg crc err happened. mistral interrupt_source_status register contents: 00000000,
20200802 timer 0 int happened.
inband int happened.
lo pg crc err happened.
programmable int 0 int happened.
mistral interrupt_status_10 register contents: 00000000, 00000000 fatal mistral
happened
```

  This error is not logged to the NVRAM log and can only be seen on the console just before the supervisor engine crashes. This problem is resolved in software release 6.4(1). (CSCdz65338)
- In a mixed-environment network with MAC address reduction enabled on some switches and disabled on other switches, you might experience a spanning tree loop because of the merging of different VLANs. After you merge two VLANs using a device such as LocalDirector, the switch with MAC address reduction enabled is the root switch and is the root switch for both the merged VLANs. A spanning tree loop might occur in one of the VLANs depending on the topology and the spanning tree parameters. This bug is present in software releases 5.5, 6.3, 7.1, 7.2, 7.3, 7.4, and 7.5. The workaround is to enable MAC address reduction on all the switches in the network if possible. This problem is resolved in software release 6.4(1). (CSCdz69457)
- In a redundant configuration with high availability and core dump enabled, and a PCMCIA Flash card in each supervisor engine, you might experience a Bus Error exception causing a reboot on the standby supervisor engine after writing the core dump to the PCMCIA Flash card. Once the standby supervisor engine comes back online, the standby MSFC might fail to respond to SCP polls from the supervisor engine and reset. The workaround is to disable core dump on both supervisor engines. This problem is resolved in software release 6.4(1). (CSCdz69145)

- You might only be allowed one log in attempt when using SSH and RADIUS as the authentication protocol. Changing the log in attempts variable using the **set authentication login attempt** *count* **telnet** command does not change the number of log in attempts in this situation. This problem is resolved in software release 6.4(1). (CSCdy78497)

Open and Resolved Caveats in Software Release 6.3(10)

These sections describe open and resolved caveats in supervisor engine software release 6.3(10):

- Open Caveats in Software Release 6.3(10), page 102
- Resolved Caveats in Software Release 6.3(10), page 102

Open Caveats in Software Release 6.3(10)

This section describes open caveats in supervisor engine software release 6.3(10):

- When RGMP is enabled, the switch might reset when you enter the **set igmp disable** command. This problem occurs only when RGMP is enabled.

  Workaround: Disable RGMP before disabling IGMP snooping by issuing the following commands in order:

  - **set rgmp disable**
  - **set igmp disable**

  (CSCdy14752)

- 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 6.3(10)

This section describes resolved caveats in supervisor engine software release 6.3(10):

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. This problem is resolved in software release 6.3(10). (CSCdu43064)
- When you log into the switch using either TACACS or RADIUS authentication and use RCP for remote file copying, the TACACS or RADIUS user login name is used instead of the RCP username (which is set using the **set rcp username** *username* command). The workaround is to configure the TACACS or RADIUS username on the server from which you are using RCP to copy files. This problem is resolved in software release 6.3(10). (CSCdy05707)

- The switch might not prompt for local login authentication after RADIUS servers have not been able to respond to an authentication request. After the RADIUS servers (primary as well as secondary) fail to respond, the switch should try the local login authentication or some other (such as TACACS) per the configuration. This problem is resolved in software release 6.3(10). (CSCdy19729)
- The switch might accept a BPDU with the contents zeroed out and process it as BID 0000.0000.0000, priority 0, and msg age expiry 0. Processing the BPDU causes switch instability. The switch should discard BPDUs if any parameters are out of range. This problem is resolved in software release 6.3(10). (CSCdy46624)
- Troubleshooting inband issues is somewhat difficult due to a lack of information. To facilitate the debugging of inband failures, additional data regarding CPU usage, backplane traffic, and inband receive and transmit rates have been added to the NVRAM logs and syslogs. This problem is resolved in software release 6.3(10). (CSCdy62612)
- Using the SNMP portCopyEntry MIB to update an active span's attribute (such as direction) might cause memory corruption. There are no problems using the same MIB to create/delete or change row status to active or not in service. The workaround is to change an active span's parameters from SNMP as follows:

  1. Set the row status to "not-in-service."
  2. Change the entry's parameter.
  3. Activate the row status.

  This problem is resolved in software release 6.3(10). (CSCdy64837)
- With the release 6.3.8, 6.3.9, and 7.3.1 software images, the software might erroneously reset the out-of-band management channel causing subsequent FIB updates to be improperly installed in the hardware. This problem affects Layer 3 forwarding. This problem is resolved in software release 6.3(10). (CSCdy75968)
- In rare conditions, PVST+ systems may advertise an incorrect bridge priority. This problem is resolved in software release 6.3(10). (CSCdy88023)
- When using the **set spantree root** command with a network diameter of 2 and a hello time of 1, the resulting calculation for "max age" is changed to 5 which is unacceptable to other switches. The workaround is to set the max age to a minimum value of 6 (use the **set spantree maxage** *agingtime* command). This problem is resolved in software release 6.3(10). (CSCdy85719)
- When a supervisor engine switches over to the standby supervisor engine due to heavy traffic on the supervisor engine management port, the switch displays messages similar to the following:

  ```
  %SYS-2-MOD_NOINBANDRESPONSE:Module 2 not responding over inband, rx=2 pps, tx=2 pps,
  CPU:78.12%, backplane: 42%
  %SYS-2-MOD_INBANDTEST:Module 1 error detected ... testing
  %SYS-0-MOD_INBANDFAILURE:Module 1 local inband failure... resetting module
  %SYS-5-MOD_RESET:Module 1 reset from Software
  ```

  On Supervisor Engine 1A, the rx and tx values are not reported correctly as they are lower than expected. On Supervisor Engine 2, the rx and tx values are reported correctly. This problem is resolved in software release 6.3(10). (CSCdz12126)
- When a supervisor engine switches over to the standby supervisor engine due to an inband test failure, the rx/tx, CPU, and backplane values are not always being logged. This problem might be seen on both Supervisor Engine 1A and on Supervisor Engine 2. This problem is resolved in software release 6.3(10). (CSCdz12283)
- If larger than normal spanning-tree protocol (STP) packets are received on a dot1q trunk, the switch might experience memory corruption. The memory corruption could lead to a system reset. This problem is resolved in software release 6.3(10). (CSCdz02959)

- The **set igmp ratelimit** command is not stored in NVRAM. This issue will be addressed in a future release. Currently, you have to use text config mode to preserve igmp rate limit settings across reboots. With software release 6.3(10), when you set the rate-limit values when the config is in binary mode, you are warned with the following message:

  ```
  Warning:The rate-limit settings are preserved after reboot only in config mode text.
  ```

  (CSCdy05729)

- Prior to software release 6.3(10), an IGMP version 3 packet with more than one group in the same packet was discarded. This has been fixed in software release 6.3(10). Software releases 6.3(x) run IGMP version 2 and there is no support for version 3. An IGMP version 3 report is treated as a set of IGMP version 2 reports for each of the multicast groups forming the group records in IGMP version 3 reports regardless of the filter mode of the IGMP version 3 report. (CSCdw61628)

Open and Resolved Caveats in Software Release 6.3(9)

These sections describe open and resolved caveats in supervisor engine software release 6.3(9):

- Open Caveats in Software Release 6.3(9), page 104
- Resolved Caveats in Software Release 6.3(9), page 105

Open Caveats in Software Release 6.3(9)

This section describes open caveats in supervisor engine software release 6.3(9):

- When RGMP is enabled, the switch might reset when you enter the **set igmp disable** command. This problem occurs only when RGMP is enabled.

  Workaround: Disable RGMP before disabling IGMP snooping by issuing the following commands in order:

  - **set rgmp disable**
  - **set igmp disable**

  (CSCdy14752)

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP “link down” on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)

- 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 6.3(9)

This section describes resolved caveats in supervisor engine software release 6.3(9):

- Parity errors might cause the supervisor engine to reset. This problem is resolved in software release 6.3(9). (CSCdx86436)
- With a WS-X6K-SUP1A-2GE supervisor engine, the switch might not send an NVRAM failure trap. This problem is resolved in software release 6.3(9). (CSCdy18916)
- A switch running software release 6.3(7) might hang when you enter the **ping** command (from enable mode) through a Telnet session and then terminate the Telnet session. When this occurs, the supervisor engine stops processing all protocols but continues to switch traffic that could create a spanning tree loop. You should use aggressive UDLD and loop guard to prevent a spanning tree loop. This problem is resolved in software release 6.3(9). (CSCdy00355)
- An SNMP MIBwalk over CISCO-PAGP-MIB might cause the switch to reset. This problem was observed after an LACP channel was configured with the distribution set as "**set port channel all distribution session both**." If the channel distribution is set to its default, the reset does not occur. This problem is resolved in software release 6.3(9). (CSCdy20189)
- When you use Secure Shell (SSH) encryption with a RADIUS server for authentication, and that server is configured to allow you to go directly to the enable mode, you might only be able to get to the user mode. To get to the enable mode, you might have to authenticate one more time by providing the enable password again (you must configure the $enab15$ username). With Telnet sessions, you can go directly to the enable mode. This problem is resolved in software release 6.3(9). (CSCdy26331)
- A switch with redundant supervisor engines might display the following error messages and stop functioning correctly:

  ```
  SYS-3-SUP_ASENDFAIL:gentcp_act unable to send data to standby
  SYS-3-SUP_ACONNFAIL:gentcp_act unable to connect with standby
  ```

  This problem might occur when a command that requires remote execution (such as dir 2/, squeeze 2/slot0) is entered on the switch. When you enter these type of commands, a message is sent to the standby supervisor engine. If the time that is taken to execute this command is significant, then during this time you could enter the commands on the active supervisor engine that require remote execution. Entering a second remote-execution command before the first one finishes can break the remote execution connection between the supervisor engines. With software releases 6.3(9) and later, entering a second command causes the following error to be displayed:

  ```
  File system in use (3). Try again later.
  ```

  The workaround is to not enter a second remote-execution command before the previous command finishes. This problem is resolved in software release 6.3(9). (CSCdv20161)
- If a WS-X6516 module has a faulty GBIC, SCP communication to the WS-X6516 module might fail. This problem might lead to spanning tree loops. This problem is resolved in software release 6.3(9). (CSCdy09795)
- In some circumstances, the switch might experience a TLB exception if you disable IGMP snooping while RGMP packets are being received by the switch. The workaround is to disable RGMP before disabling IGMP snooping. This problem is resolved in software release 6.3(9). (CSCdx60209)
- When a VLAN mapping change occurs in the root switch, some of the nonroot switches might not get updated with the new mapping. This problem is a cornercase found in software release 7.3(2). The workaround is to modify the VLAN mapping on the root switch or disable and then reenable the root port on the nonroot switch. This problem is resolved in software release 6.3(9). (CSCdy16164)

- When an inband ping fails, the diagnostics might fail and cause a switchover to the redundant supervisor engine. This problem is resolved in software release 6.3(9). (CSCdx10436)
- On a network of Catalyst 6000 family switches, when backbone fast is enabled, there is a risk of creating a loop of RLQ BPDUs (backbone fast BPDUs) if (and only if) there is a device in the network that is transparently bridging BPDUs between at least three VLANs (such as a LocalDirector attached in three VLANs or a hub). This problem can cause high CPU utilization in the StpBPDUrx process on the problem switch. This problem is resolved in software release 6.3(9). (CSCdy53023)
- In extremely rare conditions, a switch with a PFC (not PFC2) running Multicast Multilayer Switching (MMLS) may stop forwarding traffic for a (S,G) flow. This occurs because the entry, although installed in the NetFlow, may not be marked in the correct state (used state). This problem is resolved in software release 6.3(9). (CSCdw93241)
- Multicast traffic coming from a WAN interface might not be switched. The workaround is to disable multicast MLS. This problem is resolved in software release 6.3(9). (CSCdv65393)
- Packets smaller than 64 bytes that are transmitted by the supervisor engine might be improperly padded with an excess 4 bytes due to improper length settings. The excess 4 bytes was incorrectly added for CRC. This problem is resolved in software release 6.3(9). (CSCdy43680)

Open and Resolved Caveats in Software Release 6.3(8)

These sections describe open and resolved caveats in supervisor engine software release 6.3(8):

- Open Caveats in Software Release 6.3(8), page 106
- Resolved Caveats in Software Release 6.3(8), page 107

Open Caveats in Software Release 6.3(8)

This section describes open caveats in supervisor engine software release 6.3(8):

- When RGMP is enabled, the switch might reset when you enter the **set igmp disable** command. This problem occurs only when RGMP is enabled.

  Workaround: Disable RGMP before disabling IGMP snooping by issuing the following commands in order:

  - **set rgmp disable**
  - **set igmp disable**

  (CSCdy14752)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP “link down” on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)

- 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 6.3(8)

This section describes resolved caveats in supervisor engine software release 6.3(8):

- When the backup supervisor engine takes over in a system configured for Supervisor Engine 2 redundancy, the trunking information tables are not built correctly on the Gigabit Ethernet port. This problem is also evidenced by the absence of the "TrunkFramesTx" counter in the output of the **show trunk detail** command. The problem occurs when a switchover takes place from the active to the redundant supervisor engine and ports 1/1 and 2/1 on the supervisor engines have been configured for channeling. A port on the formerly active supervisor engine is not participating in the channel even though it is in trunking mode.

  Workaround: The only way to recover from this problem and rebuild the trunking table is by entering the **shutdown** command followed by the **no shutdown** command on the affected port. This problem is resolved in software release 6.3(8). (CSCdy12940)
- Reserved address 01-00-5e-00-00-xx traffic is flooded throughout the VLAN with IGMP snooping enabled even when you enter the **set cam permanent** command. This problem is resolved in software release 6.3(8). (CSCdx86394)
- A Catalyst 6000 family switch with dual MSFCs running Cisco IOS 12.1(8a)E3 and PIM might show higher than normal CPU utilization on the NDR MSFC. An increase in input drops might also occur on the VLAN interface connected downstream of the multicast traffic. This problem is resolved in software release 6.3(8). (CSCdx78283)
- When you enter the **show port** and **show counters** commands using the CLI, FCS errors are generated, but when the SNMP object dot3StatFCSError is polled, no errors are indicated. This problem is resolved in software release 6.3(8). (CSCdx88030)
- A Cisco 7940 IP phone connected to a Catalyst 6509 switch initially receives an IP address from the data VLAN rather than the auxiliary VLAN configured on the port. This problem is resolved in software release 6.3(8). (CSCdx66655)
- Cisco 7960 IP phones do not appear as connected to the switch when you enter the **show cdp neighbor** command, even though the phones are sending CDP packets and the switch is receiving them. This problem is resolved in software release 6.3(8). (CSCdy02051)
- If you set the screen length to 0 using the **set length** command and then enter the **show snmp oid** command, a system reset occurs. This problem is resolved in software release 6.3(8). (CSCdx94474)
- With high availability enabled, the active supervisor engine might intermittently reset, bringing up the standby supervisor engine. The active supervisor engine might reset when there is no identifiable fault condition. This problem is resolved in software release 6.3(8). (CSCdx25470)

- On a Supervisor Engine 2 in a Catalyst 6500 series switch, the following messages can be seen in the log after that supervisor engine resets:

```
09. 6/12/2002,15:11:22: send_scp:MCP/EOBC not responding
10. 6/12/2002,15:12:27: ProcessStatusPing:Module 1 local SCP error
detected... resetting module
11. 6/12/2002,15:12:27: ProcessStatusPing:Module 1 SLCP not responding...
resetting module
```

  This problem is resolved in software release 6.3(8). (CSCdx88297)

- The Catalyst 6000 family switch might experience a slow memory leak during the multicast receive (McastRx) process. This problem might happen if you configure RSPAN and IGMP snooping entries are created in the RSPAN VLAN. The workaround is to disable RSPAN. This is a corner case related to a more generic problem. The memory leak can occur whenever source-only IGMP snooping entries are created in a VLAN without any router port. You can detect this problem by entering the **show multicast group** command and looking for an entry without an output port. This problem is resolved in software release 6.3(8). (CSCdv11016)
- In very rare circumstances, IGMP packets destined to address 224.0.0 [1,4,5,6,d] can reach the supervisor engine at an excessive rate causing high CPU utilization. Depending on the network topology and the network condition, this problem may cause other processes to become unstable. This problem is resolved in software release 6.3(8). (CSCdx09717)
- The VMPS process on the switch might fail for particular MAC addresses. This problem is resolved in software release 6.3(8). (CSCdx45232)
- You might experience a memory leak in the ciscoFlashCopyTable object when you do a “set” operation. This problem is resolved in software release 6.3(8). (CSCdx55656)
- You might experience a memory leak when hot swapping a module. This problem is resolved in software release 6.3(8). (CSCdx58476)
- You might experience a memory leak when you enable RMON and reset a module. This problem is resolved in software release 6.3(8). (CSCdx61519)
- An SNMP MIBwalk with a community string in the format <community string>@<vlan> returns an incorrect value. This problem is resolved in software release 6.3(8). (CSCdx66883)
- When using RADIUS authentication, you might not be able to reach enable mode. If you put Attribute 18 (reply message) before the service-type=6 attribute, the system fails to put you in enable mode. The following server configuration can cause the problem:
  - Username = swi
  - Reply message = PASSCODe Accepted
  - Service-Type = Administrative

  If you put the Service-Type before the Reply message, then the configuration works. The root cause is that while the supervisor engine software is processing the Reply message attribute, it corrupts the attribute following it. This problem is resolved in software release 6.3(8). (CSCdx70904)
- You might see MMLS partial shortcuts although a Layer 3 entry exists for the source in question. This problem can occur with a Supervisor Engine 1 running MMLS. The shortcut may remain partial although the router tries to install an MFD, due to a wrong entry being matched when searching NetFlow. This problem is resolved in software release 6.3(8). (CSCdx69414)

- With a Supervisor Engine 1A/2 running software release 6.3(3), you might experience a memory leak/depleted memory that results in the switch crashing. The problem causes the following messages to display:

```
2002 Mar 01 14:25:28 %SYS-3-SYS_MEMLOW:Malloc usage exceeded 90%
2002 Mar 01 14:25:28 %SYS-3-SYS_MEMLOW:Malloc usage exceeded 90%
2002 Mar 01 14:25:28 %SYS-3-SYS_MEMLOW:Malloc usage exceeded 90%
2002 Mar 01 14:25:28 %SYS-3-SYS_MEMLOW:Malloc usage exceeded 90%
```

  This problem is resolved in software release 6.3(8). (CSCdx19098)

Open and Resolved Caveats in Software Release 6.3(7)

These sections describe open and resolved caveats in supervisor engine software release 6.3(7):

- Open Caveats in Software Release 6.3(7), page 109
- Resolved Caveats in Software Release 6.3(7), page 109

Open Caveats in Software Release 6.3(7)

This section describes open caveats in supervisor engine software release 6.3(7):

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- 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 6.3(7)

This section describes resolved caveats in supervisor engine software release 6.3(7):

- After a switch is rebooted with protocol filtering disabled and an OSPF neighbor is brought up on a FlexWAN module, the OSPF neighbor is lost after protocol filtering is enabled. This problem does not occur on Ethernet interfaces.

  Workaround: Perform a shut/no shut on the interface.

  This problem is resolved in software release 6.3(7). (CSCdx46569)
- After a supervisor switchover, the MSFC on the new standby supervisor may not come online.

  Workaround: Reload the MSFC. This situation happens only if the Cisco IOS Release 12.1(11b)E image is loaded on the MSFC and is independent of the Catalyst software version used.

  This problem is resolved in software release 6.3(7). (CSCdw79129)

- The Catalyst 6500 series switch sends all commands entered to the TACACS server instead of only the configuration commands. This problem is resolved in software release 6.3(7). (CSCdx48518)
- In a system with redundant supervisor engines and redundant MSFC2s, if you perform a manual switchover, you will disable high availability on the active supervisor engine, and the system will go into an inconsistency state. This problem is resolved in software release 6.3(7). (CSCdv18261)
- The output of the **show process memory** command displays incorrect values for Memory Allocated, Memory Freed, and Memory Holding. This problem is resolved in software release 6.3(7). (CSCdv85014)
- In a redundant system with a Switch Fabric Module, the redundant supervisor engine fails to bring the Switch Fabric Module online, causing a synchronization error for the switch fabric channel on the redundant supervisor engine. This problem is resolved in software release 6.3(7). (CSCdw05049)
- In a system containing mixed power supplies, the active power management LED for the supervisor engine does not change from orange to green when one power supply is removed. This problem is resolved in software release 6.3(7). (CSCdw53593)
- When an NMI bus timeout occurs, messages are displayed that indicate whether the cause is due to a backplane timeout or a supervisor engine timeout. These messages do not show up in the **show log** command output. This problem is resolved in software release 6.3(7). (CSCdw57262)
- Multicast packet drops in the Non-DR switch may occur during a DR failover if static or permanent multicast CAM entries are used.

  Workaround: Perform the following actions to force the multicast Layer 2 static CAM entries to be created before IGMP snooping creates source-only entries:

  - Stop the multicast traffic.
  - Clear all the CAM permanent entries.
  - Create the CAM entries again (including the internal router ports).
  - Start the multicast traffic.

  This problem is resolved in software release 6.3(7). (CSCdw57540)
- If you execute the **show acl** *acl* **inracl** command, the MMLS process in the route processor stops, causing every flow to be software switched.

  Workaround: Do not execute the **show acl** *acl* **inracl** command.

  This problem is resolved in software release 6.3(7). (CSCdw64398)
- Unicast RPF enhancements fail when configured on an MSFC doing MLS CEF switching. This problem is resolved in software release 6.3(7). (CSCdw84636)
- Transferring a configuration file using the **tftpGrp** command to a Catalyst 6000 family switch with TACACS enabled causes the transfer to fail with no error messages. This problem is resolved in software release 6.3(7). (CSCdw85913)
- A system reset occurs at bootup during global synchronization. This problem is resolved in software release 6.3(7). (CSCdw86070)
- A command is needed to adjust the debounce timer for Gigabit Ethernet fiber ports. This problem is resolved in software release 6.3(7) by the **set port debounce timer** {*mod/port*} *value* command where *value* equals a range from 100 ms (default) to 10000 ms. (CSCdw91987)
- Aggregate entries for Gigabit Ethernet and Fast Ethernet channels may be missing in the ifTable and ifXTable for Catalyst 6000 family switches. This problem is resolved in software release 6.3(7). (CSCdx00296)

- If you configure IP PIM dense mode on label-shared interfaces, different behavior is seen between the ODM algorithm and the BDD algorithm. If IP PIM dense mode is configured on one of the label-shared interfaces, the labels should not be shared. This behavior does not occur when ODM is the merge algorithm. This problem is resolved in software release 6.3(7). (CSCdx08772)
- The console or the Telnet session locks up and outputs incorrect information after you enter the **show proc cpu** *mod* (where *mod* is any module except the supervisor engine) command on a Catalyst 6000 family switch. This problem is resolved in software release 6.3(7). (CSCdx12377)
- In Supervisor Engine 2 systems, traffic may show up on a capture port if the ACL lookup result is Layer 3 deny and traffic is on the same VLAN as the capture port. This problem is resolved in software release 6.3(7). (CSCdx13690)
- If a GBIC is unplugged, sometimes the link stays up. This problem is resolved in software release 6.3(7). (CSCdx14435)
- MMLS does not function after a high-availability switchover. This problem is resolved in software release 6.3(7). (CSCdx1480)
- In certain topologies, a Catalyst 6500 series switch running IGMP snooping may experience a Layer 2 loop of PIM reachability.

  Workaround: Disable IGMP snooping by entering the **set igmp disable** command.

  This problem is resolved in software release 6.3(7). (CSCdx17913)
- Entering the **clear config all** command causes inband failures and resets the supervisor engine.This problem is resolved in software release 6.3(7). (CSCdx22157)
- The Catalyst 6500 series switch with a Supervisor Engine 2 does not print log messages or any other information in the **show log** output. This problem is resolved in software release 6.3(7). (CSCdx26043)
- The SrCreateV3SnmpMessage operation may fail if syslog messages are sent to a Network Management System server at the same time. This problem is resolved in software release 6.3(7). (CSCdx37286)
- If two Catalyst 6500 series switches are connected by an EtherChannel over two different modules and one module fails, some of the traffic originally on a link in the failed module, may not successfully fail over to a link in the other module. This problem is resolved in software release 6.3(7). (CSCdx37869)
- If a software reset occurs on a Catalyst 6000 family switch with a PFC or PFC2 with at least one security or QoS ACL configured, the supervisor engine enters the debugger mode instead of rebooting. This problem is resolved in software release 6.3(7). (CSCdx37897)
- The MTU of a jumbo frame-enabled port does not change to 9216. Instead, the MTU remains at the default value of 1500. This problem is resolved in software release 6.3(7). (CSCdx41639)
- The SNMP output after a MIBwalk shows that bridge information does not exist for ports in any VLAN other than VLAN 1. This problem is resolved in software release 6.3(7). (CSCdx46174)
- The Catalyst 6000 family switch fails to communicate with the Network Management System through SNMP when you use an SNMP community string containing the backslash character. This problem is resolved in software release 6.3(7). (CSCdx46965)
- A reload occurs when you attempt to NVGEN the **mls qos trust extend** command configuration on OSM WAN interfaces. This problem is resolved in software release 6.3(7). (CSCdx50977)

- When making a Telnet connection to a switch configured with authentication, authorization, and accounting (AAA) through Shiva Access Manager, the switch sets the TACACS privilege level to 15. Authentication fails if users have a privilege level lower than 15.

  Workaround: Configure Shiva Access Manager users with privilege level 15.

  This problem is resolved in software release 6.3(7). (CSCdx08395)
- If you terminate a **ping** or a DNS lookup by pressing **Ctrl-C**, the process is terminated but the memory allocated to the process is not properly freed. This problem is resolved in software release 6.3(7). (CSCdx40797, CSCdx40481)
- When the FIB table is under exception, in rare cases the system may reload. This problem is resolved in software release 6.3(7). (CSCdv64828).
- A reload occurs when you enter the **ping** command. This problem is resolved in software release 6.3(7). (CSCdx48959)
- When opening a large number of SSH sessions, it may run out of memory, and cause the switch to reload.

  Workaround: Limit the total number of SSH sessions allowed open at the same time to 10.

  This problem is resolved in software release 6.3(7). (CSCdw71589)
- With SNMP, the switch returns "RESOURCE_UNAVAILABLE_ERROR" when modifying the vlanTrunkPortTable. This problem exists only in software release 6.3(6). This problem is resolved in software release 6.3(7). (CSCdx23585)

Open and Resolved Caveats in Software Release 6.3(6)

These sections describe open and resolved caveats in supervisor engine software release 6.3(6):

- Open Caveats in Software Release 6.3(6), page 112
- Resolved Caveats in Software Release 6.3(6), page 113

Open Caveats in Software Release 6.3(6)

This section describes open caveats in supervisor engine software release 6.3(6):

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 SNMP, the switch returns "RESOURCE_UNAVAILABLE_ERROR" when modifying the vlanTrunkPortTable. This problem exists only in software release 6.3(6). (CSCdx23585)

Resolved Caveats in Software Release 6.3(6)

This section describes resolved caveats in supervisor engine software release 6.3(6):

- In a system with a Supervisor Engine 2 and an MSFC2, packets forwarded over a GRE tunnel are dropped or forwarded over a non-GRE interface. This problem is resolved in software release 6.3(6). (CSCdx06944)
- In a system running software release 5.5(11), runts may increment on Gigabit Ethernet ports that are in a not-connected state if those ports are configured with the **set port negotiation** *mod/port* **disable** command. This problem is resolved in software release 6.3(6). (CSCdw52996)
- Polling the vlanTrunkPortTable MIB object from the CISCO-VTP-MIB causes high CPU utilization. This problem is resolved in software release 6.3(6). (CSCdx07214)
- If a RACL fails to get mapped to an interface in a system with either a Supervisor Engine 1 or 2 and high availability configured, an incorrect TCAM look up might result after one of the MSFCs reloads. This problem is resolved in software release 6.3(6). (CSCdx14864)
- Protocol Information is not reported in NDE if full VLAN flow mask is specified. This problem is resolved in software release 6.3(6). (CSCdx01951)
- In rare circumstances, a designated port might be stuck in the spanning tree "listening" state and still be transmitting BPDUs. This does not introduce problems with spanning tree convergence or cause loops. This problem is resolved in software release 6.3(6). (CSCdv89566)
- During bootup in a redundant configuration, the active supervisor engine reboots twice if the diagnostic mode is set to bypass. The workaround is to set the diagnostic mode to minimal or complete. This problem is resolved in software release 6.3(6). (CSCdw36342—duplicate of CSCdw32758, CSCdu33276)
- In rare circumstances, an MT-RJ Gigabit Ethernet port with autonegotiation enabled might not be able to achieve link up after being disabled and then enabled. This problem is resolved in software release 6.3(6). (CSCdw50266)
- In rare circumstances, a Gigabit Ethernet GBIC port cannot achieve link up through autonegotiation. This problem is resolved in software release 6.3(6). (CSCdw52651)
- The vlanPortIslOperStatus MIB returns incorrect trunking status. This problem is resolved in software release 6.3(6). (CSCdw24363)
- The switch might reload if VTP is configured in client or server mode and connected to a Catalyst 4000 family switch with a Supervisor Engine III. The workaround is to configure VTP in transparent mode. This problem is resolved in software release 6.3(6). (CSCdw41158)

- When you try to delete snmpVacmAccessEntry, the system might respond with an "Entry not found" message. This problem is resolved in software release 6.3(6). (CSCdw36075)
- On Supervisor Engine 2, source and destination indices might be reported as 0 in the NetFlow Data Export (NDE) record. To fix the problem, the source and destination ifindices and nexthop information is now filled in by looking up the FIB table. Note that this may not always yield accurate results, especially in times of route changes. This problem is resolved in software release 6.3(6). (CSCdt21216)
- When the 8-port T1/E1 PSTN interface module has an active voice call, the **show port voice active** command might not display any output. This problem is resolved in software release 6.3(6). (CSCdu67459)
- ARP entries for default gateways might not age out. This problem is resolved in software release 6.3(6). (CSCdv14247)
- The switch might reset with a TLB exception after entering the **set tacacs server host** command. This problem is resolved in software release 6.3(6). (CSCdv37751)
- A supervisor engine configured as an NTP client might lose synchronization with the NTP server although NTP updates are being received. This problem is resolved in software release 6.3(6). (CSCdv39229)
- In a redundant system, ToS bytes might not be marked for multicast packets; unicast packets are marked correctly. The workaround is to set the default action for IP to **trust-dscp** as follows: **set qos acl default-action ip trust-dscp**. This problem is resolved in software release 6.3(6). (CSCdv67672)
- If you have switches running Cisco IOS software on the supervisor engine and the MSFC and switches running Catalyst software on the supervisor engine with Cisco IOS software on the MSFC, and these switches are in the same VTP domain, some older releases of Cisco IOS software will send out VTP updates containing the Token Ring translated VLAN configuration (default configuration), which is not properly handled by Catalyst software prior to release 6.3(3). With Catalyst software release 6.3(3), a temporary mechanism was introduced to protect the local VLAN database by changing the VTP mode to transparent. With Catalyst software release 6.3(6), this problem is resolved and the Catalyst software works properly with the Cisco IOS software. (CSCdv77448)
- With a 2-port LACP channel misconfiguration (one side set to on, the other side set to off), the Spanning Tree Protocol might not detect a loop and fail to put the ports into errdisable state. This problem is resolved in software release 6.3(6). (CSCdv83868)
- When WS-X6248 or WS-X6348 modules are running at a fixed 10 Mbps, the link might not come up after the partner port is disabled and then enabled. The workaround is to disconnect and then reconnect the cable. This problem is resolved in software release 6.3(6). (CSCdv87677)
- If you press **Ctrl-C** from an SSH window while performing a TFTP download, the switch might reset with a TLB exception. This problem is resolved in software release 6.3(6). (CSCdw04909)
- When an interface IP address is updated or removed using the **ip address** *A.B.C.D* or **no ip address** commands, the received FIB entry for the old IP address is not removed. This situation results in stale FIB entries on the supervisor engine. This problem is resolved in software release 6.3(6). (CSCdw12196)

- Connectivity from community ports to some promiscuous ports may break when you are mapping several isolated VLAN ports at once (such as **set pvlan 769 120 7/25-36**). The workaround is to enter port ranges as follows:

  set pvlan 769 120 7/25

  set pvlan 769 120 7/26-35

  set pvlan 769 120 7/36

  This problem is resolved in software release 6.3(6). (CSCdw22333)

- In a redundant system with Secure Shell (SSH) encryption, you might get disconnected from the switch when entering the **dir** or **show flash** commands on the standby supervisor engine bootflash or slot0 Flash memory. This problem is resolved in software release 6.3(6). (CSCdw29826)
- When running Multicast Multilayer Switching (MMLS) on a Supervisor Engine 1, on reloading the MSFC, the "mroute entry" may not be created when the RPF interface is Packet over SONET. This problem is resolved in software release 6.3(6). (CSCdw30626)
- In a system with a switch fabric module installed, a fabric-enabled module may not come online after you power it down and up or perform an OIR. This problem occurs only if the switching mode reverts to bus-mode. The workaround is to reset the system. This problem is resolved in software release 6.3(6). (CSCdw30824)
- Supervisor engine software release 6.3(2) introduced the **set mls agingtime long-duration** command. On Supervisor Engine 2, you cannot verify the long-duration value. You can see the value on Supervisor Engine 1 using the **show mls** command. With software release 6.3(6), the **show mls** command now displays the long-duration value on Supervisor Engine 2.

  Caveat CSCdw28551 fixes one other problem that affects Supervisor Engine 1 and Supervisor Engine 2: If you set the configuration mode to "text" (either NVRAM or Flash), even if the long-duration aging timer value had been set, it does not show up in either the running or startup configurations and is not retained after a reset. This problem does not affect binary mode configuration. With software release 6.3(6), the granularity for the **set mls agingtime long-duration** command has been reduced to 8 seconds. (CSCdw28551)
- If you start a Telnet session to the switch and you get the login prompt but do not log in, you still might be able to view the logging on the switch if session logging is enabled which is the default. The workaround is to disable Telnet logging or use an IP permit list to restrict access. This problem is resolved in software release 6.3(6). (CSCdw39634)
- The system might reload while sending out syslog messages to Telnet and SSH sessions. The workaround is to enter the **set logging telnet disable** command. This problem is resolved in software release 6.3(6). (CSCdw54106)
- Setting a MIB object with the wrong value might result in a 48-byte loss of memory. This problem is resolved in software release 6.3(6). (CSCdw54653)
- The exported NDE records might contain a zero value in the dstIndex field. This problem is resolved in software release 6.3(6). (CSCdw57664)
- When MLS IP directed broadcast is configured in the exclude-router mode, directed broadcast packets are sent to the MSFC. This problem is resolved in software release 6.3(6). (CSCdw52256)
- With a Supervisor Engine 1 and ATM and/or WAN modules, the switch might reload when you enter the **show mls entry ip protocol udp** command. This problem is resolved in software release 6.3(6). (CSCdw42749)
- After a high availability switchover, the "port sync-restart-delay" configuration might be lost. This problem is resolved in software release 6.3(6). (CSCdw55240)

- When setting the MIB object caqIpAceProtocolType in the CISCO-CATOS-ACL-QOS-MIB to zero (0) to create a QoS ACL matching all IP traffic, the created ACL only matches IP traffic carrying "0" in the protocol field of the IP header. This problem is resolved in software release 6.3(6). (CSCdw59270)
- A switch running IGMP snooping may stop adding multicast router ports to the outgoing interface list of all multicast groups. The workaround is to disable and then reenable IGMP snooping on the switch. This problem is resolved in software release 6.3(6). (CSCdw59483)
- When you set the IGMP mode to "igmp-cgmp" and reset the switch, the switch might come up in the "igmp-only" mode when it should be in the "igmp-cgmp" mode. This problem is resolved in software release 6.3(6). (CSCdw60417)
- In rare circumstances, in systems with redundant supervisor engines and high availability enabled, when a POS Optical Services Module interface is going from down to up, the standby supervisor engine might reload. This problem is not seen with other interface types. This problem is resolved in software release 6.3(6). (CSCdw64846)
- Ia 13-slot chassis with the diagnostics set to "minimal" mode and a WAN module installed, after a non-high availability switchover, a minor hardware error might be reported on the standby supervisor engine. This problem is resolved in software release 6.3(6). (CSCdw65064)
- After a high-availability switchover, NetFlow version 7 might not export flows. This problem is resolved in software release 6.3(6). (CSCdw80772)
- On switches with Catalyst software installed on the Supervisor Engine 2 and Cisco IOS installed on the MSFC2, the supervisor engine will accept 512-MB DRAM, but will work only up to 256 MB. This gives you the opportunity to upgrade your DRAM to 512 MB in the event you change your operating system to Cisco IOS on both the Supervisor Engine 2 and the MSFC2. However, with 512-MB DRAM installed on a Supervisor Engine 2 running Catalyst software on the supervisor engine and Cisco IOS on the MSFC, boot messages and the **show version** command only show 256 MB. This problem is resolved in software release 6.3(6). (CSCdw84513)
- PortFast might not work on access ports. After you enter the **set spantree portfast** *mod_num/port_num* **enable trunk** command on an access port, the **show port spantree** command indicates that PortFast is enabled but the port is still listening and learning STP states. This problem is resolved in software release 6.3(6). (CSCdw85694)
- On a switch with high availability enabled, a switchover might cause UDLD in a neighbor switch to put its connecting link port (that was connected to the active supervisor engine undergoing the switchover) into errdisable state. This occurs when the banner (**set banner motd** *text*) is really long on the switch experiencing the switchover. This problem is resolved in software release 6.3(6). (CSCdw71357)
- On a switch configured with MISTP-PVST+ and 802.1Q tunneling, an attempt to change the native VLAN for the 802.1Q trunk port results in BPDUs continuing to be sent with the 1q-tag as VLAN ID=1 which was originally configured as the default. While this problem is occurring, adding the native VLAN to the trunk port's allowed list causes the root bridge to stop sending BPDUs. The workaround is to put the native VLAN into the MISTP instance. This problem is resolved in software release 6.3(6). (CSCdw77209)
- The 802.1X authenticator PAE does not honor EAPOL-Logoff frames. Windows XP sends an EAPOL-Logoff frame when an authenticated user logs off. This is normal behavior. However, the switch is not processing the frame because it is sent with a packet body length value of 0. 0 is actually a valid body length for an EAPOL-Logoff frame, but the switch is checking the length and tossing it out because it is 0. This problem is resolved in software release 6.3(6). (CSCdw94109)

- Under some circumstances, the configuration for EtherChannels might fail when the configuration is taken from a TFTP server or Flash memory, if the ports that belong to that channel are up. This problem is resolved in software release 6.3(6). (CSCdw30990)
- When a module transitions from the “OK” state to the “Other” state there is no log message specifically indicating that such a change has occurred. This problem is resolved in software release 6.3(6). (CSCdw35101)
- When port security is enabled on a port that has been configured as an auxiliary VLAN port, the attached phone does not register when the module is reset. The workaround is to disable port security on the port. This problem is resolved in software release 6.3(6). (CSCdw75648)
- When a link goes up and down repeatedly, the autostate mechanism might fail and the VLAN interface state on the MSFC and the VLAN state on the supervisor engine go out of synchronization. The workaround is to enable spanning tree for the VLAN and enable PortFast on the port. This problem is resolved in software release 6.3(6). (CSCdw75382)
- You might see a loss of unicast forwarding across a 4-port Gigabit EtherChannel between two Catalyst 6000 family switches if RSPAN is configured on a VLAN and you have IGMP joins coming on a port that is part of the EtherChannel. If RSPAN is not configured, there is no problem. The problem appears shortly after enabling multiple “Semantic Ghost” sessions using IP multicast. Broadcast, multicast, and unknown unicast traffic is not affected. The workaround is to disable and then reenable channel ports on one side of the link. This problem is resolved in software release 6.3(6). (CSCdw70357)
- If spanning tree is disabled for any VLAN and the inband interface fails to transmit the PDU, there could be a reload. This problem is resolved in software release 6.3(6). (CSCdw86020)
- The syslog message SYS-5-MOD_DCPWRMISMATCH should be changed to SYS-1-MOD_DCPWRMISMATCH because the message indicates a severe problem (faulty module needs to be replaced). This problem is resolved in software release 6.3(6). (CSCdw75441)
- Creating a VLAN through SNMP might force the VTP mode to client. This problem does not exist if the VLAN is configured through the CLI. This problem is resolved in software release 6.3(6). (CSCdw92651)
- A switch running IGMP snooping may stop adding multicast router ports to the outgoing interface list of all multicast groups. The workaround is to disable and then reenable IGMP snooping on the switch. This problem is resolved in software release 6.3(6). (CSCdw59483)
- The switch does not respond correctly to community strings containing a forward slash (/). The workaround is to remove the forward slash from the community string. This problem is resolved in software release 6.3(6). (CSCdx03088)

Open and Resolved Caveats in Software Release 6.3(5)

These sections describe open and resolved caveats in supervisor engine software release 6.3(5):

- Open Caveats in Software Release 6.3(5), page 118
- Resolved Caveats in Software Release 6.3(5), page 118

Open Caveats in Software Release 6.3(5)

This section describes open caveats in supervisor engine software release 6.3(5):

- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- In a system with a switch fabric module installed, a fabric-enabled module may not come online after you power it down and up or perform an OIR. This problem occurs only if the switching mode reverts to bus-mode. The workaround is to reset the system. (CSCdw30824)
- In rare circumstances, a designated port might be stuck in the spanning tree "listening" state and still be transmitting BPDUs. This does not introduce problems with spanning tree convergence or cause loops. (CSCdv89566)
- During bootup in a redundant configuration, the active supervisor engine reboots twice if the diagnostic mode is set to bypass. The workaround is to set the diagnostic mode to minimal or complete. (CSCdw36342)
- In rare circumstances, an MT-RJ Gigabit Ethernet port with autonegotiation enabled might not be able to achieve link up after being disabled and then enabled. (CSCdw50266)
- In rare circumstances, a Gigabit Ethernet GBIC port cannot achieve link up through autonegotiation. (CSCdw52651)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- 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)

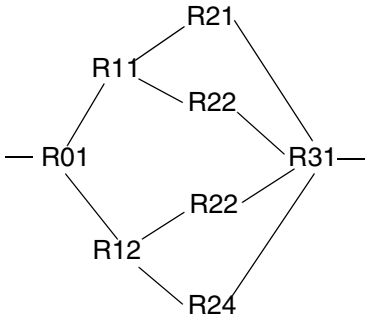
Resolved Caveats in Software Release 6.3(5)

This section describes resolved caveats in supervisor engine software release 6.3(5):

- Improper handling of IGMP version 3 packets might cause the switch to reload. The Catalyst 6000 family switches currently do not officially support IGMP version 3 but we are able to handle IGMP version 3 packets. IGMP version 3 provides support for multiple groups to be included in a message and each group can be associated with a number of IP addresses that can result in large packets. Currently we do not have the ability to parse multiple groups, which might cause problems. The workaround is to downgrade IGMP version 3 hosts to send only IGMP version 2 joins and even when sending version 3 joins, have only one group in the join message. This problem is resolved in software release 6.3(5). (CSCdu80305) (CSCdv45868) (CSCdw46716).

- A new CLI command has been added to include Layer 4 ports in a load-balancing hash. When multiple paths are available to reach a destination (see Figure 1), the new hash is applied to pick the path to be used for forwarding. Prior to this enhancement, the CEF load balancing on PFC2 only used a source IP/destination IP-based hash.

Figure 1 Network Example



For the above network topology, the following configuration is recommended:

  - Use the defaults for load balancing in routers R01, R21, R22, R23, and R24
  - Include Layer 4 ports for load balancing in routers R11 and R12

Use the following command to include or exclude Layer 4 ports in the hash:

```
set mls cef load-balance {full | source-destination-ip}
```

This problem is resolved in software release 6.3(5). CSCdv64614

- In a redundant configuration running a software release prior to release 6.2(1), if the active supervisor engine experiences a minor hardware problem, the switch might not automatically failover to the standby supervisor engine. Software releases 6.2(1) and later have a “redundancy enhancement” feature that provides more efficient system fault detection and recovery mechanisms for redundant configurations. This feature is on by default in releases 6.2(1) and later. The above problem can be avoided by upgrading to releases 6.2(1) or later. (CSCdw46041)
- In situations where static/permanent multicast CAM entries are used, during a designated router failover, the multicast *odd* Layer 2 ltl indices programming might be effected. The problem is still there when the original designated router reboots and comes online. This ltl indices programming problem could lead to multicast packet drops in the nondesignated router. The workaround is to force the multicast Layer 2 static CAM entries to be created first, before IGMP snooping creates source only entries (after seeing the traffic). The workaround is accomplished as follows:
  - Stop the multicast traffic.
  - Clear all the CAM permanent entries.
  - Create the CAM entries again, including the internal router ports.
  - Start the multicast traffic.

  This problem is resolved in software release 6.3(5). (CSCdw57540)
- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(5). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(4a)

These sections describe open and resolved caveats in supervisor engine software release 6.3(4a):

Open Caveats in Software Release 6.3(4a)

This section describes open caveats in supervisor engine software release 6.3(4a):

- In a system with a switch fabric module installed, a fabric-enabled module may not come online after you power it down and up or perform an OIR. This problem occurs only if the switching mode reverts to bus-mode.

  The workaround is to reset the system. (CSCdw30824)

- In rare circumstances, a designated port might be stuck in the spanning tree "listening" state and still be transmitting BPDUs. This does not introduce problems with spanning tree convergence or cause loops. (CSCdv89566)

- In rare circumstances, an MT-RJ Gigabit Ethernet port with autonegotiation enabled might not be able to achieve link up after being disabled and then enabled. (CSCdw50266)

- In rare circumstances, a Gigabit Ethernet GBIC port cannot achieve link up through autonegotiation. (CSCdw52651)

- During bootup in a redundant configuration, the active supervisor engine reboots twice if the diagnostic mode is set to bypass. The workaround is to set the diagnostic mode to minimal or complete. (CSCdw36342)

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)

- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 6.3(4a)

This section describes resolved caveats in supervisor engine software release 6.3(4a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(4a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(4)

These sections describe open and resolved caveats in supervisor engine software release 6.3(4):

- Open Caveats in Software Release 6.3(4), page 121
- Resolved Caveats in Software Release 6.3(4), page 122

Open Caveats in Software Release 6.3(4)

This section describes open caveats in supervisor engine software release 6.3(4):

- In a system with a switch fabric module installed, a fabric-enabled module may not come online after you power it down and up or perform an OIR. This problem occurs only if the switching mode reverts to bus-mode.

  The workaround is to reset the system. (CSCdw30824)
- In rare circumstances, a designated port might be stuck in the spanning tree "listening" state and still be transmitting BPDUs. This does not introduce problems with spanning tree convergence or cause loops. (CSCdv89566)
- In rare circumstances, an MT-RJ Gigabit Ethernet port with autonegotiation enabled might not be able to achieve link up after being disabled and then enabled. (CSCdw50266)
- In rare circumstances, a Gigabit Ethernet GBIC port cannot achieve link up through autonegotiation. (CSCdw52651)
- During bootup in a redundant configuration, the active supervisor engine reboots twice if the diagnostic mode is set to bypass. The workaround is to set the diagnostic mode to minimal or complete. (CSCdw36342)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 6.3(4)

This section describes resolved caveats in supervisor engine software release 6.3(4):

- During module bringup, the port interfaces are operational but the MOD_PORTINTFOUTOFSYNC syslog is incorrectly emitted. No user action is required. This problem is more often seen with fabric-enabled WAN modules. This problem is resolved in software release 6.3(4). (CSCdw36125)
- In a switch with redundant supervisor engines and a four-port Etherchannel formed with the four uplink ports, when two ports on the standby supervisor engine go down when the standby supervisor engine is removed, there might be traffic loss of up to 20 seconds across the EtherChannel. This problem is resolved in software release 6.3(4). (CSCdw06736)
- When IGMP snooping is enabled, multicast control-plane traffic, such as PIM Hellos and IGMP join/leaves, are not correctly handled by the switch when arriving over a WS-X6101 (LANE module). This situation disrupts multicast traffic to receivers that are connected to this module. A workaround is to disable IGMP snooping. This problem was in software releases 6.3(2) and 7.1(1). This problem is resolved in software release 6.3(4). (CSCdw24562)
- HSRP switchover is not always reliable on VLAN interfaces configured with multiple HSRP groups and secondary IP addresses. The MSFC software shows that the switch is active for an HSRP group, but the supervisor engine hardware might not be properly programmed to recognize the HSRP MAC as a router MAC. Therefore, traffic destined to the HSRP MAC of the problem group will be switched in software, causing high interrupt-driven CPU utilization. In some cases, initiating another HSRP switchover for the problem group will resolve the problem. However, in some cases, you must reset the entire switch to force correct MAC address programming (resetting the MSFC only will not recover from the problem). This problem is resolved in software release 6.3(4). (CSCdw32821)
- In a Catalyst 6000 family switch with Supervisor Engine 2 running supervisor engine software prior to software release 6.3(4), multicast packet loss for a particular group might be seen in either of the following circumstances:
  - When an output interface (OIF) is deleted from the MMLS shortcut entry for that group
  - When IGMP Fast Leave is enabled and the last host leaves that group triggering a multicast fast-drop (MFD) delete on the router

  The amount of packet loss in either of these cases would be very small, but would vary depending on the multicast traffic rate for the group and the amount of time it takes for these delete processes to occur in the switch. This problem is resolved in software release 6.3(4). (CSCdv67153)

- When a Catalyst 6000 family switch Gigabit Ethernet port is connected to a partner through DWDM equipment, there could be autonegotiation timing issues dependent on the DWDM configuration. Under these conditions, autonegotiation will fail and the link will not come up. The workaround is to remove autonegotiation from both ends of the link or change the DWDM configuration. This problem is resolved in software release 6.3(4).

  Additionally, to address the timing issues, two new CLI commands are introduced in software release 6.3(4):

  set port sync-restart-delay *mod/port delay*

  show port sync-restart-delay *mod/port*

  Refer to the *Catalyst 6000 Family Command Reference,* Release 6.3 for command usage information. (CSCdv58675)

- Due to the Secure Shell (SSH) CRC-32 integrity check vulnerability, unauthorized attempts to access a number of networked Catalyst 6000 family switches might cause the switches to reset with watchdog timeouts. This problem is resolved in software release 6.3(4). (CSCdv85279)

- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. This problem is resolved in software release 6.3(4). (CSCdv32362)

- The **set port broadcast** command "rounds off" any fractional value to the lowest numeric value. For example, if you enter **set port broadcast** *mod/port 0.99%*, it would round the threshold value to 0 percent (you would not have a threshold value). Another example is if you enter **set port broadcast** *mod/port 1.99%*, it would set the threshold to 1 percent (the lowest numeric nonfractional value). This problem is resolved in software release 6.3(4). (CSCdv32874)

- When you query for SNMP object "portOperStatus" from the CISCO-STACK MIB, the ports on the 8-port T1 PSTN interface module (WS-X6608-T1) might report the wrong value such as value 2 (OK) even if the port is down or not connected. This problem is resolved in software release 6.3(4). (CSCdv53207)

- On switches with Supervisor Engine 2/MSFC2, a large number of access control lists (ACLs) with many "range," "lt," and "gt" operations might fail logical operator unit (LOU) expansion and not be programmed into hardware. The ACLs are processed in software. This problem is resolved in software release 6.3(4). (CSCdv66630)

- In certain instances, disabling IGMP snooping may cause a Catalyst 6000 family switch running software release 6.3(2) to reload with a watchdog timeout. This problem is resolved in software release 6.3(4). (CSCdv73706)

- A port scanning tool report might list TCP port 7161 (TCP port 7161 is used for internal purposes on the switch). In this particular case, the Cisco Secure Scanner reported the switch listening on TCP port 7161. There is no security issue because switches validate all connection requests and all external connection requests are dropped; no external connection can be established. This problem is resolved in software release 6.3(4). (CSCdv76430)

- When the switch is running out of Layer 4 operators, it attempts to expand an ACE into an equivalent set of multiple ACEs. In certain cases, the expansion logic is not optimal enough, and may fail the operation resulting in a syslog message that reports a failure to fit the ACL into the TCAM. This problem is resolved in software release 6.3(4). (CSCdv79139)

- The 48-port 10/100BASE-TX Ethernet module (WS-X6548-RJ-45) might drop frames smaller than 68 bytes. The problem was observed when a non-Catalyst device was connected to a WS-X6548-RJ-45 module through an 802.1Q trunk. This problem is resolved in software release 6.3(4). (CSCdv86149)

- With a Supervisor Engine 1 and a lot of reflexive ACEs configured and timing out at the same time, the switch might fail with a watchdog timer exception. This problem is resolved in software release 6.3(4). (CSCdv76879)
- Upgrading from supervisor engine software release 6.1.4 to release 6.3.3 might cause TCP and UDP access lists to convert to full IP access lists that could render the switch unreachable. This problem is resolved in software release 6.3(4). (CSCdw06965)
- When accessing the switch through an HTTP interface, the switch might reset with a TLB exception. This problem is resolved in software release 6.3(4). (CSCdw02887)
- If you have two switches with redundant supervisor engines, and they are connected through an EtherChannel configured on port 1/1 and 2/1 on both chassis, if you remove the active supervisor engine in one chassis and then power cycle the second chassis, you might lose connectivity over the channel. This problem only occurs if the channel mode is set to **on** on both chassis. The workaround is to set the channel mode to **desirable**. This problem is resolved in software release 6.3(4). (CSCdv01221)
- Changing the CISCO-STP-EXTENSIONS-MIB object "stpxUplinkFastEnabled" to enable does not change the required bridge parameters as the equivalent CLI command does. This problem is resolved in software release 6.3(4). (CSCdw07008)
- Some Cisco Catalyst switches, running certain Catalyst OS software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to reload and result in a switch reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack.

  This vulnerability is documented as Cisco bug ID CSCdw19195. There are workarounds available to mitigate the vulnerability. An advisory is posted at this URL:

  http://www.cisco.com/warp/public/707/catos-telrcv-vuln-pub.shtml

  The following workarounds can be implemented.

  – If SSH is available in the code base, use SSH instead of Telnet and disable Telnet.

    For instructions how to do this, refer to this URL:

    http://www.cisco.com/warp/public/707/ssh_cat_switches.html.

  – Apply Access Control Lists (ACLs) on routers / switches / firewalls in front of the vulnerable switches such that traffic destined for Telnet port 23 on the vulnerable switches is only allowed from the network management subnets.

  This problem is resolved in software release 6.3(4). (CSCdw19195)

Open and Resolved Caveats in Software Release 6.3(3)x1

These sections describe open and resolved caveats in supervisor engine software release 6.3(3)x1:

- Open Caveats in Software Release 6.3(3)x1, page 125
- Resolved Caveats in Software Release 6.3(3)x1, page 125

Open Caveats in Software Release 6.3(3)x1

This section describes open caveats in supervisor engine software release 6.3(3)x1:

- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.3(3)x1

This section describes resolved caveats in supervisor engine software release 6.3(3)x1:

- An error can occur with management protocol processing. Use the following URL for further information:
  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(3)x1. (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(3)x

These sections describe open and resolved caveats in supervisor engine software release 6.3(3x):

- Open Caveats in Software Release 6.3(3)x, page 125
- Resolved Caveats in Software Release 6.3(3)x, page 126

Open Caveats in Software Release 6.3(3)x

This section describes open caveats in supervisor engine software release 6.3(3)x:

- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)

- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.3(3)x

This section describes resolved caveats in supervisor engine software release 6.3(3)x:

- 48-port 10/100BASE-TX Ethernet module (WS-X6548-RJ-45) ports configured as dot1q trunks will drop any dot1q encapsulated frames that are less than 68 bytes. This problem is resolved in software release 6.3(3)x. (CSCdv86149)

Open and Resolved Caveats in Software Release 6.3(3a)

These sections describe open and resolved caveats in supervisor engine software release 6.3(3a):

- Open Caveats in Software Release 6.3(3a), page 126
- Resolved Caveats in Software Release 6.3(3a), page 127

Open Caveats in Software Release 6.3(3a)

This section describes open caveats in supervisor engine software release 6.3(3a):

- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 6.3(3a)

This section describes resolved caveats in supervisor engine software release 6.3(3a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(3a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(3)

These sections describe open and resolved caveats in supervisor engine software release 6.3(3):

- Open Caveats in Software Release 6.3(3), page 127
- Resolved Caveats in Software Release 6.3(3), page 128

Open Caveats in Software Release 6.3(3)

This section describes open caveats in supervisor engine software release 6.3(3):

- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.3(3)

This section describes resolved caveats in supervisor engine software release 6.3(3):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. This problem is present in all 6.x releases prior to release 6.3(3). This problem is resolved in software release 6.3(3). (CSCdv54808)
- If you have an EtherChannel configured with two ports in ON mode, when you set one of the channel ports to EtherChannel mode OFF, the other port does not join spanning tree and you lose connectivity over that port. The workaround is to either set both ports to ON mode or set both ports to OFF mode. This problem is resolved in software release 6.3(3). (CSCdu77808)
- The switch might reset with a TLB exception after running the **clear config snmp** command. This problem is resolved in software release 6.3(3). (CSCdu32549)
- When a Catalyst 6000 family switch running supervisor engine software is connected to a switch running Cisco IOS software on the supervisor engine and both switches have VTP enabled, the Cisco IOS VTP might have a higher VTP configuration revision. In this event, the Cisco IOS switch tries to update the VTP on the switch running supervisor engine software. The switch running Cisco IOS has VLAN 1 translated to VLAN 1003 by default (Token Ring type VLAN), and the switch running supervisor engine software does not support this configuration resulting in an undefined VLAN configuration. If you try to configure the affected VLAN (VLAN 1 in this case), the system might reset with a watchdog timeout. This problem was corrected as follows: When the switch running supervisor engine software experiences the problem, it changes to VTP transparent mode and the following message is displayed:

  ```
  VTP-4-UNSUPPORTEDCFGRCVD:Rcvd VTP advert with unsupported vlan config on trunk 3/24 -
  VTP mode changed to transparent
  ```

  This problem is resolved in software release 6.3(3). (CSCdu32627)
- You might experience a problem with the following configuration: A Layer-2 Gigabit Ethernet port on the WS-X6516-GBIC module is linked to a Gigabit port on the OSM-4GE-WAN-GBIC module. Both ports are configured as a trunk. For each subinterface configured on the OSM side, the corresponding VLAN spanning tree on the Layer 2 trunk is put in blocking mode. The **show spantree statistics** command for that VLAN shows that for every BPDU the switch sends, the switch receives a BPDU back; the OSM module is looping the BPDUs back to the Layer 2 port on the WS-X6516-GBIC module. The workaround is to disable spanning tree on the Layer 2 VLANs that are trunked to the OSM Gigabit port; do this using the **set spantree disable** *vlan_id* command. This problem is resolved in software release 6.3(3). (CSCdu48827)
- This problem might occur when you Telnet into the switch and are prompted for a password. In software releases prior to 6.x.x, if you press the Enter key three times without entering a password, the connection is closed and the prompt returns to the device where the Telnet session was initiated. In version 6.x.x, the prompt continues to come back, regardless of how many times you press the Enter key. This problem is resolved in software release 6.3(3). (CSCdv21334)
- The switch might experience a memory leak if TACACS accounting is enabled and multiple Telnet sessions are established (concurrently or nonconcurrently). The memory leak could lead to a system reset or the switch could become unreachable. The workaround is to disable TACACS accounting and then reset the switch to free up the memory buffers. This problem is resolved in software release 6.3(3). (CSCdv38306)

- The switch might be unreachable on the management VLAN and not appear in the **show cdp neighbors** command output, however, user traffic is normal. Under these conditions, the switch displays a "Run out of system memory, screen scrolling disabled" message. The workaround is to disable TACACS accounting using the **set accounting commands disable** command and then reset the switch. This problem is resolved in software release 6.3(3). (CSCdu25416)
- When there is a native VLAN mismatch on a dot1Q trunking port, and one of the native VLANs is VLAN 1, changing the channel mode of the port from auto to desirable might cause the port to repeatedly leave and then join the bridge port. The workaround is to fix the native VLAN mismatch. This problem is resolved in software release 6.3(3). (CSCdv39631)
- In rare circumstances, a port might be connected but not added to the spanning tree database and therefore not be able to pass traffic. The workaround is to move the connection to another port. This problem is resolved in software release 6.3(3). (CSCdv42998)
- A switch with Supervisor Engine 2 and MSFC2 may sometimes forward packets for some subnets to the wrong next hop. The problem is due to outdated prefix entries being present when hardware TCAM blocks are freed up; the hardware may forward the packet due to a match with an outdated entry. The workaround is to use the **clear ip route** command. This problem is resolved in software release 6.3(3). (CSCdv49956)
- On a switch with Supervisor Engine 2, you might not be able to add permanent CAM table entries when a port is trunked and in a down state. When the port is trunked and in a down state, the **set cam permanent** command fails when it is part of any VLAN other than the native VLAN. This problem is resolved in software release 6.3(3). (CSCdv55032)
- When the active HSRP router configured on the MSFC goes to standby state, the router CAM entry for the virtual MAC address is not removed; packets are sent to the standby router instead of the active router. This results in hosts connected to the local switch losing connectivity to their default gateway (HSRP router). This problem is resolved in software release 6.3(3). (CSCdv56346)
- After a high-availability switchover, the inconsistency checker might not detect mask corruption in a TCAM entry. This problem is resolved in software release 6.3(3). (CSCdv63408)
- With a Switch Fabric Module (SFM) installed, after a high-availability switchover, unicast and multicast traffic might get duplicated. This problem is resolved in software release 6.3(3). (CSCdv62160)
- During normal operation, when a switch receives a PIMv1 reachability packet (from the route processor) when IGMP snooping is enabled, the switch processor realizes that the packet is not a real IGMP packet and floods it to all ports in the VLAN (except the port on which it was received). The problem is that the switch processor is sending the packet back on the port on which it was received. The packet is then looped at Layer 2 causing the switch to become unusable. PIMv1 uses IGMP for control messages and these are forwarded to 224.0.0.2, that is, to all multicast routers not to all PIM routers. The workaround is to reset the switch. This problem is resolved in software release 6.3(3). (CSCdv66125)

Open and Resolved Caveats in Software Release 6.3(2a)

These sections describe open and resolved caveats in supervisor engine software release 6.3(2a):

- Open Caveats in Software Release 6.3(2a), page 130
- Resolved Caveats in Software Release 6.3(2a), page 131

Open Caveats in Software Release 6.3(2a)

This section describes open caveats in supervisor engine software release 6.3(2a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- When the active HSRP router configured on the MSFC goes to standby state, the router CAM entry for the virtual MAC address is not removed; packets are sent to the standby router instead of the active router. This results in hosts connected to the local switch losing connectivity to their default gateway (HSRP router). (CSCdv56346)
- With a Switch Fabric Module (SFM) installed, after a high-availability switchover, unicast and multicast traffic might get duplicated. (CSCdv62160)
- During normal operation, when a switch receives a PIMv1 reachability packet (from the route processor) when IGMP snooping is enabled, the switch processor realizes that the packet is not a real IGMP packet and floods it to all ports in the VLAN (except the port on which it was received). The problem is that the switch processor is sending the packet back on the port on which it was received. The packet is then looped at Layer 2 causing the switch to become unusable. PIMv1 uses IGMP for control messages and these are forwarded to 224.0.0.2, that is, to all multicast routers not to all PIM routers. The workaround is to reset the switch. This problem is resolved in software release 6.3(3). (CSCdv66125)
- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP “link down” on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- If you have an EtherChannel configured with two ports in ON mode, when you set one of the channel ports to EtherChannel mode OFF, the other port does not join spanning tree and you lose connectivity over that port. The workaround is to either set both ports to ON mode or set both ports to OFF mode. (CSCdu77808)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as “not-connected.” This error does not affect operation. (CSCds00575)
- 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 6.3(2a)

This section describes resolved caveats in supervisor engine software release 6.3(2a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(2a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(2)

These sections describe open and resolved caveats in supervisor engine software release 6.3(2):

- Open Caveats in Software Release 6.3(2), page 131
- Resolved Caveats in Software Release 6.3(2), page 132

Open Caveats in Software Release 6.3(2)

This section describes open caveats in supervisor engine software release 6.3(2):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- When the active HSRP router configured on the MSFC goes to standby state, the router CAM entry for the virtual MAC address is not removed; packets are sent to the standby router instead of the active router. This results in hosts connected to the local switch losing connectivity to their default gateway (HSRP router). (CSCdv56346)
- With a Switch Fabric Module (SFM) installed, after a high-availability switchover, unicast and multicast traffic might get duplicated. (CSCdv62160)
- During normal operation, when a switch receives a PIMv1 reachability packet (from the route processor) when IGMP snooping is enabled, the switch processor realizes that the packet is not a real IGMP packet and floods it to all ports in the VLAN (except the port on which it was received). The problem is that the switch processor is sending the packet back on the port on which it was received. The packet is then looped at Layer 2 causing the switch to become unusable. PIMv1 uses IGMP for control messages and these are forwarded to 224.0.0.2, that is, to all multicast routers not to all PIM routers. The workaround is to reset the switch. This problem is resolved in software release 6.3(3). (CSCdv66125)
- On the Intrusion Detection System Module (IDSM), WS-X6381-IDS, the standard-time time zone name that is entered using the **set timezone** *zone_name* command is missing when the IDSM requests a time update from the supervisor engine. (CSCdv32362)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP “link down” on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- If you have an EtherChannel configured with two ports in ON mode, when you set one of the channel ports to EtherChannel mode OFF, the other port does not join spanning tree and you lose connectivity over that port. The workaround is to either set both ports to ON mode or set both ports to OFF mode. (CSCdu77808)

- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.3(2)

This section describes resolved caveats in supervisor engine software release 6.3(2):

- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. This problem is present in all 6.x releases prior to release 6.3(2). This problem is resolved in software release 6.3(2). (CSCdu84704)
- With the PFC2, the "router_sc" field in the flows from NDE version 7 are not configurable using the **ip flow-export source** command on the MSFC2. This problem is resolved in software release 6.3(2). (CSCdu10983)
- When autonegotiation is disabled on a Gigabit Ethernet port and the port is left enabled (but has no link), the port might clock noise into the port in the form of runt packets. After link up, the port may lose received packets at 33 percent, 50 percent, or 100 percent. The workaround is to disable and then reenable the port. To avoid the problem entirely, enable autonegotiation on both ends of the link. This problem is resolved in software release 6.3(2). (CSCdt26686)
- On Catalyst 6000 family switches with redundant supervisor engines (MSFC and PFC) and Multicast Multilayer Switching (MMLS) enabled, disabling hardware versioning might cause the MSFC on the standby supervisor engine to not respond to SCP ping messages. When this happens, a router down event is posted to MMLS but the wrong MSFC module number is posted. MMLS might delete the hardware entries for the MSFC that is still online. The workaround is to reset the MSFC. This problem is resolved in software release 6.3(2). (CSCdu49107)
- The standby supervisor engine might reset with a breakpoint exception under the following conditions:
  - High availability is enabled
  - The following sequence of commands is repeated several times:

    set qos bridged-microflow-policing enable 1-1000

    set qos bridged-microflow-policing enable 1025-4098

    set qos bridged-microflow-policing disable 1-1000

    set qos bridged-microflow-policing disable 1025-4098

  This problem is resolved in software release 6.3(2). (CSCdu55420)

- The MSFC2 might come up faulty after a system reset. This problem is resolved in supervisor engine software release 6.3(2) and Cisco IOS Release 12.1(8a) or higher. (CSCdu51076)
- After reloading the MSFC or MSFC2, the switch might reset due to a watchdog timeout. This problem is resolved in software release 6.3(2). (CSCdu75432)
- In rare circumstances, some VTP VLAN-related high-availability events may be improperly opened and then not closed on the standby supervisor engine. This problem is resolved in software release 6.3(2). (CSCdu64647)
- The switch can process multicast joins at approximately 1000 joins per second or slightly more depending on the load on the system. If the input rate is much more, the switch might start to drop IGMP packets. If the multicast trace printing is set to a level greater than 1, you might see an "IGMP dropped packet" message which could lead to further slowing and a possible reset. The workaround is to disable multicast trace printing by entering the **set trace mcast 0** command. This problem is resolved in software release 6.3(2). (CSCdu73369)
- Under certain conditions, flow statistics for multicast shortcuts might not be sent to the MSFC from the supervisor engine. If this occurs, the MSFC will continually delete and install multicast shortcuts for active flows. This condition can be verified by entering the **show mls ip multicast** command on the MSFC and observing the "Packets switched:" counter. This counter is updated every 10 seconds for active flows. If a flow is seen to be incrementing on the supervisor engine (enter the **show mls multicast group** *group* **source** *source* command on the supervisor engine), but is not incrementing on the MSFC, then this condition is verified. The workaround is to disable and then reenable IGMP snooping. This problem is resolved in software release 6.3(2). (CSCdu78467)
- A host is sending a DVMRP packet (essentially an IGMP unicast packet type in the IP header) to the MSFC through an application called "mrinfo." The unicast IGMP packet destined to the MSFC, might be forwarded by the switch to all ports participating in the same VLAN even though the packet is a unicast packet destined to the MSFC. The workaround is to disable IGMP snooping on the switch. This problem is resolved in software release 6.3(2). (CSCdu81012)
- On the ATM module with supervisor engine software releases 6.2(2) and 6.3(1), the **show sprom** *mod_num sprom_num* command might not display the three SPROMs individually. This problem is resolved in software release 6.3(2). (CSCdu88045)
- With high availability enabled and a large number of interfaces configured, the system might reset with a breakpoint exception when both MSFCs are reset within a few seconds of one another. This problem is resolved in software release 6.3(2). (CSCdu83560)
- With high availability enabled, the Catalyst 6000 family switch might reset with a TLB exception when the standby supervisor engine is coming up after a high-availability switchover. The reset might also occur when EtherChannels are toggled. This problem is resolved in software release 6.3(2). (CSCdv00340)
- In extremely rare conditions, the WS-X6248-RJ-45 10/100BASE-T module might stop forwarding traffic. The module LEDs still show green, CDP traffic is working, and both ends have link. The module receives traffic but does not transmit. This problem is resolved in software release 6.3(2). (CSCdt75278)
- When the 24-port FXS analog interface module (WS-X6224-FXS) is the last device in a VLAN, the VLAN interface goes down. This problem is resolved in software release 6.3(2). (CSCdu82910)
- In extremely rare conditions, when the diagnostic level is set to complete and the switch is power cycled numerous times, the incorrect TCAM mask may be programmed. The workaround is to run the diagnostics at the minimal level. This problem is resolved in software release 6.3(2). (CSCdu89628)

- You might not be able to include spaces in the "community_string" when using the following CLI command: **set snmp community access_type** *community_string*. This problem is resolved in software release 6.3(2). (CSCdv08254)
- A port in PAgP nonsilent mode may behave as if it is in PAgP silent mode if the port has been connected to a nonsilent partner. Therefore, the port may be posted to spanning tree after reset and could cause channel disturbance. This problem is resolved in software release 6.3(2). (CSCdu85834)
- The **set mls agingtime long** *agingtime* command was hidden. It is now available in enable mode. Additionally, the "long aging time" can be displayed using the **show mls** command. This problem is resolved in software release 6.3(2). (CSCdu57528)
- Switches with Supervisor Engine 2 and MSFC2 might experience problems with MLS and CEF. This situation can be seen by the switch sending packets out to the incorrect next hop that might result in either routing loops or the incorrect path (nonoptimal) being used. Symptoms of this problem are as follows:

1. The routing table is showing a correct route (**show ip route** x.x.x.x).
2. The ARP table is showing a correct MAC address for the next hop (**show ip arp** x.x.x.x).
3. The CEF table is correct for route (**show ip cef** x.x.x.x **detail**).
4. The adjacency table is correct (**show adjacency vlan** x).
5. The SW-FIB entry on the Supervisor Engine 2 is correct (**show mls entry cef ip** x.x.x.x/m).
6. The shadow CEF entry on the Supervisor Engine 2 is correct.
7. The packets are getting forwarded to the incorrect next hop.

The workaround is to use the **clear ip route** command.

Before using the **clear ip route** command, verify if steps 1 through 4 are correct. If they are not correct, the problem is most likely Cisco IOS CEF related. This problem is resolved in software release 6.3(2). (CSCdu85211)

- Multicast traffic might stop when you reload or hot insert a WAN module into the switch. This problem is resolved in software release 6.3(2). (CSCdv16667)
- On switches with a Supervisor Engine 1 with MSFC2, when there is an MSFC2 switchover, the hardware IPX shortcuts in the Supervisor Engine 1 may get cleared and then relearned from the MSFC2. During this process, the IPX packets will momentarily hit the MSFC2 CPU. This problem occurs only on an MSFC2 switchover and only with the Supervisor Engine 1 with IPX traffic (there is no problem with the Supervisor Engine 2 or IP traffic). The problem is evident in Cisco IOS Releases 12.1(8a)E2 or earlier and supervisor engine software releases 6.3(1) or earlier.

  This problem is resolved in Cisco IOS Releases 12.1(8a)E3 or later and supervisor engine software releases 6.3(2) and later. (CSCdv01043)
- The switch might drop IP packets because of an incorrect next-hop address programmed by the FIB; the next-hop address might be programmed as a tunnel interface in software. MLS entries show the incorrect next-hop MAC address. This problem is resolved in software release 6.3(2). (CSCdu66626)
- A bus error exception might occur when spanning tree receives an abnormal-sized BPDU on a VLAN and spanning tree is disabled on that VLAN. This problem is resolved in software release 6.3(2). (CSCdu69958)
- Entering the **show security acl log flow ip any any** command in a high-traffic condition with a large number of IP flows may cause switches with the Supervisor Engine 2 to reset with a "mistral interrupt." This problem is resolved in software release 6.3(2). (CSCdu83719)

- When SRM is enabled in a high-availability configuration, the **show module** command might display the status of the MSFCs incorrectly. This problem is resolved in software release 6.3(2). (CSCdv06441)
- The switch might reset with a breakpoint exception in systems with redundant Supervisor Engine 1 configurations that have ASLB (the **set lda** command set) and high availability enabled. This problem is resolved in software release 6.3(2). (CSCdv13493)
- The switch might generate traps with an invalid agent address. When initializing the trap PDU, an invalid agent address, 0.0.0.0, may fill in the data field agent_addr but the trap is still sent out. This problem is resolved in software release 6.3(2). (CSCdv21194)
- When the native VLAN of a trunking port is changed to a VLAN that is not part of the allowed VLANs list, the port shows up in two VLANs after it becomes a nontrunk port. The workaround is to keep the native VLAN in the allowed VLANs list. This problem is resolved in software release 6.3(2). (CSCdu42440)
- When there is an ATM module installed, the switch might reset with a TLB exception while operating on FLASH-MIB objects. This problem is resolved in software release 6.3(2). (CSCdu62043)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)
- In a WS-C6513 slot chassis with an SFM 2 installed, do not install OSMs in slots 4, 9, or 13. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu57062)
- After enabling protocol filtering on a switch with Supervisor Engine 1 and MSFC2, Layer 3 IP traffic might not be MLS switched. The Layer 3 traffic is not sent to the MSFC2 to be routed and traffic stops. The workaround is to disable protocol filtering. Note that MLS shortcuts will not form until the active MSFC2 is reset. This problem is resolved in software release 6.3(2). (CSCdu85304)
- The **show acl harestart** command is a hidden command but is currently available in enable mode. The **harestart** option is an engineering command used during a development phase and has destructive side effects. It should *never* be used in the field. This option will be removed. This problem is resolved in software release 6.3(2). (CSCdv37654)
- On a Supervisor Engine 1 with MSFC, the inband FX1000 port might receive packets but does not transmit them. When the port is in this state, you might see the following symptoms:
  - The switch generates the following message every minute on every connected port if CDP is enabled:

    ```
    2001 Aug 21 15:25:46 EDT -04:00 %CDP-3-SENDFAIL:Transmit failure on port 3/2
    ```

  - The switch is not able to ping its default gateway
  - No devices are able to ping the sc0 interface
  - Traffic through the switch is being forwarded

  The workaround is to reboot the switch. This problem is resolved in software release 6.3(2). (CSCdv15176)
- When the supervisor engine receives an SNMP-Get/GetNext for the objects in the “interfaces” group that correspond to port 15/1 or 16/1 on the MSFC2, the supervisor engine replies with a SNMP-GetReply with a value of 0. However, the MSFC2 correctly reports incoming and outgoing packets when the **show mac** *15/1* or *16/1* command is used. This problem is resolved in software release 6.3(2). (CSCdv25250)

- In rare circumstances, when the switch needs to clear the complete FIB table, it may reload. This problem is resolved in software release 6.3(2). (CSCdv27091)
- In rare circumstances, the Supervisor Engine 2 might reset with an exception during the FIB process. This problem is resolved in software release 6.3(2). (CSCdv11795)
- In rare circumstances, with high availability enabled on the supervisor engines and configuration synchronization enabled on the MSFCs, the standby supervisor engine might reload with a "PID=X SyncTask" exception when the designated MSFC is reloaded. This problem is resolved in software release 6.3(2). (CSCdv18850)
- When trying to apply a policy route map to a private VLAN interface, the MSFC might issue the following message:

  ```
  %ACL-3-PVLAN_ATTACHACLFAIL:Failed to map router ACL to private VLAN 111
  ```

  The workaround is to reconfigure the private VLAN as a regular VLAN. This problem is resolved in software release 6.3(2). (CSCdv29779)
- The PortFast status (portSpantreeFastStart) might be reported incorrectly through SNMP for internal MSFC trunk ports. This causes false alarms for network management products monitoring the portfast state (such as CiscoWorks 2000 Campus Manager). This problem is resolved in software release 6.3(2). (CSCdv19071)
- When a mapped ACL is modified and committed on the active supervisor engine, high-availability synchronization may cause a memory leak on the standby supervisor engine. This problem applies to both Supervisor Engine 1 and Supervisor Engine 2 with high availability enabled and might occur in software releases 5.4(x), 5.5(x), and 6.x. This problem is resolved in software release 6.3(2). (CSCdv38983)
- The Intrusion Detection System Module (IDSM), WS-X6381-IDS, might report alarms with timestamps that are off by one hour from the time displayed on the switch console. The problem occurs if the **set summertime enable** or **set summertime disable** commands are entered on the console while the IDSM is removed or offline. The IDSM may not be notified of any changes when it comes online resulting in the IDSM improperly correcting for daylight saving time. This problem also occurs when the IDSM is first installed and after a new software image has been installed. The workaround is to enable or disable summertime mode and then set the current time when the IDSM is online. These two steps must be performed in the specified order to work properly. An example of the correct order follows:

  ```
  set summertime enable
  set time 12:00:00 09/05/2001
  ```

  This problem is resolved in software release 6.3(2). (CSCdu82389)
- When enabling and disabling unicast RPF with a large routing table, the switch might reset. The commands that would cause this are **ip verify unicast reverse-path** and **no ip verify unicast reverse-path**. This problem is resolved in software release 6.3(2). (CSCdu17478)
- An alarm event might not be generated even though the "alarmValue" has continuously peaked above the "risingThreshold" value. The workaround is to create a trap destination table. This problem is resolved in software release 6.3(2). (CSCdv06651)
- When Multicast Multilayer Switching (MMLS) is running on a switch with redundant supervisor engines and MSFC2s, the active supervisor engine may reset when the PIM-NDR tries to prune an OIF. This can occur under a heavy traffic load when LTL indices used by multicast are exhausted. This problem is resolved in software release 6.3(2). (CSCdu89469)

- In rare circumstances, Secure Shell (SSH) encryption configured switches running supervisor engine software release 6.1(x) or later are vulnerable to a memory corruption problem. Memory corruption and a Syscall exception might occur if the existing encryption keys are cleared while a new key is being generated using the **set crypto key rsa** *bit* **force** command. The workarounds are as follows:
  - Do not attempt to clear the old encryption keys while generating new keys using the **force** option
  - Clear old encryption keys before generating new keys

  This problem is resolved in software release 6.3(2). (CSCdv47234)
- When a subnet entry is being downloaded from the MSFC to the supervisor engine with a mask of 32, it is not programmed correctly in the hardware. This problem is resolved in software release 6.3(2). (CSCdv00961)
- In rare circumstances, with a Supervisor Engine 2 with MSFC2, a packet may get forwarded by the hardware to the wrong next hop. The workaround is to use the **clear ip route** command. This problem is resolved in software release 6.3(2). (CSCdt53782)
- You cannot configure IP, IPX, and MAC ACLs with "dscp 0" under a single policer on the Supervisor Engine 2/PFC2 although this was possible with the Supervisor Engine 1/PFC1. This problem is resolved in software release 6.3(2). (CSCdv22507)

Open and Resolved Caveats in Software Release 6.3(1a)

These sections describe open and resolved caveats in supervisor engine software release 6.3(1a):

- Open Caveats in Software Release 6.3(1a), page 137
- Resolved Caveats in Software Release 6.3(1a), page 139

Open Caveats in Software Release 6.3(1a)

This section describes open caveats in supervisor engine software release 6.3(1a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)

- During system bootup, with a switch fabric module installed, all fabric-enabled modules may fail to come online if the diagnostics are set to "complete" mode and there are a large number of security ACLs (VACLs). Additionally, the standby supervisor engine may fail to respond over the inband channel. These problems are only seen in release 6.3(1). The workaround is to reset the fabric-enabled modules using the **reset** *mod* command.

  To prevent the problem from happening again on a system reset, set the diagnostics level to "minimal" (which is the default) using the **set test diaglevel minimal** command. (CSCdu78714)

  Note This problem has not been seen in later releases.

- If you have an EtherChannel configured with two ports in ON mode, when you set one of the channel ports to EtherChannel mode OFF, the other port does not join spanning tree and you lose connectivity over that port. The workaround is to either set both ports to ON mode or set both ports to OFF mode. (CSCdu77808)
- In a WS-C6513 slot chassis with an SFM 2 installed, do not install OSMs in slots 4, 9, or 13. (CSCdu57062)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 the PFC2, the "router_sc" field in the flows from NDE version 7 are not configurable using the **ip flow-export source** command on the MSFC2. (CSCdu10983)

Resolved Caveats in Software Release 6.3(1a)

This section describes resolved caveats in supervisor engine software release 6.3(1a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.3(1a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.3(1)

These sections describe open and resolved caveats in supervisor engine software release 6.3(1):

- Open Caveats in Software Release 6.3(1), page 139
- Resolved Caveats in Software Release 6.3(1), page 140

Open Caveats in Software Release 6.3(1)

This section describes open caveats in supervisor engine software release 6.3(1):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- The **set port flowcontrol** *mod/port* **send desired** command causes a DTP "link down" on the specified port, and the port is not added to spanning tree. The workaround is to disable and then reenable the port. (CSCdu43064)
- During system bootup, with a switch fabric module installed, all fabric-enabled modules may fail to come online if the diagnostics are set to "complete" mode and there are a large number of security ACLs (VACLs). Additionally, the standby supervisor engine may fail to respond over the inband channel. These problems are only seen in release 6.3(1). The workaround is to reset the fabric-enabled modules using the **reset** *mod* command.

  To prevent the problem from happening again on a system reset, set the diagnostics level to "minimal" (which is the default) using the **set test diaglevel minimal** command. (CSCdu78714)
- If you have an EtherChannel configured with two ports in ON mode, when you set one of the channel ports to EtherChannel mode OFF, the other port does not join spanning tree and you lose connectivity over that port. The workaround is to either set both ports to ON mode or set both ports to OFF mode. (CSCdu77808)
- In a WS-C6513 slot chassis with an SFM 2 installed, do not install OSMs in slots 4, 9, or 13. (CSCdu57062)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)

- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 the PFC2, the "router_sc" field in the flows from NDE version 7 are not configurable using the **ip flow-export source** command on the MSFC2. (CSCdu10983)

Resolved Caveats in Software Release 6.3(1)

This section describes resolved caveats in supervisor engine software release 6.3(1):

- In rare circumstances, when a GBIC Gigabit port is in auto-negotiation enable mode, there is a small time window when configuration changes may occur, and if the remote side of the link changes flow-control parameters within this window, the port on this end of the link may miss the configuration changes and fail to enter correct flow-control mode. This problem is resolved in software release 6.3(1). (CSCdu02663)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). This problem is present in all 6.x releases prior to release 6.3(1). This problem is resolved in software release 6.3(1). (CSCdu38986)
- Including a control character, such as ^C, in a comment line of a configuration file causes the commands following the comment line to be ignored when the configuration file is copied to the running configuration. This problem occurs with all 6.x software releases prior to 6.3(1). This problem is resolved in software release 6.3(1). (CSCdu58728)
- If the system boots up and both SPAN and RSPAN sessions are present, the egress SPAN test might fail for some fabric-enabled modules. Reset the fabric-enabled module to recover from the egress SPAN test failure. Note that when the system boots, a "Minor hardware problem in Module X" message displays and the **show test** *mod* command shows that the EgressSpanTest failed. This problem is resolved in software release 6.3(1). (CSCdu25856)
- When resetting all the Catalyst 6000 family switches in your network topology at the same time, the CBL might not be set properly for some ports (port in forwarding state and CBL set to blocking state). The workaround is to reset one switch at a time or change some mapping configurations on the switch with the problem. This problem is resolved in software release 6.3(1). (CSCdt80179)
- On a Catalyst 6000 family switch, enabling CGMP on the MSFC might modify all membership report source MAC addresses to the supervisor engine MAC address when in "IGMP-CGMP" mode. This would cause all downstream multicast forwarding on CGMP-enabled switches to fail. The workaround is to disable CGMP on all downstream switches. This problem is resolved in software release 6.3(1). (CSCdu28872)

- On a Catalyst 6000 family switch running 6.1.3 and later releases, the CAM permanent filter can be configured but the filter does not show up in the configuration file. This problem is resolved in software release 6.3(1). (CSCdu10501)
- When IGMP snooping is enabled on system with a Supervisor Engine 2, IP packets with protocol number 0 are permitted when ingressing on a VLAN that is mapped with an ACL. This problem is resolved in software release 6.3(1). (CSCdu54041)
- When Autostate is enabled, a VLAN interface should not transition to up state until at least one port in the VLAN is forwarding traffic. This problem is resolved in software release 6.3(1). (CSCdu05914)
- Pinging the nondesignated MSFC2/Supervisor Engine 2 across a WAN interface does not work. This problem is resolved in software release 6.3(1). (CSCdu37990)
- When protocol filtering is enabled, packets not destined to the MSFC may get routed. This problem is resolved in software release 6.3(1). (CSCdu44627)
- Pings from a VLAN that is not configured on the MSFC to another VLAN that is configured on the MSFC fail when the configuration includes an MSFC2 and Supervisor Engine 2. This problem is resolved in software release 6.3(1). (CSCdt96536)

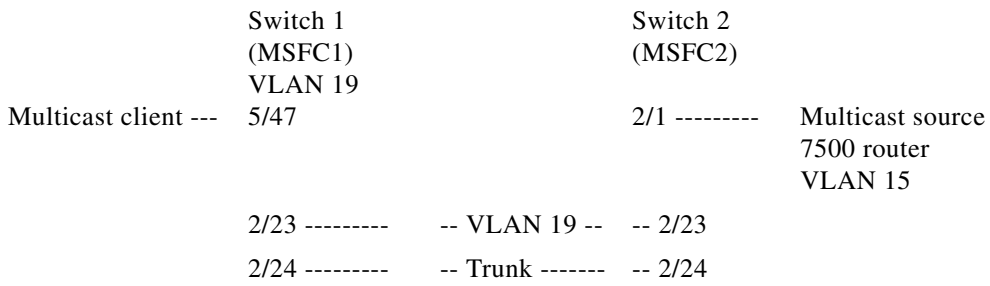
  With software release 6.3(1), by default, packets are bridged to the router rather than being redirected. In software releases prior to release 6.3(1), packets were redirected to the router. If you want to have the packets redirected rather than bridged, enter this command: **set mls rate 300**.
- When an MSFC2 is reloaded from the MSFC2 prompt during heavy traffic, VLAN interfaces may not come up. Symptoms include the IBC interface going down and loopback diagnostics failing for the MSFC2 from the switch side. This problem is resolved in software release 6.3(1). (CSCdu32703)
- It is not possible to configure the debounce timer on a per port basis for Gigabit Ethernet interfaces. This problem is resolved in software release 6.3(1). (CSCdt94458)
- In a system with a Switch Fabric Module installed, the ACL capture feature does not work unless one of the following conditions are met:
  - Traffic is captured and exits on a nonfabric-enabled module port.

  or
  - Traffic is captured and exits on the same fabric-enabled module.

  The WS-X6380 and WS-X6381 modules will not see traffic sent to fabric-enabled modules in the system if the switch is operating in truncated mode. This problem is resolved in software release 6.3(1). (CSCdu31887)
- If the Catalyst 6000 family switch is forwarding traffic in flow-through mode and one fabric-enabled module is already present in the system and you insert, reset, or power up a second fabric-enabled module together with a nonfabric-enabled module, the switching mode changes and some diagnostics may fail for the fabric-enabled modules. Reset the fabric-enabled module to recover from this diagnostics failure. This problem is resolved in software release 6.3(1). (CSCdu22799)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. This problem is resolved in software release 6.3(1). (CSCdu11300)
- 802.1X configuration allows incorrect command syntax. This problem is resolved in software release 6.3(1). (CSCdu27021)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. This problem is resolved in software release 6.3(1). (CSCds39392)

- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. This problem is resolved in software release 6.3(1). (CSCds38753)
- Executing the following tasks in sequence leaves incorrect entries in the forwarding table:
  - 1. Enabling IGMP snooping
  - 2. Enabling protocol filtering
  - 3. Disabling IGMP snooping
  - 4. Disabling protocol filtering

  The workaround is to manually clear these entries. This problem is resolved in software release 6.3(1). (CSCds69447)
- IGMP snooping and multicast MLS might not work reliably because the router ports are not selected correctly in hardware. This problem is resolved in software release 6.3(1). (CSCdt31924)
- Octets associated with ifInDiscard packets might not be counted. This problem is resolved in software release 6.3(1). (CSCdt62359)
- When the ifOperStatus value for the port changes (the port is enabled and disabled, or the link is brought up and down), the ifLastChange value for the port does not change. This problem is resolved in software release 6.3(1). (CSCdt69418)
- When IGMP snooping is enabled and the QoS default action is set to non-zero on one of the two switches in the topology below, both MSFCs might experience high CPU utilization (99 percent). The problem does not occur if the QoS default action is set equally on both switches or if IGMP snooping is disabled.



  This problem is resolved in software release 6.3(1). (CSCdt73910)
- When a Cisco IOS ACL is merged with a VACL for the same interface, and if the resulting ACL exceeds the size of the TCAM, the ACL compiler returns an error. This error is not handled properly and causes the supervisor engine to reload. This problem is resolved in software release 6.3(1). (CSCdu10105)
- In extremely rare conditions, the Catalyst 6000 family switch might hang and not pass any traffic when a 24-MB Flash PC card (PCMCIA) is hot swapped very rapidly or when the Flash card is removed when data is being written/read to/from the Flash card. This problem is resolved in software release 6.3(1). (CSCdu23412)

- There is a problem with parallel TACACS+/RADIUS/KERBEROS access. Authentication protocols (TACACS+, RADIUS, Kerberos) use a global character array to store the user input (such as passwords). As the buffer is global, it is shared by all console and Telnet sessions and may contain input from multiple Telnet sessions which might cause incorrect password input for authentication.

  The following example is used for clarification.

  - User A—username test, password cisco
  - User B—username test2, password cisco

  User A Telnets to the switch, types "test," presses Enter, types the password, but does not press Enter. On the other host, User B also Telnets to the switch, types "test2," presses Enter, types the wrong password and presses Enter which causes a login failure. User A goes back to the first switch and because the password is already there, User A presses Enter, but the password is treated as an incorrect password.

  This problem is resolved in software release 6.3(1). (CSCdu35551)

- When an RMON event and alarm are added to a Catalyst 6000 family switch running software release 6.1(2), only the alarm will survive a reload. The workaround is to reinstall the event after a reload. This problem is resolved in software release 6.3(1). (CSCdu26550)
- The chassis temperature alarm does not return the correct status through both CLI and SNMP. This problem is resolved in software release 6.3(1). (CSCds21308)
- In extremely rare conditions, all ports on the WS-X6248-RJ45 module might become unreachable with traffic forwarding stopping on all ports. The port LEDs would be orange and the **show port** command would show the ports as connected. The workaround is to reset the module using the **reset** command. This problem is resolved in software release 6.3(1). (CSCds75479)
- When polling a Supervisor Engine 1A through SNMP, there must be at least a 1 millisecond delay between successive SNMP "Gets." Without a minor delay, the Catalyst 6000 family switch will output the following display message:

  ```
  2001 Mar 30 14:03:53 %IP-3-UDP_SOCKOVFL:UDP socket 1034 overflow
  ```

  This problem does not affect switch performance. This problem is resolved in software release 6.3(1). (CSCdt86655)

- When using the channelized T1 port adapter with the FlexWAN module, traffic might not be dCEF switched and instead be fast switched by the MSFC2. The problem is caused by the PFC2 not setting the correct CEF entry. This problem is resolved in software release 6.3(1). (CSCdu11349)
- The **clear counters** command does not clear EtherChannel MAC counters displayed using the **show channel mac** command. This problem is resolved in software release 6.3(1). (CSCdt89431)
- When an EtherChannel bundles ports across different modules, if one of the modules that contains the channeling ports gets reset, it may cause ports to leave the bridge port and to converge again while the module comes back online. This problem is resolved in software release 6.3(1). (CSCdu17107)
- You might not be able to enable logging for dynamic VLANs using the **set logging level dvlan** command:

  ```
  Console> (enable) set logging level dvlan 7
   Invalid Facility
  Console> (enable)
  ```

  This problem is resolved in software release 6.3(1). (CSCdu19163)

- After an MSFC switchover, the loopback interfaces of the two MSFCs are unpingable. There are three workarounds:
  - Enter the **clear ip route** command on the designated MSFC.
  - Set the "maximum-paths" to 5 or 6.
  - Set the bandwidths of the interfaces so there is only one best path between both MSFCs. If you are using EIGRP, the variance should be one.

  This problem is resolved in software release 6.3(1). (CSCdu23536)
- In extremely rare conditions, a breakpoint exception might occur when you are creating a large number of high availability events, such as adding and deleting VLANs using a script. The only workaround is to reset the switch. This problem is resolved in software release 6.3(1). (CSCdt73213)
- The GVRP protocol cannot be configured on WAN module Gigabit ports. This problem is resolved in software release 6.3(1). (CSCdu22779)
- In certain instances, WAN modules may not be recognized as modules that can utilize the Switch Fabric Module, so when WAN modules are installed, the switching mode may not be correct. Traffic will switch normally, but overall system throughput may be affected. Since the incorrect switching mode is observed after a WAN module is powered down, reset, or disabled, for maximum throughput it is recommended that you do not reset, power down, or disable WAN cards. This problem is resolved in software release 6.3(1). (CSCdt05051)
- The Cisco IOS **show sprom** command does not work. This problem is resolved in software release 6.3(1). (CSCdt75741)
- A token ring VLAN on the active supervisor engine might be translated into another VLAN on the standby supervisor engine after performing a high-availability switchover. This problem is resolved in software release 6.3(1). (CSCdu08852)
- When the spanning tree mode is set to MISTP or MISTP-PVST+, stpxSpanningTreePathCostMode can only be set to "long." However, in software releases 6.1(x) and 6.2(1), when stpxSpanningTreePathCostMode is set to "short," there is no error and when stpxSpanningTreePathCostMode is set to "long," there is a "commitFailed" error. This problem is resolved in software release 6.3(1). (CSCdu27119)
- An entry (*, G) installed as a complete shortcut will change to a partial shortcut entry when the OIF changes to NULL. When the OIF is reinstalled, the (*, G) entry does not return to a complete shortcut but remains a partial shortcut. If traffic for this group is being sent at a high rate, you may observe high CPU utilization on the MSFC. This problem is resolved in software release 6.3(1). (CSCdu30097)
- A new MIB object, sysStatus, was added to display the operational status of the system. This problem is resolved in software release 6.3(1). (CSCdu31559)
- When you start a Telnet session from the Catalyst 6000 family switch and press **Ctrl-C** immediately after entering the **telnet** *ip_address* command, you stop the Telnet session but the terminal session (console or Telnet) locks. If you press **Ctrl-C** again, a new prompt appears but you still cannot enter commands. The workaround is to reset the switch. This problem is resolved in software release 6.3(1). (CSCdu33233)
- The Catalyst 6000 family switch sends the wrong trap OID (.1.3.6.1.2.1.47.2.1.0.1) for the entConfigChange MIB. This problem is resolved in software release 6.3(1). (CSCdu34057)
- The OIF of an active (s, g) flow may change to NULL temporarily and then return to the correct OIF state. When this happens, multicast traffic on that flow is temporarily black-holed while the OIF is NULL. This problem is resolved in software release 6.3(1). (CSCdu35684)

- On Supervisor Engine 2, if an ACL uses more than one TCP flag combination with different results, traffic may not be correctly access controlled after modifying the TCP flag combinations. This problem is resolved in software release 6.3(1). (CSCdu38180)
- On the Catalyst 6000 family switch, you might experience this problem with SNMP. When you configure SNMP as follows, you can then modify the configuration through snmpset:
  - snmp community read-only workgroup
  - snmp community read-write workgroup
  - snmp community read-write-all workgroup

  When you remove the read-write and read-write-all and then run the snmpset again, you can modify the configuration even though you removed the read-write. This problem is resolved in software release 6.3(1). (CSCdu38452)
- The "hidden" commands, **set igmp mode** and **show igmp mode**, have been moved to enable mode. For descriptions of these commands, see the *Catalyst 6000 Family Command Reference*, software release 6.3. This problem is resolved in software release 6.3(1). (CSCdu39547)
- If two or more route-map entries are used for the same map that is used for policy routing on an interface, the TCAM might overflow during TCAM expansion. The TCAM "entry capacity exceeded" message displays immediately after the policy route-map statement is applied to the interface:

  ```
  12:28:12: %FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
   12:28:12: %FM-4-RACL_REDUCED: Interface Vlan196 routed traffic will be software
  switched in ingress direction(s)
  ```

  This problem is resolved in software release 6.3(1). (CSCdu40762)
- In extremely rare conditions, the FIB table on Supervisor Engine 2 may be inaccurate. If this occurs, it would be after reloading the MSFC2. The workaround is to execute the following commands in the order given on the MSFC2:
  - 1. **no ip routing**
  - 2. **ip routing**

  Note that this results in temporary traffic disruption. This problem is resolved in software release 6.3(1). (CSCdu43281)
- When clearing a primary VLAN (of a private VLAN) on the active supervisor engine, the VLAN might not be cleared properly on the standby supervisor engine. This may cause problems with the VLAN after a high-availability switchover. This problem is resolved in software release 6.3(1). (CSCdu31513)
- If you attempt to set a long LCD banner (more than 800 characters) from the switch console using the **set banner lcd** command, memory corruption may be detected causing the switch to reset unexpectedly. This problem is resolved in software release 6.3(1). (CSCdu45862)
- When the NetFlow type is set to "full-vlan" or "source," the online diagnostic inline rewrite tests fail when a module is hot inserted. The "full-vlan" and "source" NetFlow types can only be triggered by the router and then cannot be set back using the **set mls flow** *flow_type* CLI command, as the router's decision has the highest priority. Online diagnostics support only the three basic netflow types: destination, destination-source, and full. With software release 6.3(1), support for "full-vlan" and "source" has been added. This problem is resolved in software release 6.3(1). (CSCdu44306)
- If an OC-12 ATM Module (WS-X6101-OC12-SMF/MMF) is installed but in a disabled state and a high-availability switchover occurs, the switch might reset with a Bus Timeout NMI. The workaround is to enable the ATM module or power down the module if it is not in use. This problem is resolved in software release 6.3(1). (CSCdu11713)

- Under very rare circumstances, the WS-X6248 10/100BASE-T modules could get into a fatal state that is beyond recovery by the built-in software recovery mechanisms. If this occurs, the only way to recover from this error condition is to completely reset the module or power the module off and then on. The **set lcperroraction** command has been modified and enhanced to react automatically upon detection of this fatal error condition. The LCPERRORACTION can be set to one of the following three levels:
  - LCPERRORACTION ignore: This is the default level. Errors are logged. No action is taken.
  - LCPERRORACTION operator: Errors are logged. In addition, the system prints a message requesting that you manually power the module off and then on.
  - LCPERRORACTION system: Errors are logged. The system automatically powers the module off and then on.

  This problem is resolved in software release 6.3(1). (CSCdu15333)
- Due to a firmware bug on the WS-X6516-GE-TX module, packets greater than 1536 bytes are dropped when a port is set to the following:
  - Trunking
  - Speed is 10 or 100
  - MTU is disabled

  This problem is resolved in software release 6.3(1). (CSCdu45812)
- For switches with Supervisor Engine 2 modules: With a 2-port channel across two uplink modules, removing one of the uplink modules causes partial traffic loss if there is a second channel on the uplink modules. This problem is resolved in software release 6.3(1). (CSCdu34191)

Open and Resolved Caveats in Software Release 6.2(3a)

These sections describe open and resolved caveats in supervisor engine software release 6.2(3a):

- Open Caveats in Software Release 6.2(3a), page 146
- Resolved Caveats in Software Release 6.2(3a), page 152

Open Caveats in Software Release 6.2(3a)

This section describes open caveats in supervisor engine software release 6.2(3a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)

- If the system boots up and both SPAN and RSPAN sessions are present, the egress SPAN test might fail for some fabric-enabled modules. Reset the fabric-enabled module to recover from the egress SPAN test failure. Note that when the system boots, a "Minor hardware problem in Module X" message displays and the **show test** *mod* command shows that the EgressSpanTest failed. (CSCdu25856)
- In a WS-C6513 slot chassis with an SFM 2 installed, do not install OSMs in slots 4, 9, or 13. (CSCdu57062)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 the PFC2, the "router_sc" field in the flows from NDE version 7 are not configurable using the **ip flow-export source** command on the MSFC2. (CSCdu10983)
- For any GBIC Gigabit port in auto-negotiation enable mode, there is a small time window for configuration changes and if the other end of the link changes the configuration word within this window, the port on this end of the link will miss the change. (CSCdu02663)
- Pinging the non-designated MSFC2/Supervisor Engine 2 across a WAN interface does not work. (CSCdu37990)
- When Autostate is enabled, a VLAN interface needs to transition to up state as soon as at least one port in the VLAN is forwarding traffic. (CSCdu05914)
- When protocol filtering is enabled, packets not destined to the MSFC may get routed. (CSCdu44627)
- Pings from a VLAN that is not configured on the MSFC to another VLAN that is configured on the MSFC fail when the configuration includes an MSFC2 and Supervisor Engine 2. (CSCdt96536)
- There is a problem with parallel TACACS+/RADIUS/KERBEROS access. Authentication protocols (TACACS+, RADIUS, Kerberos) use a global character array to store the user input (such as passwords). As the buffer is global, it is shared by all console and Telnet sessions and may contain input from multiple Telnet sessions which might cause incorrect password input for authentication.

  The following example is used for clarification.

  - User A—username test, password cisco
  - User B—username test2, password cisco

User A Telnets to the switch, types "test," presses Enter, types the password, but does not press Enter. On the other host, User B also Telnets to the switch, types "test2," presses Enter, types the wrong password and presses Enter which causes a login failure. User A goes back to the first switch and because the password is already there, User A presses Enter, but the password is treated as an incorrect password. (CSCdu35551)

- In extremely rare conditions, the Catalyst 6000 family switch might hang and not pass any traffic when a 24-MB Flash PC card (PCMCIA) is hot swapped very rapidly or when the Flash card is removed when data is being written/read to/from the Flash card. (CSCdu23412)
- Octets associated with ifInDiscard packets might not be counted. (CSCdt62359)
- If the Catalyst 6000 family switch is forwarding traffic in flow-through mode and one fabric-enabled module is already present in the system and you insert, reset, or power up a second fabric-enabled module together with a non fabric-enabled module, the switching mode changes and some diagnostics may fail for the fabric-enabled modules. Reset the fabric-enabled module to recover from this diagnostics failure. (CSCdu22799)
- The chassis temperature alarm does not return the correct status through both CLI and SNMP. (CSCds21308)
- In extremely rare conditions, all ports on the WS-X6248-RJ45 module might become unreachable with traffic forwarding stopping on all ports. The port LEDs would be orange and the **show port** command would show the ports as connected. The workaround is to reset the module using the **reset** command. (CSCds75479)
- When polling a Supervisor Engine 1A through SNMP, there must be at least a 1 millisecond delay between successive SNMP "Gets." Without a minor delay, the Catalyst 6000 family switch will output the following display message:

  ```
  2001 Mar 30 14:03:53 %IP-3-UDP_SOCKOVFL:UDP socket 1034 overflow
  ```

  This problem does not affect switch performance. (CSCdt86655)
- The **clear counters** command does not clear EtherChannel MAC counters displayed using the **show channel mac** command. (CSCdt89431)
- When an EtherChannel bundles ports across different modules, if one of the modules that contains the channeling ports gets reset, it may cause ports to leave the bridge port and to converge again while the module comes back online. (CSCdu17107)
- When the spanning tree mode is set to MISTP or MISTP-PVST+, stpxSpanningTreePathCostMode can only be set to "long." However, in software releases 6.1(x) and 6.2(1), when stpxSpanningTreePathCostMode is set to "short," there is no error and when stpxSpanningTreePathCostMode is set to "long," there is a "commitFailed" error. (CSCdu27119)
- A new MIB object, sysStatus, was added to display the operational status of the system. (CSCdu31559)
- On the Catalyst 6000 family switch, you might experience this problem with SNMP. When you configure SNMP as follows, you can then modify the configuration through snmpset:
  - snmp community read-only qwest
  - snmp community read-write qwest
  - snmp community read-write-all qwest

  When you remove the read-write and read-write-all and then run the snmpset again, you can modify the configuration even though you removed the read-write. (CSCdu38452)

- If two or more route-map entries are used for the same map that is used for policy routing on an interface, the TCAM might overflow during TCAM expansion. The TCAM "entry capacity exceeded" message displays immediately after the policy route-map statement is applied to the interface:

```
12:28:12: %FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
 12:28:12: %FM-4-RACL_REDUCED: Interface Vlan196 routed traffic will be software
switched in ingress direction(s)
```

  (CSCdu40762)

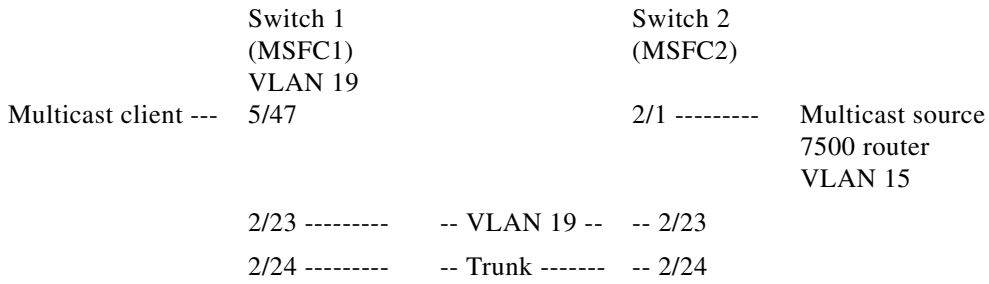
- If you attempt to set a long LCD banner (more than 800 characters) from the switch console using the **set banner lcd** command, memory corruption may be detected causing the switch to reset unexpectedly. (CSCdu45862)
- In extremely rare conditions, the FIB table on Supervisor Engine 2 may be inaccurate. If this occurs, it would be after reloading the MSFC2. The workaround is to execute the following commands in the order given on the MSFC2:
  - 1. **no ip routing**
  - 2. **ip routing**

  Note that this results in temporary traffic disruption. (CSCdu43281)
- When the NetFlow type is set to "full-vlan" or "source," the online diagnostic inline rewrite tests fail when a module is hot inserted. The "full-vlan" and "source" NetFlow types can only be triggered by the router and then cannot be set back using the **set mls flow** *flow_type* CLI command, as the router's decision has the highest priority. Online diagnostics support only the three basic netflow types: destination, destination-source, and full. With software release 6.3(1), support for "full-vlan" and "source" has been added. (CSCdu44306)
- If an OC-12 ATM Module (WS-X6101-OC12-SMF/MMF) is installed but in a disabled state and a high-availability switchover occurs, the switch might reset with a Bus Timeout NMI. The workaround is to enable the ATM module or power down the module if it is not in use. (CSCdu11713)
- Due to a firmware bug on the WS-X6516-GE-TX module, packets greater than 1536 bytes are dropped when a port is set to the following:
  - Trunking
  - Speed is 10 or 100
  - MTU is disabled

  (CSCdu45812)
- When protocol filtering is enabled, packets not destined to the router may get routed. The workaround is to disable protocol filtering. (CSCdu44627)
- For switches with Supervisor Engine 2 modules: With a 2-port channel across two uplink modules, removing one of the uplink modules causes partial traffic loss if there is a second channel on the uplink modules. (CSCdu34191)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. (CSCdu11300)
- 802.1X configuration allows incorrect command syntax. (CSCdu27021)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)

- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- Executing the following tasks in sequence leaves incorrect entries in the forwarding table:
  - 1. Enabling IGMP snooping
  - 2. Enabling protocol filtering
  - 3. Disabling IGMP snooping
  - 4. Disabling protocol filtering

  The workaround is to manually clear these entries. (CSCds69447)
- IGMP snooping and multicast MLS might not work reliably because the router ports are not selected correctly in hardware. (CSCdt31924)
- When the ifOperStatus value for the port changes (the port is enabled and disabled, or the link is brought up and down), the ifLastChange value for the port does not change. (CSCdt69418)
- When IGMP snooping is enabled and the QoS default action is set to non-zero on one of the two switches in the topology below, both MSFCs might experience high CPU utilization (99 percent). The problem does not occur if the QoS default action is set equally on both switches or if IGMP snooping is disabled.



  (CSCdt73910)
- When a Cisco IOS ACL is merged with a VACL for the same interface, and if the resulting ACL exceeds the size of the TCAM, the ACL compiler returns an error. This error is not handled properly and causes the supervisor engine to reload. (CSCdu10105)
- When an RMON event and alarm are added to a Catalyst 6000 family switch running software release 6.1(2), only the alarm will survive a reload. The workaround is to reinstall the event after a reload. (CSCdu26550)
- When using the channelized T1 port adapter with the FlexWAN module, traffic might not be dCEF switched and instead be fast switched by the MSFC2. The problem is caused by the PFC2 not setting the correct CEF entry. (CSCdu11349)
- You might not be able to enable logging for dynamic VLANs using the **set logging level dvlan** command:

```
Console> (enable) set logging level dvlan 7
 Invalid Facility
Console> (enable)
```

  (CSCdu19163)

- After an MSFC switchover, the loopback interfaces of the two MSFCs are unpingable. There are three workarounds:
  - Enter the **clear ip route** command on the designated MSFC.
  - Set the "maximum-paths" to 5 or 6.
  - Set the bandwidths of the interfaces so there is only one best path between both MSFCs. If you are using EIGRP, the variance should be one.

  (CSCdu23536)
- In extremely rare conditions, a breakpoint exception might occur when you are creating a large number of high availability events, such as adding and deleting VLANs using a script. The only workaround is to reset the switch. (CSCdt73213)
- The GVRP protocol cannot be configured on WAN module Gigabit ports. (CSCdu22779)
- In certain instances, WAN modules may not be recognized as modules that can utilize the Switch Fabric Module, so when WAN modules are installed, the switching mode may not be correct. Traffic will switch normally, but overall system throughput may be affected. Since the incorrect switching mode is observed after a WAN module is powered down, reset, or disabled, for maximum throughput it is recommended that you do not reset, power down, or disable WAN cards. (CSCdt05051)
- The Cisco IOS **show sprom** command does not work. (CSCdt75741)
- A token ring VLAN on the active supervisor engine might be translated into another VLAN on the standby supervisor engine after performing a high-availability switchover. (CSCdu08852)
- When you start a Telnet session from the Catalyst 6000 family switch and press **Ctrl-C** immediately after entering the **telnet** *ip_address* command, you stop the Telnet session but the terminal session (console or Telnet) locks. If you press **Ctrl-C** again, a new prompt appears but you still cannot enter commands. The workaround is to reset the switch. (CSCdu33233)
- The Catalyst 6000 family switch sends the wrong trap OID (.1.3.6.1.2.1.47.2.1.0.1) for the entConfigChange MIB. (CSCdu34057)
- On Supervisor Engine 2, if an ACL uses more than one TCP flag combination with different results, traffic may not be correctly access controlled after modifying the TCP flag combinations. (CSCdu38180)
- When clearing a primary VLAN (of a private VLAN) on the active supervisor engine, the VLAN might not be cleared properly on the standby supervisor engine. This may cause problems with the VLAN after a high-availability switchover. (CSCdu31513)
- Under very rare circumstances, the WS-X6248 10/100BASE-T modules could get into a fatal state that is beyond recovery by the built-in software recovery mechanisms. If this occurs, the only way to recover from this error condition is to completely reset the module or power the module off and then on. The **set lcperroraction** command has been modified and enhanced to react automatically upon detection of this fatal error condition. The LCPERRORACTION can be set to one of the following three levels:
  - LCPERRORACTION ignore: This is the default level. Errors are logged. No action is taken.
  - LCPERRORACTION operator: Errors are logged. In addition, the system prints a message requesting that you manually power the module off and then on.
  - LCPERRORACTION system: Errors are logged. The system automatically powers the module off and then on. (CSCdu15333)

Resolved Caveats in Software Release 6.2(3a)

This section describes resolved caveats in supervisor engine software release 6.2(3a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.2(3a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.2(3)

These sections describe open and resolved caveats in supervisor engine software release 6.2(3):

- Open Caveats in Software Release 6.2(3), page 152
- Resolved Caveats in Software Release 6.2(3), page 157

Open Caveats in Software Release 6.2(3)

This section describes open caveats in supervisor engine software release 6.2(3):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- If the system boots up and both SPAN and RSPAN sessions are present, the egress SPAN test might fail for some fabric-enabled modules. Reset the fabric-enabled module to recover from the egress SPAN test failure. Note that when the system boots, a "Minor hardware problem in Module X" message displays and the **show test** *mod* command shows that the EgressSpanTest failed. (CSCdu25856)
- In a WS-C6513 slot chassis with an SFM 2 installed, do not install OSMs in slots 4, 9, or 13. (CSCdu57062)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 the PFC2, the "router_sc" field in the flows from NDE version 7 are not configurable using the **ip flow-export source** command on the MSFC2. (CSCdu10983)
- For any GBIC Gigabit port in auto-negotiation enable mode, there is a small time window for configuration changes and if the other end of the link changes the configuration word within this window, the port on this end of the link will miss the change. (CSCdu02663)
- Pinging the non-designated MSFC2/Supervisor Engine 2 across a WAN interface does not work. (CSCdu37990)
- When Autostate is enabled, a VLAN interface needs to transition to up state as soon as at least one port in the VLAN is forwarding traffic. (CSCdu05914)
- When protocol filtering is enabled, packets not destined to the MSFC may get routed. (CSCdu44627)
- Pings from a VLAN that is not configured on the MSFC to another VLAN that is configured on the MSFC fail when the configuration includes an MSFC2 and Supervisor Engine 2. (CSCdt96536)
- There is a problem with parallel TACACS+/RADIUS/KERBEROS access. Authentication protocols (TACACS+, RADIUS, Kerberos) use a global character array to store the user input (such as passwords). As the buffer is global, it is shared by all console and Telnet sessions and may contain input from multiple Telnet sessions which might cause incorrect password input for authentication.

  The following example is used for clarification.

  - User A—username test, password cisco
  - User B—username test2, password cisco

  User A Telnets to the switch, types "test," presses Enter, types the password, but does not press Enter. On the other host, User B also Telnets to the switch, types "test2," presses Enter, types the wrong password and presses Enter which causes a login failure. User A goes back to the first switch and because the password is already there, User A presses Enter, but the password is treated as an incorrect password. (CSCdu35551)
- In extremely rare conditions, the Catalyst 6000 family switch might hang and not pass any traffic when a 24-MB Flash PC card (PCMCIA) is hot swapped very rapidly or when the Flash card is removed when data is being written/read to/from the Flash card. (CSCdu23412)
- Octets associated with ifInDiscard packets might not be counted. (CSCdt62359)
- If the Catalyst 6000 family switch is forwarding traffic in flow-through mode and one fabric-enabled module is already present in the system and you insert, reset, or power up a second fabric-enabled module together with a non fabric-enabled module, the switching mode changes and some diagnostics may fail for the fabric-enabled modules. Reset the fabric-enabled module to recover from this diagnostics failure. (CSCdu22799)
- The chassis temperature alarm does not return the correct status through both CLI and SNMP. (CSCds21308)

- In extremely rare conditions, all ports on the WS-X6248-RJ45 module might become unreachable with traffic forwarding stopping on all ports. The port LEDs would be orange and the **show port** command would show the ports as connected. The workaround is to reset the module using the **reset** command. (CSCds75479)
- When polling a Supervisor Engine 1A through SNMP, there must be at least a 1 millisecond delay between successive SNMP "Gets." Without a minor delay, the Catalyst 6000 family switch will output the following display message:

  ```
  2001 Mar 30 14:03:53 %IP-3-UDP_SOCKOVFL:UDP socket 1034 overflow
  ```

  This problem does not affect switch performance. (CSCdt86655)
- The **clear counters** command does not clear EtherChannel MAC counters displayed using the **show channel mac** command. (CSCdt89431)
- When an EtherChannel bundles ports across different modules, if one of the modules that contains the channeling ports gets reset, it may cause ports to leave the bridge port and to converge again while the module comes back online. (CSCdu17107)
- When the spanning tree mode is set to MISTP or MISTP-PVST+, stpxSpanningTreePathCostMode can only be set to "long." However, in software releases 6.1(x) and 6.2(1), when stpxSpanningTreePathCostMode is set to "short," there is no error and when stpxSpanningTreePathCostMode is set to "long," there is a "commitFailed" error. (CSCdu27119)
- A new MIB object, sysStatus, was added to display the operational status of the system. (CSCdu31559)
- On the Catalyst 6000 family switch, you might experience this problem with SNMP. When you configure SNMP as follows, you can then modify the configuration through snmpset:
  - snmp community read-only qwest
  - snmp community read-write qwest
  - snmp community read-write-all qwest

  When you remove the read-write and read-write-all and then run the snmpset again, you can modify the configuration even though you removed the read-write. (CSCdu38452)
- If two or more route-map entries are used for the same map that is used for policy routing on an interface, the TCAM might overflow during TCAM expansion. The TCAM "entry capacity exceeded" message displays immediately after the policy route-map statement is applied to the interface:

  ```
  12:28:12: %FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
   12:28:12: %FM-4-RACL_REDUCED: Interface Vlan196 routed traffic will be software
  switched in ingress direction(s)
  ```

  (CSCdu40762)
- If you attempt to set a long LCD banner (more than 800 characters) from the switch console using the **set banner lcd** command, memory corruption may be detected causing the switch to reset unexpectedly. (CSCdu45862)
- In extremely rare conditions, the FIB table on Supervisor Engine 2 may be inaccurate. If this occurs, it would be after reloading the MSFC2. The workaround is to execute the following commands in the order given on the MSFC2:
  - 1. **no ip routing**
  - 2. **ip routing**

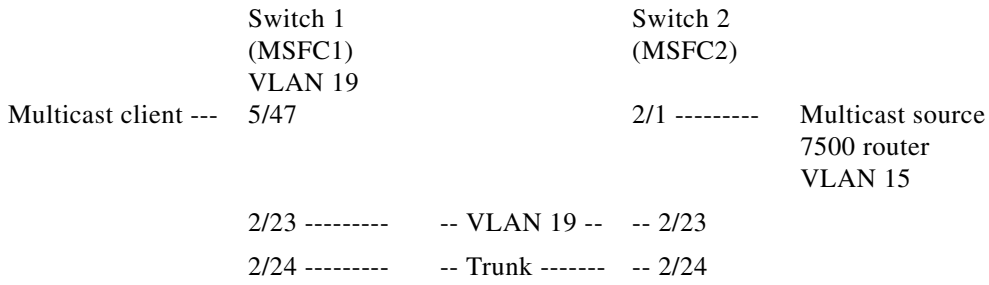
  Note that this results in temporary traffic disruption. (CSCdu43281)

- When the NetFlow type is set to “full-vlan” or “source,” the online diagnostic inline rewrite tests fail when a module is hot inserted. The “full-vlan” and “source” NetFlow types can only be triggered by the router and then cannot be set back using the **set mls flow** *flow_type* CLI command, as the router's decision has the highest priority. Online diagnostics support only the three basic netflow types: destination, destination-source, and full. With software release 6.3(1), support for “full-vlan” and “source” has been added. (CSCdu44306)
- If an OC-12 ATM Module (WS-X6101-OC12-SMF/MMF) is installed but in a disabled state and a high-availability switchover occurs, the switch might reset with a Bus Timeout NMI. The workaround is to enable the ATM module or power down the module if it is not in use. (CSCdu11713)
- Due to a firmware bug on the WS-X6516-GE-TX module, packets greater than 1536 bytes are dropped when a port is set to the following:
  - Trunking
  - Speed is 10 or 100
  - MTU is disabled

  (CSCdu45812)
- When protocol filtering is enabled, packets not destined to the router may get routed. The workaround is to disable protocol filtering. (CSCdu44627)
- For switches with Supervisor Engine 2 modules: With a 2-port channel across two uplink modules, removing one of the uplink modules causes partial traffic loss if there is a second channel on the uplink modules. (CSCdu34191)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. (CSCdu11300)
- 802.1X configuration allows incorrect command syntax. (CSCdu27021)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a “%FM-2-TCAM_ERROR:TCAM programming error 5” message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- Executing the following tasks in sequence leaves incorrect entries in the forwarding table:
  - 1. Enabling IGMP snooping
  - 2. Enabling protocol filtering
  - 3. Disabling IGMP snooping
  - 4. Disabling protocol filtering

  The workaround is to manually clear these entries. (CSCds69447)
- IGMP snooping and multicast MLS might not work reliably because the router ports are not selected correctly in hardware. (CSCdt31924)
- When the ifOperStatus value for the port changes (the port is enabled and disabled, or the link is brought up and down), the ifLastChange value for the port does not change. (CSCdt69418)

- When IGMP snooping is enabled and the QoS default action is set to non-zero on one of the two switches in the topology below, both MSFCs might experience high CPU utilization (99 percent). The problem does not occur if the QoS default action is set equally on both switches or if IGMP snooping is disabled.



  (CSCdt73910)

- When a Cisco IOS ACL is merged with a VACL for the same interface, and if the resulting ACL exceeds the size of the TCAM, the ACL compiler returns an error. This error is not handled properly and causes the supervisor engine to reload. (CSCdu10105)
- When an RMON event and alarm are added to a Catalyst 6000 family switch running software release 6.1(2), only the alarm will survive a reload. The workaround is to reinstall the event after a reload. (CSCdu26550)
- When using the channelized T1 port adapter with the FlexWAN module, traffic might not be dCEF switched and instead be fast switched by the MSFC2. The problem is caused by the PFC2 not setting the correct CEF entry. (CSCdu11349)
- You might not be able to enable logging for dynamic VLANs using the **set logging level dvlan** command:

```
Console> (enable) set logging level dvlan 7
 Invalid Facility
Console> (enable)
```

  (CSCdu19163)

- After an MSFC switchover, the loopback interfaces of the two MSFCs are unpingable. There are three workarounds:
  - Enter the **clear ip route** command on the designated MSFC.
  - Set the “maximum-paths” to 5 or 6.
  - Set the bandwidths of the interfaces so there is only one best path between both MSFCs. If you are using EIGRP, the variance should be one.

  (CSCdu23536)

- In extremely rare conditions, a breakpoint exception might occur when you are creating a large number of high availability events, such as adding and deleting VLANs using a script. The only workaround is to reset the switch. (CSCdt73213)
- The GVRP protocol cannot be configured on WAN module Gigabit ports. (CSCdu22779)

- In certain instances, WAN modules may not be recognized as modules that can utilize the Switch Fabric Module, so when WAN modules are installed, the switching mode may not be correct. Traffic will switch normally, but overall system throughput may be affected. Since the incorrect switching mode is observed after a WAN module is powered down, reset, or disabled, for maximum throughput it is recommended that you do not reset, power down, or disable WAN cards. (CSCdt05051)
- The Cisco IOS **show sprom** command does not work. (CSCdt75741)
- A token ring VLAN on the active supervisor engine might be translated into another VLAN on the standby supervisor engine after performing a high-availability switchover. (CSCdu08852)
- When you start a Telnet session from the Catalyst 6000 family switch and press **Ctrl-C** immediately after entering the **telnet** *ip_address* command, you stop the Telnet session but the terminal session (console or Telnet) locks. If you press **Ctrl-C** again, a new prompt appears but you still cannot enter commands. The workaround is to reset the switch. (CSCdu33233)
- The Catalyst 6000 family switch sends the wrong trap OID (.1.3.6.1.2.1.47.2.1.0.1) for the entConfigChange MIB. (CSCdu34057)
- On Supervisor Engine 2, if an ACL uses more than one TCP flag combination with different results, traffic may not be correctly access controlled after modifying the TCP flag combinations. (CSCdu38180)
- When clearing a primary VLAN (of a private VLAN) on the active supervisor engine, the VLAN might not be cleared properly on the standby supervisor engine. This may cause problems with the VLAN after a high-availability switchover. (CSCdu31513)
- Under very rare circumstances, the WS-X6248 10/100BASE-T modules could get into a fatal state that is beyond recovery by the built-in software recovery mechanisms. If this occurs, the only way to recover from this error condition is to completely reset the module or power the module off and then on. The **set lcperroraction** command has been modified and enhanced to react automatically upon detection of this fatal error condition. The LCPERRORACTION can be set to one of the following three levels:
  - LCPERRORACTION ignore: This is the default level. Errors are logged. No action is taken.
  - LCPERRORACTION operator: Errors are logged. In addition, the system prints a message requesting that you manually power the module off and then on.
  - LCPERRORACTION system: Errors are logged. The system automatically powers the module off and then on. (CSCdu15333)

Resolved Caveats in Software Release 6.2(3)

This section describes resolved caveats in supervisor engine software release 6.2(3):

- A (*,G) entry, installed as a complete shortcut, changes to a partial shortcut entry when the OIF changes to NULL. When the OIF is reinstalled, the (*,G) entry does not return to a complete shortcut but remains a partial shortcut. If traffic for this group is sent at a high rate, high CPU utilization may be observed on the MSFC. This problem is resolved in software release 6.2(3). (CSCdu30097)
- The OIF of an active (S,G) flow may change to NULL temporarily and then return to the correct OIF state. When this happens, multicast traffic on that flow is temporarily black-holed while OIF is NULL. This problem is resolved in software release 6.2(3). (CSCdu35684)
- The broadcast, multicast, and unicast suppression feature does not work on WS-X6K-SUP2-2GE and WS-X6516-GBIC modules. This problem is resolved in software release 6.2(3). (CSCdu58909)

- When you reload an MSFC2 from the MSFC2 prompt during heavy traffic, VLAN interfaces may not come up. Symptoms include the IBC interface going down and loopback diagnostics failing for the MSFC2 from the switch side. This problem is resolved in software release 6.2(3). (CSCdu32703)
- With the Catalyst 6000 CiscoView (CV) images, if you use the QoS Device Management, deleting an entry from the Policy Selection might fail. The workaround is to reboot the switch. This problem is resolved in software release 6.2(3). (CSCdu11515)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to configure WRR, the WRR Weight column is not supported for some port types. This problem is resolved in software release 6.2(3). (CSCdu11460)

Open and Resolved Caveats in Software Release 6.2(2a)

These sections describe open and resolved caveats in supervisor engine software release 6.2(2a):

- Open Caveats in Software Release 6.2(2a), page 158
- Resolved Caveats in Software Release 6.2(2a), page 159

Open Caveats in Software Release 6.2(2a)

This section describes open caveats in supervisor engine software release 6.2(2a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- With the Catalyst 6000 CiscoView (CV) images, if you use the QoS Device Management, deleting an entry from the Policy Selection might fail.

  Workaround: Reboot the switch. (CSCdu11515)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to configure WRR, the WRR Weight column is not supported for some port types. (CSCdu11460)
- If the Catalyst 6000 family switch is forwarding traffic in flow-through mode and one fabric-enabled module is already present in the system and you insert, reset, or power up a second fabric-enabled module together with a non fabric-enabled module, the switching mode changes and some diagnostics may fail for the fabric-enabled modules. Reset the fabric-enabled module to recover from this diagnostics failure. (CSCdu22799)

- If the system boots up and both SPAN and RSPAN sessions are present, the egress SPAN test might fail for some fabric-enabled modules. Reset the fabric-enabled module to recover from the egress SPAN test failure. Note that when the system boots, a "Minor hardware problem in Module X" message displays and the **show test** *mod* command shows that the EgressSpanTest failed. (CSCdu25856)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. (CSCdu11300)
- 802.1X configuration allows incorrect command syntax. (CSCdu27021)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)
- In a system with a Switch Fabric Module installed, the ACL capture feature does not work unless one of the following conditions are met:
  - Traffic is captured and exits on a nonfabric-enabled module port.

  or
  - Traffic is captured and exits on the same fabric-enabled module.

  The WS-X6380 and WS-X6381 modules will not see traffic sent to fabric-enabled modules in the system if the switch is operating in truncated mode. (CSCdu31887)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.2(2a)

This section describes resolved caveats in supervisor engine software release 6.2(2a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.2(2a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.2(2)

These sections describe open and resolved caveats in supervisor engine software release 6.2(2):

Open Caveats in Software Release 6.2(2)

This section describes open caveats in supervisor engine software release 6.2(2):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- With the Catalyst 6000 CiscoView (CV) images, if you use the QoS Device Management, deleting an entry from the Policy Selection might fail.

  Workaround: Reboot the switch. (CSCdu11515)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to configure WRR, the WRR Weight column is not supported for some port types. (CSCdu11460)
- If the Catalyst 6000 family switch is forwarding traffic in flow-through mode and one fabric-enabled module is already present in the system and you insert, reset, or power up a second fabric-enabled module together with a non fabric-enabled module, the switching mode changes and some diagnostics may fail for the fabric-enabled modules. Reset the fabric-enabled module to recover from this diagnostics failure. (CSCdu22799)
- If the system boots up and both SPAN and RSPAN sessions are present, the egress SPAN test might fail for some fabric-enabled modules. Reset the fabric-enabled module to recover from the egress SPAN test failure. Note that when the system boots, a "Minor hardware problem in Module X" message displays and the **show test** *mod* command shows that the EgressSpanTest failed. (CSCdu25856)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. (CSCdu11300)
- 802.1X configuration allows incorrect command syntax. (CSCdu27021)
- You cannot enable WCCP Layer 2 redirection and Cisco IOS Firewall at the same time on switches with Supervisor Engine 2 running supervisor engine software release 6.2(2) and Cisco IOS Release 12.1(6)E1 through 12.1(7a)E1. The features work independently. This problem is resolved in Cisco IOS Release 12.1(8a)E. (CSCdu25221)

- In a system with a Switch Fabric Module installed, the ACL capture feature does not work unless one of the following conditions are met:
  - Traffic is captured and exits on a nonfabric-enabled module port.

  or

  - Traffic is captured and exits on the same fabric-enabled module.

  The WS-X6380 and WS-X6381 modules will not see traffic sent to fabric-enabled modules in the system if the switch is operating in truncated mode. (CSCdu31887)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.2(2)

This section describes resolved caveats in supervisor engine software release 6.2(2):

- If the CV image cannot be launched on Solaris and Netscape clients, or if launching the CV image generates an Access Control Error, clear the browser cache or make sure the Plug-In and JRE versions match.

  To change the JRE version to match with the Plug-In, open the Java Plug-In Control Panel at JAVA_PLUGIN_INSTALL_DIRECTORY/j2pi/ControlPanel (the standard Java Plug-In installation directory is /opt/NSCPcom/), select the **Advanced** tab, then the **Java Run Time Environment** option, and specify "Use Java Plug-in Default." This problem is resolved in software release 6.(2)2. (CSCdu32540)
- Opening configuration dialogs after resizing the CiscoView browser window on a Solaris/Netscape Communicator client with Java plug-in 1.3.0 causes a Java IllegalComponentStateException error. The workaround is to open the same dialog again. This problem is resolved in software release 6.(2)2. (CSCdu32555)
- If you initiate a Console or Telnet session to a Catalyst 6000 family switch and then cancel the connection attempt using the **Cntrl-C** command before the connection is established, a 16-byte memory leak occurs. This problem is resolved in software release 6.(2)2. (CSCdu29283)

- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the user bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the nontrunk port. The forwarded packets do not go through blocked ports. This problem is resolved in software release 6.2(2). (CSCdu10858)
- Internal states are not cleaned up properly when an MFD Install fails from one of the RPs in a dual router scenario. This problem is resolved in software release 6.2(2). (CSCdu05988)
- Multicast packets switched from WS-X6516-GBIC module to a nonfabric-enabled module are replicated twice. This situation causes twice the amount of output packets to be reported. This problem is resolved in software release 6.2(2). (CSCdt91046)
- After repeatedly removing and then reapplying large Cisco IOS ACLs, the MSFC2 is unable to program the PFC again with the ACL information. The MSFC returns the following messages from the feature manager:

  %ACL-3-TCAMFULL:Acl engine TCAM table is full

  %ACL-3-RACLMAPCOMMITFAIL:Failed to map Router ACL to VLAN 2

  %FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded

  %FM-4-RACL_REDUCED: Interface Vlan2 routed traffic will be software switched in egress direction(s)

  After resetting the MSFC, the entire ACL table gets compiled and downloaded successfully but after removing and then reapplying, it fails to get compiled. This problem is resolved in software release 6.2(2). (CSCdu08689)
- Community string indexing is broken in software release 6.1(3) for indices 0 and 4096. When polling these indices with ro_community@0 or ro_community@4096, the switch times out and does not respond. This situation has the side effect of causing User Tracking to discover only end stations in VLAN 1 on the affected switches. This problem is resolved in software release 6.2(2). (CSCdu18790)
- Multicast MLS traffic does not flow across a FlexWAN serial interface configured for frame-relay unless a well-known multicast DCLI is configured on the router (through the **frame-relay multicast-dlci** interface configuration command) or is configured on the switch and signalled through LMI. This problem is resolved in software release 6.2(2). (CSCds71312)
- If you make many port configuration changes when a FlexWAN is present in a chassis with fabric-enabled modules, a depletion of memory resources could occur. This problem is resolved in software release 6.2(2). (CSCdt32508)
- Multiple Cisco IOS software and Catalyst software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices. To remove the vulnerabilities, Cisco is offering free software upgrades for all affected platforms. The defects are documented in DDTS records CSCds32217, CSCds16384, CSCds19674, CSCdr59314, CSCdr61016, and CSCds49183. In addition to specific workarounds for each vulnerability, affected systems can be protected by preventing SNMP access.

  This notice will be posted at

  http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml.(CSCds19674)
- The value of dot1dTpPortInDiscards object contains same value of object ifInDiscards for a bridge port. This problem is resolved in software release 6.2(2). (CSCdt71890)
- Routers connected through ATM/WAN links might not be recognized as PIM neighbors by the switch. This problem is resolved in software release 6.2(2). (CSCdt66502)

- If you clear a spanning tree misconfiguration on the non-root side, the hello timer does not restart on the root switch. This problem is resolved in software release 6.2(2). (CSCdu08407)
- cseL3ActiveFlows may report high (spurious) values when NDE is enabled and disabled. This problem is resolved in software release 6.2(2). (CSCdt77457)

Open and Resolved Caveats in Software Release 6.1(4b)

These sections describe open and resolved caveats in supervisor engine software release 6.1(4b):

- Open Caveats in Software Release 6.1(4b), page 163
- Resolved Caveats in Software Release 6.1(4b), page 164

Open Caveats in Software Release 6.1(4b)

This section describes open caveats in supervisor engine software release 6.1(4b):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the nontrunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)

- 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 6.1(4b)

This section describes resolved caveats in supervisor engine software release 6.1(4b):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.1(4b). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.1(4)

These sections describe open and resolved caveats in supervisor engine software release 6.1(4):

- Open Caveats in Software Release 6.1(4), page 164
- Resolved Caveats in Software Release 6.1(4), page 165

Open Caveats in Software Release 6.1(4)

This section describes open caveats in supervisor engine software release 6.1(4):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)

- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the nontrunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.1(4)

This section describes resolved caveats in supervisor engine software release 6.1(4):

- IP packets with a multicast source address to a unicast destination may not be dropped by hardware switching on the PFC2 when unicast reverse path forwarding is enabled. This problem is resolved in software release 6.1(4). (CSCdu04848)
- Under certain circumstances the IPX packets forwarded by the PFC2 have source MAC addresses of all zeros for the directly connected networks. This is seen with the Rconsole application and NCP packets. A reboot or reset of the MSFC2 could be one cause of the problem. The only workaround is to issue the **clear ipx route** command or disable ipx mls (**no mls ipx**) which disables CEF on the Supervisor Engine 2. This problem is resolved in software release 6.1(4). (CSCdu05814)
- The MSFC2 with ROMMON 6.1(3.1) and software release 6.1(3) might show an invalid version number in the **show module** and **show version** command displays. This problem is resolved in software release 6.1(4). (CSCdu16735)
- In a system with a Supervisor Engine 2 and PFC2 (no MSFC2) policing of multicast traffic might fail; unicast traffic is policed correctly. This problem is resolved in software release 6.1(4). (CSCdt95267)

Open and Resolved Caveats in Software Release 6.1(3a)

These sections describe open and resolved caveats in supervisor engine software release 6.1(3a):

- Open Caveats in Software Release 6.1(3a), page 166
- Resolved Caveats in Software Release 6.1(3a), page 166

Open Caveats in Software Release 6.1(3a)

This section describes open caveats in supervisor engine software release 6.1(3a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.1(3a)

This section describes resolved caveats in supervisor engine software release 6.1(3a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.1(3a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.1(3)

These sections describe open and resolved caveats in supervisor engine software release 6.1(3):

Open Caveats in Software Release 6.1(3)

This section describes open caveats in supervisor engine software release 6.1(3):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- 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 6.1(3)

This section describes resolved caveats in supervisor engine software release 6.1(3):

- VLAN 2035 cannot be used as an auxiliary VLAN due to an incorrect LTL index mapping. This problem is resolved in software release 6.1(3). (CSCds64624)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(4)E2 are reset every 9 minutes by the Supervisor Engine 2. This problem is resolved in Cisco IOS Releases 12.1(5a)E3 and later. (CSCdt02646)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(5a)E3 do not support high availability for Supervisor Engine 2. This problem is resolved in Cisco IOS Releases 12.1(6)E and later. (CSCdt29354)
- If you configure large Cisco IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same Cisco IOS ACL and share the same label before might not be able to do so any more. As a result the Cisco IOS ACLs are duplicated and might not fit into TCAM. The workaround is to disable and reenable the interface. This problem is resolved in software release 6.1(3). (CSCds66134)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. This problem is resolved in software release 6.1(3). (CSCds37139)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- A switch configured as an NTP client reports an incorrect summertime value. The reported end time is advanced by one year in the **show ntp** and **show summertime** command displays. This problem is resolved in software release 6.1(3). (CSCdt43350)
- After a system reset, the following message might display: “RMON Alarm Timer exit: malloc scp queue buffers failed.” The message might display even though there is still sufficient memory. This problem is resolved in software release 6.1(3). (CSCdt58390)
- In the following situation with IGMP snooping enabled, the switch might lock up with no obvious indication such as a stack dump.

External router ---------- Switch A ---------- Switch B ---------- Multicast receiver

  If the multicast receiver sends an IGMPv2 leave for a multicast group, the IGMPv2 leave is forwarded to the external router which responds with a group-specific query. Switch A then forwards this query to Switch B, which starts to build a “MAC-based” general query to determine if any additional receivers are connected. In the course of building this query, Switch B might lock up. The workaround is to disable IGMP snooping. This problem is resolved in software release 6.1(3). (CSCdt71689)
- In a redundant system with high availability enabled, if you clear a large number of VLANs (4000), it might take 20 to 30 minutes for the configuration to be synchronized to the standby supervisor engine. This problem is resolved in software release 6.1(3). (CSCds15572)

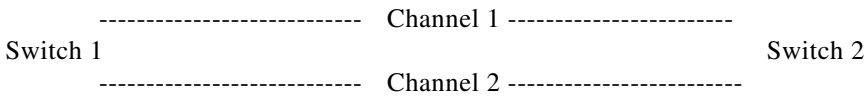
- Under some circumstances, when the first host report in response to a general IGMP query is sent at about the general query expiration time (10 seconds), the switch might fail to pass the next report on to the router. If this problem occurs three consecutive times, the router might stop forwarding traffic to this interface. Since hosts choose a random time (up to 10 seconds normally) to delay sending a report each time they receive a query, it is very unlikely that this will occur three consecutive times. As more receivers are added to a segment, the probability is reduced even more. This problem is resolved in software release 6.1(3). (CSCds36757)
- When the RGMP feature is not enabled on the switch and you enter the **show rgmp group** command, the supervisor engine might reset. This problem is resolved in software release 6.1(3). (CSCds44030)
- When two or more multicast clients attempt to join the same multicast address group at the same time (within 10 seconds of each other), all clients, except the first, fail to join the group. If a client on a CGMP-enabled switch attempts to join a multicast group within 10 seconds of the first client, the join request never arrives at the multicast router, no CGMP message comes back from the multicast router, and the client fails to join the multicast group. This problem is resolved in software release 6.1(3). (CSCds84004)
- The link LED on the WS-X6316 module stays on after the cable is disconnected. This problem is resolved in software release 6.1(3). (CSCds89169)
- The default content and length of the NTP authentication fields in the NTP client request packet changed between software releases 4.x and 5.x, causing problems with time servers. This problem is resolved in software release 6.1(3). (CSCds90575)
- The switch does not accept TACACS+ authorization replies from the CiscoSecure server. This problem is resolved in software release 6.1(3). (CSCds92279)
- When you use too many range operators in ACLs, there might be a failure in installing or in some cases reinstalling the ACL because of insufficient layer 4 operations. This problem might occur even though there is sufficient TCAM space. The problem is due not to a failure of the expansion itself, since the ranges can be easily expanded into a few ACLs. This problem is resolved in software release 6.1(3). (CSCdt03840)
- The 64-bit counters for IfOutOctets jump to twice the actual value when the 32-bit counters roll over to zero, having approached their maximum value of 4,294,967,295. This problem causes erroneous readings when counter data is displayed. There is no workaround. This problem is resolved in software release 6.1(3). (CSCdt12257)
- The CLI allows private VLANs to be set to a non-Ethernet type which is an invalid configuration. Changing the VLAN type for private VLANs has been restricted to allow only Ethernet. This problem is resolved in software release 6.1(3). (CSCdt15295)
- If you disable spanning tree on a switch that has a redundant EtherChannel configuration, spanning tree on a neighboring switch will not converge and spanning tree loops might occur. This problem is resolved in software release 6.1(3). (CSCdt18726)
- The switch might reset if you create a conceptual row with index 0.0.0.0 in the vmVmpsTable. This problem is resolved in software release 6.1(3). (CSCdt25320)
- If you have already customized the switch console prompt using the **set prompt** command, the switch might reload after entering the **set system name** command with a name longer than 64 characters. This problem is resolved in software release 6.1(3). (CSCdt26711)
- In a Supervisor Engine 1 system, when you apply a reflexive ACL to a VLAN interface on the MSFC or MSFC2 and the reflexive ACL timeout value is set too low, or there are a lot of reflexive ACEs causing frequent additions and deletions of entries, intermittent traffic loss might occur on the interface. This problem is resolved in software release 6.1(3). (CSCdt26889)

- In a Supervisor Engine 2 system running 6.1(1d), you might see high CPU utilization (100 percent) when NDE is used in a heavy traffic setting. This problem is resolved in software release 6.1(3). Note that NDE is a CPU intensive task and does utilize the CPU when a high number of flows need to be aged out. (CSCdt30476)
- After a non-high-availability switchover, Layer 3 multicast traffic might get blocked as it transits the internal VLANs if the MSFC missed configuring the default ACL for the internal VLANs. The workaround is to reload the designated MSFC. This problem is resolved in software release 6.1(3). (CSCdt21295)
- SNMP MIB objects dot1dStpBridgeMaxAge, dot1dStpBridgeHelloTime, and dot1dStpBridgeForwardDelay do not return correct values when the spanning tree mode is set to either MISTP or MISTP-PVST+. This problem is resolved in software release 6.1(3). (CSCdt32156)
- When you set the RMON historyControlInterval to a small number such as 1 or 2 seconds, the system might reload. The workaround is to increase the historyControlInterval value. This problem is resolved in software release 6.1(3). (CSCdt51180)
- The switch might reset if you attempt to delete a nonexistent VLAN through the SNMP vtpVlanEditTable. This problem is resolved in software release 6.1(3). (CSCdt38160)
- The **show ip permit** command might cause the switch to reset. The workaround is to disable DNS on the switch. This problem is resolved in software release 6.1(3). (CSCdt55237)
- If the VLAN mapping to an MISTP instance is done in PVST+ mode followed by the spanning tree mode being set to MISTP, a switchover might cause the VLAN mapping for VLANs in the range of 1025 to 4094 to be lost. This problem is resolved in software release 6.1(3). (CSCdt56754)
- Every time a port toggles, the following SNMP message might display:

  ```
  %SNMP-5-NEWROOTTRAP:New Root Trap for Vlan[1]
  ```

  This problem is resolved in software release 6.1(3). (CSCdt59597)
- Fallback of an UplinkFast port configured as part of an EtherChannel causes a 5- to 10-second connectivity drop. This problem is resolved in software release 6.1(3). (CSCdt60420)
- With protocol filtering enabled, IP packets including OSPF and multicast packets might get blocked when egressing the WAN interfaces. The workaround is to disable protocol filtering. This problem is resolved in software release 6.1(3). (CSCds46969)
- If you have an MSFC2 running 12.1.5b(E7) and use EIGRP as the routing protocol, there might be packet loss when using the default network for the return path of the packets. There is no packet loss when using a default route instead of the default network. This problem is resolved in software release 6.1(3). Note that the MSFC2 must be running 12.1(6)E1 or later. (CSCdt65160)
- The switch might reset with a TLB exception if the forward slash (/) character is inadvertently used. For example, if you enter **show mls statistics entry ip destination /** using the forward slash character instead of a question mark (?), the switch might reload. This problem is resolved in software release 6.1(3). (CSCdt73779)
- On a switch with redundant Supervisor Engine 2s, PFC2s, and MSFC2s when the HSRP active MSFC2 switches from one MSFC2 to the other, the corresponding FIB entry (on the NMP) for the virtual IP address could be changed from “RECEIVE” to “RESOLVED” or could get deleted from the NMP’s FIB table. This problem is resolved in software release 6.1(3). Note that the MSFC2 must be running 12.1(7)E or later. (CSCdt29644)

- In a few MISTP configurations, when the switch does not have the local mapping and only one VLAN is mapped to an instance, if the mapping is modified on the root side, the VLAN is not removed from the previous instance. The VLAN mapping transmitted in the BPDUs is still correct, but the **show spantree mistp** *instance* command displays the VLAN in two instances. This problem is resolved in software release 6.1(3). (CSCdt65307)
- There might be problems with SNMP access for the ATM module in systems with Supervisor Engine 2 (WS-X6K-SUP2-2GE). This problem is resolved in software release 6.1(3). (CSCdt47870)
- The switch might reset with a TLB exception when you are restoring the configuration from a configuration file during system boot up or right after system boot up. This problem is resolved in software release 6.1(3). (CSCdt76499)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. This problem is resolved in software release 6.1(3). (CSCdr61398)
- This problem can happen in the following scenario:



  Switch 1 is the root for VLANs 1 through 10 (the same case applies to MISTP) and it has root guard enabled on the link connected to Switch 2. Upon making Switch 2 the root for VLAN 5 (or any VLAN from 1 through 10 in this example), Switch 1 moves its ports to a root-inconsistent state (because it receives BPDUs from Switch 2) and, after some time, the channel ports go to error disable on the Switch 2 side (a spanning tree loop is detected between Switch 1 and Switch 2). The workaround is as follows: If root guard is enabled on a switch, make sure *that* switch is the root switch for the specific topology. This problem is resolved in software release 6.1(3). (CSCdt89020)
- When BPDUs are received on a WAN port that is connected to another switch through a dot1q trunk, the received BPDUs are processed by the supervisor engine which results in the following syslog messages being displayed:

  ```
  %SPANTREE-2-RX_1QNON1QTRUNK: Rcved 1Q-BPDU on non-1Q-trunk port 9/50 vlan 1038
  ```

  The BPDUs should be going to the MSFC, not the supervisor engine. This problem is resolved in software release 6.1(3). (CSCds68998)
- In extremely rare conditions, a breakpoint exception might occur when MMLS has to install a lot of multicast flows. It might happen when Layer 2 entry creation fails or ltl-index allocation fails. It is due to faulty error-case handling. The only workaround is to disable MMLS. This problem is resolved in software release 6.1(3). (CSCdt23910)
- The switch might reset with a TLB exception when CmpOctetStringWithLen() receives a null pointer. This problem is resolved in software release 6.1(3). (CSCdt75849)

Open and Resolved Caveats in Software Release 6.1(2a)

These sections describe open and resolved caveats in supervisor engine software release 6.1(2a):

Open Caveats in Software Release 6.1(2a)

This section describes open caveats in supervisor engine software release 6.1(2a):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- VLAN 2035 cannot be used for a voice VLAN due to an incorrect LTL index mapping. (CSCds64624)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(4)E2 are reset every 9 minutes by the Supervisor Engine 2. (CSCdt02646)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(5a)E3 do not support HA for Supervisor Engine 2. (CSCdt29354)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- The OAM-PVC management feature does not work in a back-to-back configuration. The PVC comes up and passes traffic until you configure the OAM management feature. After you configure the feature, the PVC goes down. When the PVC is down, entering the **show atm vc** command shows that the OAM cells on one of the devices is not receiving OAM cells. If you enter the **shut** command and then the no **shut** command, the main ATM interfaces become active. If you perform a cold boot on the switch, the PVC does not become active again until you enter the **shut** and **no shut** commands on the main interfaces on both devices at the same time or remove the OAM management feature. The workaround is not to configure OAM management. (CSCdt04481)

Note This problem has not been seen in later releases.

- If you configure large Cisco IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same Cisco IOS ACL and share the same label before might not be able to do so any more. As a result the Cisco IOS ACLs are duplicated and might not fit into TCAM. The workaround is to disable and reenable the interface. (CSCds66134)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. You need to shorten the rise and fall times, although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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. The rewrite that is generated for multicast is a Layer 3 rewrite so 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). For the packets that are bridged in the same incoming VLAN, no ToS rewrite occurs. (CSCdm72364)

Resolved Caveats in Software Release 6.1(2a)

This section describes resolved caveats in supervisor engine software release 6.1(2a):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.1(2a). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.1(2)

These sections describe open and resolved caveats in supervisor engine software release 6.1(2):

- Open Caveats in Software Release 6.1(2), page 174
- Resolved Caveats in Software Release 6.1(2), page 175

Open Caveats in Software Release 6.1(2)

This section describes open caveats in supervisor engine software release 6.1(2):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- The CiscoView that is embedded in the cat6000-supcv.6-1-1.bin and cat6000-supcv.6-1-2.bin images no longer work after May 11, 2001 because the digital certificates used to sign the Java classes have expired.

  For workarounds and additional information, see the following URL:

  http://www.cisco.com/warp/public/770/fn13613.shtml

  (CSCdu25881)

  Note This problem is not present in any other software releases and images than those mentioned in this caveat.

- VLAN 2035 cannot be used for a voice VLAN due to an incorrect LTL index mapping. (CSCds64624)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(4)E2 are reset every 9 minutes by the Supervisor Engine 2. (CSCdt02646)
- WS-X6101 ATM modules running Cisco IOS Release 12.1(5a)E3 do not support HA for Supervisor Engine 2. (CSCdt29354)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- The OAM-PVC management feature does not work in a back-to-back configuration. The PVC comes up and passes traffic until you configure the OAM management feature. After you configure the feature, the PVC goes down. When the PVC is down, entering the **show atm vc** command shows that the OAM cells on one of the devices is not receiving OAM cells. If you enter the **shut** command and then the no **shut** command, the main ATM interfaces become active. If you perform a cold boot on the switch, the PVC does not become active again until you enter the **shut** and **no shut** commands on the main interfaces on both devices at the same time or remove the OAM management feature. The workaround is not to configure OAM management. (CSCdt04481)

  Note This problem has not been seen in later releases.

- If you configure large Cisco IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same Cisco IOS ACL and share the same label before might not be able to do so any more. As a result the Cisco IOS ACLs are duplicated and might not fit into TCAM. The workaround is to disable and reenable the interface. (CSCds66134)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. You need to shorten the rise and fall times, although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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. The rewrite that is generated for multicast is a Layer 3 rewrite so 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). For the packets that are bridged in the same incoming VLAN, no ToS rewrite occurs. (CSCdm72364)

Resolved Caveats in Software Release 6.1(2)

This section describes resolved caveats in supervisor engine software release 6.1(2):

- After a module goes through a POST test, the status for the module shows "OK" even if all of the ports on the module fail the loopback status test. The module status should show "Faulty" if all ports on a module fail the loopback status test. This problem is resolved in software release 6.1(2). (CSCdt05369)
- In a redundant configuration, when the supervisor engine in slot 2 is active and one or both Gigabit Ethernet ports on the active supervisor engine are configured as ISL trunks and one or both are forwarding RSPAN VLAN-mode traffic from a SPAN source that is an 802.1Q trunk, if a switchover occurs to the supervisor engine in slot 1, the other end of the supervisor engine ISL trunk might receive 802.1Q BPDUs on all VLANs allowed on the source 802.1Q trunk for approximately 20 seconds. This problem is resolved in software release 6.1(2). (CSCds36511)

- In a redundant configuration of WS-X6K-SUP1A-2GE, when the primary supervisor is removed from the system, attempts to reset the active supervisor might fail with the message "Reset is disabled while a download is in Progress." Attempts to kill the process might be unsuccessful, requiring a power cycle of the chassis to reset the hardware. This problem is resolved in software release 6.1(2). (CSCdt09320)
- If you enter the following configuration commands in sequence through SNMP, you will lose the private VLAN configuration:

  1. **copy vlan database**

  2. **update vlan configuration**

  3. **apply vlan configuration**

  This problem is resolved in software release 6.1(2) with the following restriction: in the above steps, the SNMP-apply operation will fail if you attempt to delete a VLAN that is a primary VLAN with at least one secondary VLAN associated with it. (CSCdr97501)
- The Catalyst 6000 switch might reload if the configuration is restored from the configuration file and if EtherChannel and RMON are enabled and the following commands are entered in sequence:

  1. **clear config all**

  2. **reset**

  3. **copy flash config**

  This problem is resolved in software release 6.1(2). (CSCds79278)
- In systems with redundant supervisor engines, when a high-availability switchover occurs, as the standby supervisor engine transitions to active it might experience a watchdog timeout and a series of Bus Timeout NMIs. The standby then remains inactive. The workaround is to power cycle the switch. This problem is resolved in software release 6.1(2). (CSCdr72885)
- If you configure port security on private-VLAN ports, those ports will experience traffic failures. This problem is resolved in software release 6.1(2). (CSCds71111)
- Because a different code is being passed to the module firmware, the supervisor engine does not recognize that the modules are online; as a result, the ports do not come up. This problem is resolved in software release 6.1(2). (CSCds63341)
- In a test scenario with high traffic levels and at least 48 nonfabric-enabled ports, 10 fabric-enabled ports, and supervisor engine uplink ports all configured for high-priority voice traffic that is forwarded from the fabric-enabled cards to the supervisor uplink ports, the chassis stops forwarding packets. The links stay up and at some point the ports might start flow control. This problem is resolved in software release 6.1(2). (CSCds83339)
- If an EtherChannel is formed with ports on multiple modules, removing a module containing ports that are members of the EtherChannel deletes the EtherChannel from the VTP database. The **show spantree** command shows the remaining EtherChannel ports in forwarding state, but the **show trunk** command displays no VLANs in forwarding state. This problem is resolved in software release 6.1(2). (CSCds82742)
- When the switch is running in MISTP mode, the MSFC trunk might be put into blocking state. The **show spantree** command shows the port in forwarding state, but the **show trunk** command does not show the VLAN in forwarding state. The only workaround is to enable STP for this MISTP instance and then disable it. This problem is resolved in software release 6.1(2). (CSCds79615)

- When you change the spanning tree mode from PVST+ to MISTP-PVST+, non-trunk ports on the switch will not forward traffic unless you disable and reenable the ports. The port error counters increment on the switch while the switch fails to pass traffic, and the CAM entry for the PC attached to the port goes away. The fix is to unplug and then plug in the PC Ethernet cable or to disable then reenable the port attached to the PC. This problem is resolved in software release 6.1(2). (CSCds80011)
- NDE exports incorrect time stamps due to an error in calculating the time stamps of Layer 3 shortcuts. This problem is resolved in software release 6.1(2). (CSCds50070)
- On Catalyst 6000 Supervisor Engine 2, the temperature monitoring does not work properly in software release 6.1(1). This problem is resolved in software release 6.1(2). (CSCdr97370)
- If you configure level 2 system logging and a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. This problem is resolved in software release 6.1(2). (CSCds23497)
- HSRP does not work on a redundant supervisor engine. This problem is resolved in software release 6.1(2). (CSCds62804)
- During a switchover, the LCP processes interrupt signals that should be ignored in non-fabric enabled mode. This problem is resolved in software release 6.1(2). (CCds42775)
- The active supervisor engine fails to synchronize Switch Fabric Module interfaces from compact to truncated mode. This problem is resolved in software release 6.1(2). (CSCds43224)
- Occasionally, the boot configuration on a standby Supervisor Engine 2 running software release 6.1(1a) and later gets corrupted. This problem is resolved in software release 6.1(2). (CSCds36523)
- Supervisor Engine 2 needs support for 32 MB bootflash. This problem is resolved in software release 6.1(2). (CSCds13961)
- The WS-X6608 and WS-X6624 modules do not register with Cisco CallManager. This failure occurs either after Cisco CallManager stops or if some ports are not registered. Either condition causes the module ports to reset. After an extended period of time, the ports stop resetting themselves, which causes the WS-X6608 and WS-X6624 modules not to register with Cisco CallManager. The workaround is to reset the module. This will cause the ports to register correctly.

  This problem is resolved in software release 6.1(2). (CSCds35444)
- In a Catalyst 6000 family switch running software release 6.1(1) and with a redundant MSFC2 configuration, if you attempt to roll back the MSFC2 images temporarily by setting them to boot to ROMMON and from ROMMON load the MSFC2 image from sup-slot0:, the TFTP process might hang for an extended time period and prevent all module and switch resets as well as all CLI commands that require the download area. The workaround is to allow the first MSFC2 to come online completely and the CPU utilization on the supervisor engine to decrease before you attempt to download the image to the second MSFC2. An alternative workaround is to wait for approximately six minutes after the failure for the download area to become available for a retry.

  This problem is resolved in software release 6.1(2). (CSCds38036)
- Due to a hardware problem, the console connection occasionally hangs when traffic volume is high and there are many hosts. This problem is resolved in software release 6.1(2). (CSCds42670)
- Attempting to modify a VLAN from a Web browser connected to the Catalyst 6509 fails if internal VLANs exist in the vtpVlanEditTable. The effort to apply the table will fail with this message:

  ```
  vtpVlanApplyStatus = 9 (someOtherError)
  ```

  This problem is resolved in software release 6.1(2). (CSCds50964)

- In software releases 6.1(1), 5.5(4), and earlier, if you install more than 1024 dynamic ACEs and enable high availability, due to a a memory corruption the standby supervisor engine might reload if it becomes the active supervisor engine after the switchover. This problem is resolved in software release 6.1(2). (CSCds54441)
- The last used time stamp is less than the creation time stamp. This problem is resolved in software release 6.1(2). (CSCds56305)
- Some MLS flows are not aged out. This problem is resolved in software release 6.1(2). (CSCds73531)
- A VMPS download might fail if the supervisor engine is in slot 2 and slot 1 is empty. This problem is resolved in software release 6.1(2). (CSCds66629)
- Configurations for VTP v2 and pruning are not saved in NVRAM/CRESMIB when the switch changes from VTP_CLIENT mode to VTP_SERVER mode. If the switch resets when the VTP mode changes, the VTP v2 and pruning configurations might become incorrect. This problem is resolved in software release 6.1(2). (CSCds24430)
- In extremely rare conditions, high availability (HA) is disabled while VTP is still in the middle of its HA operation. This situation causes a problem for subsequent VTP HA operations once HA is reenabled. This problem is resolved in software release 6.1(2). (CSCds27845)
- Broadcast suppression on the Catalyst 6000 Supervisor Engine 2 does not work properly in software releases prior to 6.1(2). This problem is resolved in software release 6.1(2). (CSCds11670)
- The **show mls entry** command might display the wrong source port when a WS-X6182-2PA module is part of a flow. This is a display problem only and does not affect functionality. This problem is resolved in software release 6.1(2). (CSCds26286)
- Occasionally, IPX clients might not be able to connect to a server at bootup. This problem is resolved in software release 6.1(2). (CSCds27467)
- NDE exports incorrect time stamps due to an error in calculating the time stamps of Layer 3 shortcuts. This problem is resolved in software release 6.1(2). (CSCds50070)
- NetFlow Data Export (NDE) CPU utilization is high under moderate to heavy loads because NDE entries are not aged out correctly. The high CPU utilization occurs when NDE is enabled and the problem remains even after loads are reduced. This problem is resolved in software release 6.1(2). (CSCds51525)
- Nonalphanumeric characters are not valid in VTP domain names but can be configured in certain cases. This problem is resolved in software release 6.1(2). (CSCds34927)
- CAM entries might age out prematurely causing traffic flooding when there is heavy traffic. This problem exists in software releases 6.1.(1a) and later. This problem does not exist in prior software releases. The workaround is to set the CAM aging time to zero.

  This problem is resolved in software release 6.1(2). (CSCds71110)
- SNMP ifTable loops in a “get next” operation when:
  - HA is enabled.
  - The ifIndexing in the ifTable is not sequential (meaning there is a gap in the Index).
  - You enter a **clear config all** command.
  - You reenable high availability.
  - You enter a switch supervisor command.

  This problem is resolved in software release 6.1(2). (CSCds58124)

- When configuring security or QoS ACLs, you might receive a message that TCAM LOU usage capability has been exceeded when it has not. If this occurs, further ACL configuration with the operators in question is not possible. This problem is resolved in software release 6.1(2). (CSCds39830)
- In a redundant configuration, IPX traffic stops after a supervisor engine switchover. There are two workarounds for this problem:
  - On the designated MSFC, enter **shutdown** followed by **no shutdown** commands on the interfaces where the traffic is not being switched (this also interrupts IP traffic).
  - On the designated MSFC, enter the **no ipx network** command followed by the **ipx network** command on the interfaces where the traffic is not being switched.

  This problem is resolved in software release 6.1(2). (CSCds38761)
- With Supervisor Engine 2, to avoid a lengthy delay when applying a large configuration file, disable as many ports as possible before configuration. CSCds19350 is a duplicate of CSCds11670, which is resolved in software release 6.1(2). (CSCds19350)
- In MISTP mode, if an 802.1Q trunking EtherChannel is formed by ports on two modules, where one module has only one port in the EtherChannel and the other module powers down, then the other side of the EtherChannel detects a spanning tree loop and goes into the error disabled state. This problem is resolved in software release 6.1(2). (CSCds38397)
- If you configure MISTP and PVST+ instances and 802.1Q tunneling on redundant EtherChannels and one of the EtherChannels fails, a high-availability switchover might not complete successfully. This problem is resolved in software release 6.1(2). (CSCds33754)
- If you configure MISTP instances and more than 70,000 STP instances on a Supervisor Engine 2 or more than 25,000 STP instances on a Supervisor Engine 1, a high-availability switchover causes a watchdog timeout. This problem is resolved in software release 6.1(2). (CSCds32671)
- If you disable a MISTP instance and a high-availability switchover occurs, the EtherChannel ports do not show up in the spanning tree database and CBL/LTL is not set for those ports. After a few seconds, the problem resolves itself when the channel reforms. This problem is resolved in software release 6.1(2). (CSCds29658)
- If you move a VLAN between two STP instances, one of which has MISTP disabled, and a high-availability switchover occurs, the STP instances both claim the mapping of the VLAN. To avoid this problem, either do not disable MISTP or manually remap VLANs that are moved between STP instances with the **set vlan** *vlan_ID* **mistp-instance** *inst_number* command. This problem is resolved in software release 6.1(2). (CSCds23679)
- When you assign instances to VLANs in MISTP mode, then switch to PVST+ mode and configure PVLAN associations with the **set pvlan** command then switch back to MISTP mode, the secondary VLANs are not visible on any trunk because they will have lost the associated MISTP instance. Connectivity is also lost. You must assign the primary and secondary VLANs individually to the same MISTP instance before creating the PVLAN association, using the **set pvlan** command, or the VLANs do not join the MISTP instance. This problem is resolved in software release 6.1(2). (CSCds38394)
- When switching from MISTP-PVST+ to PVST+, the **show trunk** command might incorrectly display a port as “forwarding” when it is “blocking.” Switching operates correctly; no incorrect flooding occurs. This problem is resolved in software release 6.1(2). (CSCds28296)
- In extremely rare conditions, an EtherChannel might get put in the error-disabled state if it was formed from ports that just became trunks that did not have their native VLAN in the allowed range. This problem is resolved in software release 6.1(2). (CSCds35238)

- On Supervisor Engine 2, depending on the volume of console traffic, MLS entries might take longer to age out than expected and the system uptime might be inaccurate. This problem is resolved in software release 6.1(2). (CSCdr67657)
- In nonredundant systems, when you enter the **clear config all** command and reset the system, the ifIndex does not reset. In redundant systems with high availability enabled, when you enter the **clear config all** command and then use the **switch supervisor** command, the standby supervisor engine becomes active but you see multiple ifEntrys for the same VlanIndex. The workaround for redundant systems is to disable high availability and use the **switch supervisor** command after entering the **clear config all** command; this causes the ifIndex to reset. This problem is resolved in software release 6.1(2). (CSCds34328)
- You cannot enable MISTP mode and VTP pruning at the same time. If you enter a **set spantree mode mistp** command to enable MISTP mode, enter a **set vtp pruning disable** command to disable VTP pruning. If VTP pruning is enabled via learning from another switch in the network while MISTP is enabled, the switch changes to VTP transparent mode. This problem is resolved in software release 6.1(2). (CSCds16519)
- Routed flows that are microflow policed do not appear in the output of a **show mls statistics entry** command if the flow was present before the MSFC came online. This does not affect traffic switching. This problem is resolved in software release 6.1(2). (CSCds16891)
- When you enable the high-availability feature, do not enable RSVP. This problem is resolved in software release 6.1(2). (CSCds17369)
- The **set module power down** command is not in the configuration file for modules that are powered down. After clearing and restoring configuration, previously powered down modules are powered on. A workaround is to issue the **set module power down** commands manually after restoring the configuration. This problem is resolved in software release 6.1(2). (CSCds34320)
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a “bad value” error. The problem exists in 5.x and 6.1(1a) releases. The workaround is to use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. This problem is resolved in software release 6.1(2). (CSCds22815)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. This problem is resolved in software release 6.1(2). (CSCdk75107)
- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90 percent, some **show** commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) sh ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  The workaround, if most of the memory was used by RMON buckets, is one of the following:

  - Reduce the number of buckets for each entry.
  - Reduce the number of control entries.
  - Disable the RMON feature.

  This problem is resolved in software release 6.1(2). (CSCds30395)
- Under extreme traffic conditions and with certain hardware configurations, the supervisor engine might reset. CSCdr50405 is a duplicate of CSCdp84973, which is resolved in software release 6.1(2). (CSCdr50405)

- If remote SPAN traffic fails for an EtherChannel formed from ports on both supervisor engines, disable and reenable the ports. If traffic fails in a VLAN that is in the STP forwarding state on either supervisor engine EtherChannel ports or on WS-X6516-GBIC switching module ports, disable and reenable the ports. CSCds39270 is a duplicate of CSCds41452, which is resolved in software release 6.1(2). (CSCds39270)

Open and Resolved Caveats in Software Release 6.1(1e)

These sections describe open and resolved caveats in supervisor engine software release 6.1(1e):

- Open Caveats in Software Release 6.1(1e), page 181
- Resolved Caveats in Software Release 6.1(1e), page 182

Open Caveats in Software Release 6.1(1e)

This section describes open caveats in supervisor engine software release 6.1(1e):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- If you configure large Cisco IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same Cisco IOS ACL and share the same label before might not be able to do so any more. As a result the Cisco IOS ACLs are duplicated and might not fit into TCAM. The workaround is to disable and reenable the interface. (CSCds66134)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)

- With QoS enabled, after clearing the configuration, you might see syslog failure messages relating to setting the CoS map on the supervisor. For example, you might see this message:

  ```
  QOS-3-SETCOSMAPFAIL:Unable to set CoS map on module 1.
  ```

  (CSCdr42943)

- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. You need to shorten the rise and fall times, although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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 6.1(1e)

This section describes resolved caveats in supervisor engine software release 6.1(1e):

- An error can occur with management protocol processing. Use the following URL for further information: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw67458

  This problem is resolved in software release 6.1(1e). (CSCdw67458)

Open and Resolved Caveats in Software Release 6.1(1d)

These sections describe open and resolved caveats in supervisor engine software release 6.1(1d):

- Open Caveats in Software Release 6.1(1d), page 182
- Resolved Caveats in Software Release 6.1(1d), page 184

Open Caveats in Software Release 6.1(1d)

This section describes open caveats in supervisor engine software release 6.1(1d):

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)

- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- If you configure large Cisco IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same Cisco IOS ACL and share the same label before might not be able to do so any more. As a result the Cisco IOS ACLs are duplicated and might not fit into TCAM. The workaround is to disable and reenable the interface. (CSCds66134)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- With QoS enabled, after clearing the configuration, you might see syslog failure messages relating to setting the CoS map on the supervisor. For example, you might see this message:

  ```
  QOS-3-SETCOSMAPFAIL:Unable to set CoS map on module 1.
  ```

  (CSCdr42943)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as "not-connected." This error does not affect operation. (CSCds00575)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. You need to shorten the rise and fall times, although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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 6.1(1d)

This section describes resolved caveats in supervisor engine software release 6.1(1d):

- Software release 6.1(1d) is the minimum recommended release for hardware revisions 2.1 and later of the Supervisor Engine 2.

  If you install a new redundant Supervisor Engine 2 that is running software version 6.1(1d) or later, ensure that the primary supervisor is running the same software version. Failure to do so will cause the system to overwrite the software on the redundant supervisor engine with the older unsupported version.

  To avoid this problem, do one of the following:

  - Upgrade the existing Supervisor Engine 2 to software release 6.1(1d) or later.
  - Power down the system, remove the existing Supervisor Engine 2, replace it with the new Supervisor Engine 2, power up the system, and install the "old" Supervisor Engine 2 in slot 2. This will automatically update the software on the Supervisor Engine 2 installed in slot 2.

  (CSCdt12701)

Open and Resolved Caveats in Software Release 6.1(1c)

These sections describes open and resolved caveats in supervisor engine software release 6.1(1c):

- Open Caveats in Software Release 6.1(1c), page 184
- Resolved Caveats in Software Release 6.1(1c), page 187

Open Caveats in Software Release 6.1(1c)

This section describes open caveats in supervisor engine software release 6.1(1c).

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- CAM entries might age out prematurely causing traffic flooding when there is heavy traffic. This problem exists in software release 6.1.(1a) and later. This problem does not exist in prior software releases.

  Workaround: Set the CAM aging time to zero. (CSCds71110)

- In a redundant configuration, when the supervisor engine in slot 2 is active and one or both Gigabit Ethernet ports on the active supervisor engine are configured as ISL trunks and one or both are forwarding RSPAN VLAN-mode traffic from a SPAN source that is an 802.1Q trunk, if a switchover occurs to the supervisor engine in slot 1, the other end of the supervisor engine ISL trunk might receive 802.1Q BPDUs on all VLANs allowed on the source 802.1Q trunk for approximately 20 seconds. (CSCds36511)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- When configuring security or QoS ACLs, you might receive a message that TCAM LOU usage capability has been exceeded when it has not. If this occurs, further ACL configuration with the operators in question is not possible. (CSCds39830)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- With Supervisor Engine 2, to avoid a lengthy delay when applying a large configuration file, disable as many ports as possible before configuration. (CSCds19350)
- In a redundant configuration, IPX traffic stops after supervisor engine switchover. There are two workarounds for this problem:
  - On the designated MSFC, enter **shutdown** followed by **no shutdown** commands on the interfaces where the traffic is not being switched (this also interrupts IP traffic).
  - On the designated MSFC, enter the **no ipx network** command followed by the **ipx network** command on the interfaces where the traffic is not being switched.

  (CSCds38761)
- If you configure level 2 system logging and if a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. (CSCds23497)
- In MISTP mode, if there is an 802.1Q trunking EtherChannel formed by ports on two modules, where one module has only one port in the EtherChannel and the other module powers down, then the other side of the EtherChannel detects a spanning tree loop and goes into the error disabled state. (CSCds38397)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- With MISTP and PVST+ instances configured and 802.1Q tunneling configured on redundant EtherChannels, if one of the EtherChannels fails, an HA switchover might not complete successfully. (CSCds33754)
- With MISTP instances configured and more than 70,000 STP instances on a Supervisor Engine 2 or more than 25,000 STP instances on a Supervisor Engine 1, an HA switchover causes a watchdog timeout. (CSCds32671)
- If a MISTP instance is disabled and an HA switchover occurs, the ports in EtherChannels do not show up in the spanning tree database and CBL/LTL is not set for those ports. After a few seconds, the problem resolves itself when the channel reforms. (CSCds29658)

- If you move a VLAN between two STP instances, one of which has MISTP disabled, and an HA switchover occurs, the STP instances both claim the mapping of the VLAN. To avoid this problem, either do not disable MISTP or manually remap VLANs that are moved between STP instances with the **set vlan** *vlan_ID* **mistp-instance** *inst_number* command. (CSCds23679)
- This problem happens only when you assign instances to VLANs in MISTP mode, then switch to PVST+ mode and configure PVLAN associations with the **set pvlan** command then switch back to MISTP mode. At that point the secondary VLANs are not visible on any trunk because they will have lost the associated MISTP instance and connectivity is also lost. The primary and secondary VLANs must be individually assigned to the same MISTP instance before creating the PVLAN association using the **set pvlan** command or the VLANs do not join the MISTP instance. (CSCds38394)
- When switching from MISTP-PVST+ to PVST+, the **show trunk** command might incorrectly display a port as forwarding when it is blocking. Switching operates correctly; no incorrect flooding occurs. (CSCds28296)
- In extremely rare conditions, an EtherChannel might get put in the error-disabled state if it was formed from ports that just became trunks that did not have their native VLAN in the allowed range. (CSCds35238)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On Supervisor Engine 2, depending on the volume of console traffic, MLS entries might take longer to age out than expected and the system uptime might be inaccurate. (CSCdr67657)
- In nonredundant systems, when you enter the **clear config all** command and reset the system, the ifIndex does not reset. In redundant systems with high availability enabled, when you enter the **clear config all** command and then use the **switch supervisor** command, the standby supervisor engine becomes active but you see multiple ifEntrys for the same VlanIndex. The workaround for redundant systems is to disable high availability and use the **switch supervisor** command after entering the **clear config all** command; this causes the ifIndex to reset. (CSCds34328)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as “not-connected.” This error does not affect operation. (CSCds00575)
- MISTP mode and VTP pruning can not be enabled at the same time. If you enter a **set spantree mode mistp** command to enable MISTP mode, enter a **set vtp pruning disable** command to disable VTP pruning. If VTP pruning is enabled via learning from another switch in the network while MISTP is enabled, the switch changes to VTP transparent mode. (CSCds16519)
- Routed flows that are microflow policed do not appear in the output of a **show mls statistics entry** command if the flow was present before the MSFC came online. This does not affect traffic switching. (CSCds16891)
- When the high-availability feature is enabled, do not enable RSVP. (CSCds17369)
- The **set module power down** command is not in the configuration file for modules that are powered down. After clearing and restoring configuration, previously powered down modules are powered on. A workaround is to issue the **set module power down** commands manually after restoring the configuration. (CSCds34320)
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a “bad value” error. The problem exists in 5.x and 6.1(1a) releases. The workaround is to use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. (CSCds22815)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)

- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90%, some **show** commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) sh ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  The workaround, if most of the memory was used by RMON buckets, is one of the following:

  - Reduce the number of buckets for each entry
  - Reduce the number of control entries
  - Disable the RMON feature

  (CSCds30395)

- Under extreme traffic conditions and with certain hardware configurations, the supervisor engine might reset. (CSCdr50405)
- If remote SPAN traffic fails for an EtherChannel formed from ports on both supervisor engines, disable and reenable the ports. If traffic fails in a VLAN that is in the STP forwarding state on an EtherChannel formed from supervisor engine ports and that is in the STP forwarding state on a WS-X6516-GBIC Switching module, disable and reenable the ports. (CSCds39270)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. The rise and fall times need to be shortened although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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 6.1(1c)

This section describes resolved caveats in supervisor engine software release 6.1(1c):

- Non-SSH connection attempts to an enabled SSH service on a Catalyst 6000 switch might cause a "protocol mismatch" error, resulting in a supervisor engine failure. The supervisor engine failure causes the switch to fail to pass traffic and reboots the switch. This problem is resolved in software release 6.1(1c). (CSCds85763)

Open and Resolved Caveats in Software Release 6.1(1b)

These sections describes open and resolved caveats in supervisor engine software release 6.1(1b):

Open Caveats in Software Release 6.1(1b)

This section describes open caveats in supervisor engine software release 6.1(1b).

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- The CiscoView that is embedded in the cat6000-supcv.6-1-1.bin and cat6000-supcv.6-1-2.bin images no longer work after May 11, 2001 because the digital certificates used to sign the Java classes have expired.

  For workarounds and additional information, see the following URL:

  http://www.cisco.com/warp/public/770/fn13613.shtml

  (CSCdu25881)

  Note This problem is not present in any other software releases and images than those mentioned in this caveat.

- CAM entries might age out prematurely causing traffic flooding when there is heavy traffic. This problem exists in software release 6.1.(1a) and later. This problem does not exist in prior software releases.

  Workaround: Set the CAM aging time to zero. (CSCds71110)
- In a redundant configuration, when the supervisor engine in slot 2 is active and one or both Gigabit Ethernet ports on the active supervisor engine are configured as ISL trunks and one or both are forwarding RSPAN VLAN-mode traffic from a SPAN source that is an 802.1Q trunk, if a switchover occurs to the supervisor engine in slot 1, the other end of the supervisor engine ISL trunk might receive 802.1Q BPDUs on all VLANs allowed on the source 802.1Q trunk for approximately 20 seconds. (CSCds36511)
- When configuring security or QoS ACLs, you might receive a message that TCAM LOU usage capability has been exceeded when it has not. If this occurs, further ACL configuration with the operators in question is not possible. (CSCds39830)

- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- With Supervisor Engine 2, to avoid a lengthy delay when applying a large configuration file, disable as many ports as possible before configuration. (CSCds19350)
- In a redundant configuration, IPX traffic stops after supervisor engine switchover. There are two workarounds for this problem:
  - On the designated MSFC, enter **shutdown** followed by **no shutdown** commands on the interfaces where the traffic is not being switched (this also interrupts IP traffic).
  - On the designated MSFC, enter the **no ipx network** command followed by the **ipx network** command on the interfaces where the traffic is not being switched.

  (CSCds38761)
- If you configure level 2 system logging and if a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. (CSCds23497)
- In MISTP mode, if there is an 802.1Q trunking EtherChannel formed by ports on two modules, where one module has only one port in the EtherChannel and the other module powers down, then the other side of the EtherChannel detects a spanning tree loop and goes into the error disabled state. (CSCds38397)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- With MISTP and PVST+ instances configured and 802.1Q tunneling configured on redundant EtherChannels, if one of the EtherChannels fails, an HA switchover might not complete successfully. (CSCds33754)
- With MISTP instances configured and more than 70,000 STP instances on a Supervisor Engine 2 or more than 25,000 STP instances on a Supervisor Engine 1, an HA switchover causes a watchdog timeout. (CSCds32671)
- If a MISTP instance is disabled and an HA switchover occurs, the ports in EtherChannels do not show up in the spanning tree database and CBL/LTL is not set for those ports. After a few seconds, the problem resolves itself when the channel reforms. (CSCds29658)
- If you move a VLAN between two STP instances, one of which has MISTP disabled, and an HA switchover occurs, the STP instances both claim the mapping of the VLAN. To avoid this problem, either do not disable MISTP or manually remap VLANs that are moved between STP instances with the **set vlan** *vlan_ID* **mistp-instance** *inst_number* command. (CSCds23679)

- This problem happens only when you assign instances to VLANs in MISTP mode, then switch to PVST+ mode and configure PVLAN associations with the **set pvlan** command then switch back to MISTP mode. At that point the secondary VLANs are not visible on any trunk because they will have lost the associated MISTP instance and connectivity is also lost. The primary and secondary VLANs must be individually assigned to the same MISTP instance before creating the PVLAN association using the **set pvlan** command or the VLANs do not join the MISTP instance. (CSCds38394)
- When switching from MISTP-PVST+ to PVST+, the **show trunk** command might incorrectly display a port as forwarding when it is blocking. Switching operates correctly; no incorrect flooding occurs. (CSCds28296)
- In extremely rare conditions, an EtherChannel might get put in the error-disabled state if it was formed from ports that just became trunks that did not have their native VLAN in the allowed range. (CSCds35238)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On Supervisor Engine 2, depending on the volume of console traffic, MLS entries might take longer to age out than expected and the system uptime might be inaccurate. (CSCdr67657)
- In nonredundant systems, when you enter the **clear config all** command and reset the system, the ifIndex does not reset. In redundant systems with high availability enabled, when you enter the **clear config all** command and then use the **switch supervisor** command, the standby supervisor engine becomes active but you see multiple ifEntrys for the same VlanIndex. The workaround for redundant systems is to disable high availability and use the **switch supervisor** command after entering the **clear config all** command; this causes the ifIndex to reset. (CSCds34328)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as “not-connected.” This error does not affect operation. (CSCds00575)
- MISTP mode and VTP pruning can not be enabled at the same time. If you enter a **set spantree mode mistp** command to enable MISTP mode, enter a **set vtp pruning disable** command to disable VTP pruning. If VTP pruning is enabled via learning from another switch in the network while MISTP is enabled, the switch changes to VTP transparent mode. (CSCds16519)
- Routed flows that are microflow policed do not appear in the output of a **show mls statistics entry** command if the flow was present before the MSFC came online. This does not affect traffic switching. (CSCds16891)
- When the high-availability feature is enabled, do not enable RSVP. (CSCds17369)
- The **set module power down** command is not in the configuration file for modules that are powered down. After clearing and restoring configuration, previously powered down modules are powered on. A workaround is to issue the **set module power down** commands manually after restoring the configuration. (CSCds34320)
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a “bad value” error. The problem exists in 5.x and 6.1(1a) releases. The workaround is to use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. (CSCds22815)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)

- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90%, some **show** commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) sh ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  The workaround, if most of the memory was used by RMON buckets, is one of the following:

  - Reduce the number of buckets for each entry
  - Reduce the number of control entries
  - Disable the RMON feature

  (CSCds30395)

- Under extreme traffic conditions and with certain hardware configurations, the supervisor engine might reset. (CSCdr50405)
- If remote SPAN traffic fails for an EtherChannel formed from ports on both supervisor engines, disable and reenable the ports. If traffic fails in a VLAN that is in the STP forwarding state on either supervisor engine EtherChannel ports or on WS-X6516-GBIC switching module ports, disable and reenable the ports. (CSCds39270)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. The rise and fall times need to be shortened although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- 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 6.1(1b)

This section describes resolved caveats in supervisor engine software release 6.1(1b):

- Under some conditions, the WS-X6516-GBIC module might fail online diagnostics and not come online. This problem is resolved in software release 6.1(1b). (CSCds67513)

Open and Resolved Caveats in Software Release 6.1(1a)

These sections describes open and resolved caveats in supervisor engine software release 6.1(1a):

- Open Caveats in Software Release 6.1(1a), page 192
- Resolved Caveats in Software Release 6.1(1a), page 196

Open Caveats in Software Release 6.1(1a)

This section describes open caveats in supervisor engine software release 6.1(1a).

- Multicast traffic is not being routed across the switch for mroute entries that are partial shortcuts where the input interface is a WAN interface (such as FlexWAN and OSM). The problem is caused by misprogramming of a hardware index on the supervisor engine. The problem is triggered if the MSFC is rebooted without rebooting the switch. Once the problem manifests, the indexes will remain in the incorrect state. (CSCdv54808)
- In certain cases, a hardware register in an ASIC (register FCNTL0) can be corrupted during the fabric synchronization process. Symptoms of the problem can vary but would be expected to cause the ASIC to stop receiving/transmitting data to the fabric. This ASIC is present on all fabric-enabled modules, and provides the interface to the Switch Fabric Module (SFM). (CSCdu38986)
- A firmware issue in an ASIC's loopback-protection handling can cause switching of traffic through the Switch Fabric Module (SFM) to gradually stop. These ASICs are present on the SFM and provide switch fabric functions for the switch. Resetting the SFM resolves the problem but it can reoccur. (CSCdu84704)
- CAM entries might age out prematurely causing traffic flooding when there is heavy traffic. This problem exists in software release 6.1.(1a) and later. This problem does not exist in prior software releases.

  Workaround: Set the CAM aging time to zero. (CSCds71110)
- In a redundant configuration, when the supervisor engine in slot 2 is active and one or both Gigabit Ethernet ports on the active supervisor engine are configured as ISL trunks and one or both are forwarding RSPAN VLAN-mode traffic from a SPAN source that is an 802.1q trunk, if a switchover occurs to the supervisor engine in slot 1, the other end of the supervisor engine ISL trunk might receive 802.1Q BPDUs on all VLANs allowed on the source 802.1q trunk for approximately 20 seconds. (CSCds36511)
- When configuring security or QoS ACLs, you might receive a message that TCAM LOU usage capability has been exceeded when it has not. If this occurs, further ACL configuration with the operators in question is not possible. (CSCds39830)
- Occasionally, in a redundant Supervisor Engine 2 configuration, the FIB on the standby supervisor engine has slightly fewer entries than the FIB on the active supervisor engine. If the standby supervisor engine becomes the active supervisor engine, the MSFC2 updates the FIB with all necessary entries. (CSCds20478)

  Note CSCds20478 has not been seen in later releases.
- In a fully redundant configuration, occasionally after a switchover, when the supervisor engine that reset comes back up, fabric channel errors occur on the active Switch Fabric Module and the active Switch Fabric Module powers down and normal operation resumes with the standby Switch Fabric Module. (CSCds36157)

  Note CSCds36157 has not been seen in later releases.

- In a switch with one nonfabric-enabled switching module, to ensure successful transition to compact mode, do not remove the nonfabric-enabled switching module during an HA switchover. (CSCds37394)

  Note CSCds37394 has not been seen in later releases.

- After a reload, if the nondesignated MSFC comes online while the designated MSFC is still processing a large or complex ACL configuration, the switch might reload. (CSCds38753)
- When you connect an ISL trunk port to an access port and QoS is enabled on the switch that has the ISL trunk, the ISL header sets the USER bits in the DA. Currently, the supervisor engine drops only the packets with user bits set to 0 and 1 and forwards the packets with other bits set to the access VLAN of the non-trunk port. The forwarded packets do not go through blocked ports. (CSCdu10858)
- If the designated MSFC reloads when it is downloading a large ACL configuration to the supervisor engine, the supervisor engine might reject the ACL configuration from the new designated MSFC and display a "%FM-2-TCAM_ERROR:TCAM programming error 5" message. To recover, reset the supervisor engine. (CSCds39392)
- With Supervisor Engine 2, to avoid a lengthy delay when applying a large configuration file, disable as many ports as possible before configuration. (CSCds19350)
- In a redundant configuration, IPX traffic stops after supervisor engine switchover. There are two workarounds for this problem:
  - On the designated MSFC, enter **shutdown** followed by **no shutdown** commands on the interfaces where the traffic is not being switched (this also interrupts IP traffic).
  - On the designated MSFC, enter the **no ipx network** command followed by the **ipx network** command on the interfaces where the traffic is not being switched.

  (CSCds38761)
- If you configure level 2 system logging and if a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. (CSCds23497)
- In MISTP mode, if there is an 802.1Q trunking EtherChannel formed by ports on two modules, where one module has only one port in the EtherChannel and the other module powers down, then the other side of the EtherChannel detects a spanning tree loop and goes into the error disabled state. (CSCds38397)
- Occasionally, a module might fail to come online after a reset when UplinkFast is enabled. The workaround is to reset the module again. (CSCds37139)
- With MISTP and PVST+ instances configured and 802.1Q tunneling configured on redundant EtherChannels, if one of the EtherChannels fails, an HA switchover might not complete successfully. (CSCds33754)
- With MISTP instances configured and more than 70,000 STP instances on a Supervisor Engine 2 or more than 25,000 STP instances on a Supervisor Engine 1, an HA switchover causes a watchdog timeout. (CSCds32671)
- If a MISTP instance is disabled and an HA switchover occurs, the ports in EtherChannels do not show up in the spanning tree database and CBL/LTL is not set for those ports. After a few seconds, the problem resolves itself when the channel reforms. (CSCds29658)

- If you move a VLAN between two STP instances, one of which has MISTP disabled, and an HA switchover occurs, the STP instances both claim the mapping of the VLAN. To avoid this problem, either do not disable MISTP or manually remap VLANs that are moved between STP instances with the **set vlan** *vlan_ID* **mistp-instance** *inst_number* command. (CSCds23679)
- This problem happens only when you assign instances to VLANs in MISTP mode, then switch to PVST+ mode and configure PVLAN associations with the set pvlan command then switch back to MISTP mode. At that point the secondary VLANs are not visible on any trunk because they will have lost the associated MISTP instance and connectivity is also lost. The primary and secondary VLANs must be individually assigned to the same MISTP instance before creating the PVLAN association using the set pvlan command or the vlans do not join the MISTP instance. (CSCds38394)
- When switching from MISTP-PVST+ to PVST+, the **show trunk** command might incorrectly display a port as forwarding when it is blocking. Switching operates correctly; no incorrect flooding occurs. (CSCds28296)
- In extremely rare conditions, an EtherChannel might get put in the error-disabled state if it was formed from ports that just became trunks that did not have their native VLAN in the allowed range. (CSCds35238)
- The **set msmautostate disable** command does not work. You cannot disable automatic MSM line protocol state determination. (CSCdr61398)
- On Supervisor Engine 2, depending on the volume of console traffic, MLS entries might take longer to age out than expected and the system uptime might be inaccurate. (CSCdr67657)
- In nonredundant systems, when you enter the **clear config all** command and reset the system, the ifIndex does not reset. In redundant systems with high availability enabled, when you enter the **clear config all** command and then use the **switch supervisor** command, the standby supervisor engine becomes active but you see multiple ifEntrys for the same VlanIndex. The workaround for redundant systems is to disable high availability and use the **switch supervisor** command after entering the **clear config all** command; this causes the ifIndex to reset. (CSCds34328)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays the port status as “not-connected.” This error does not affect operation. (CSCds00575)
- MISTP mode and VTP pruning can not be enabled at the same time. If you enter a **set spantree mode mistp** command to enable MISTP mode, enter a **set vtp pruning disable** command to disable VTP pruning. If VTP pruning is enabled via learning from another switch in the network while MISTP is enabled, the switch changes to VTP transparent mode. (CSCds16519)
- Routed flows that are microflow policed do not appear in the output of a **show mls statistics entry** command if the flow was present before the MSFC came online. This does not affect traffic switching. (CSCds16891)
- When the high-availability feature is enabled, do not enable RSVP. (CSCds17369)
- The **set module power down** command is not in the configuration file for modules that are powered down. After clearing and restoring configuration, previously powered down modules are powered on. A workaround is to issue the **set module power down** commands manually after restoring the configuration. (CSCds34320)
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a “bad value” error. The problem exists in 5.x and 6.1(1a) releases. The workaround is to use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. (CSCds22815)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)

- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90%, some show commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) sh ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  The workaround, if most of the memory was used by RMON buckets, is one of the following:

  - Reduce the number of buckets for each entry
  - Reduce the number of control entries
  - Disable the RMON feature

  (CSCds30395)

- Under extreme traffic conditions and with certain hardware configurations, the supervisor engine might reset. (CSCdr50405)
- If remote SPAN traffic fails for an EtherChannel formed from ports on both supervisor engines, disable and reenable the ports. If traffic fails in a VLAN that is in the STP forwarding state on either supervisor engine EtherChannel ports or on WS-X6516-GBIC switching module ports, disable and reenable the ports. (CSCds39270)
- The WS-X6248-RJ-45 10/100 switching modules might occasionally send signals with long rise and fall times. The rise and fall times need to be shortened although testing shows that the existing signals are clear enough to be received correctly. (CSCdr39256)
- The **set/clear cops domain-name** commands might close Telnet sessions to the NMP. When the **set cops domain-name** command is run over a Telnet session to the NMP, the Telnet session might get terminated with a **connection lost** message. This could also happen with commands such as **set qos enable/disable** or **set/clear port cops roles** if the QoS policy source is set to COPS. (CSCdr54368)

  Note CSCdr54368 has not been seen in later releases.

- If there are no COPS policies defined on the COPS server and a Catalyst switch attempts to make a COPS DS connection to the COPS server, then local QoS policies will be applied or the NMP on the switch might experience a reset. The workaround is to define COPS DS policies on the COPS server before attempting to connect any devices to it. (CSCdr43041, CSCdr60174, CSCdr61165)

  Note CSCdr43041, CSCdr60174, and CSCdr61165 have not been seen in later releases.

- When enabling port security on a port, connectivity for that port gets broken. Although there is continuous traffic coming into the port, nothing gets through and no address is being secured. No static entry is present. As soon as port security is disabled on the port, a MAC address is dynamically learned and connectivity is reestablished. (CSCdr53893)

  Note This problem has not been seen in later releases.

- 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 6.1(1a)

This section describes resolved caveats in supervisor engine software release 6.1(1a):

- Online diagnostic failures are experienced on modules during boot up, online insertion, or module reset if the QoS default-action MAC ACL is reconfigured 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. In general, as the rate value specified in the policer decreases, or the amount of traffic matching all ACLs specifying that aggregate policer increases. For switches with Supervisor Engine 2 and PFC2, this problem is resolved in software release 6.1(1a). (CSCdp15471)
- Rapidly disabling and enabling QoS with the policy source set to COPS might cause the switch to reset. The workaround is to wait approximately 30 seconds after disabling QoS before reenabling it when the QoS policy source had been set to COPS. This problem is resolved in software release 6.1(1a). (CSCdp32467)
- The hcRMONCapabilities MIB object is not supported in the supervisor engine RMON software. RMON applications such as TrafficDirector that depend on the hcRMONCapabilities MIB value, might fail to discover the HC-RMON capability of a device. This problem is resolved in software release 6.1(1a). (CSCdr89597)
- Occasionally, after a high-availability switchover, when you enter any of the **show qos** commands, you might receive incorrect output about the QoS/COPS ACL mappings. Your output might show that your switch has no QoS/COPS ACL mappings when the ACLs are actually in the hardware. This applies with either COPS or locally configured ACLs (IP, IPX, MAC) and policers. This condition continues until the COPS-DS client on the new active supervisor engine establishes connection to the PDP and downloads the QoS policy, or until the local QoS configuration is reinstalled in the CLI output structures. This problem is resolved in software release 6.1(1a). (CSCdp45099)

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 with Catalyst operating system 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 software while the system is running using the stateful supervisor 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 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 special case of incompatible versions. The high availability supervisor switchover is not available, but configuration changes to the NVRAM on the active supervisor can be synchronized to the standby supervisor. Therefore, it 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 6000 Family 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 and the supervisor in slot 2 in the standby mode:

Note You must have a console connection available for both supervisors 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, 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 12 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 for 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 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 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 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 6000 family switch configuration and is divided into the following subsections:

Note Refer to the *Release Notes for Catalyst 6000 Family 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 6000 Family Module Installation Guide*.
- The Catalyst 6000 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 such that it looks like many parallel strips across the top of the faceplate.

  When a module is inserted 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 card, 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 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 reenable 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 6000 family 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 6000 family 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 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 fwddelay** 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.

Use the following guidelines to debug STP problems:

- On a Catalyst 6000 family switch with default STP parameters:
  - 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+, 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 MISTP-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 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 the high-availability feature enabled).
  - With Supervisor Engine 1 configured for PVST+ or MISTP-PVST+, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 4000 (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.

Documentation Updates for Software Release 6.1

This section describes caveats for the Catalyst 6000 family software release 6.1 documentation. These changes will be included in the next update to the documentation.

- The *Catalyst 6000 Family Quick Software Configuration* publication incorrectly documents the **set port channel** command syntax. The command syntax is:

  set port channel *mod_num*/*port_num* mode {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

- Refer to the online version of the *Catalyst 6000 Family Command Reference Release 6.1* for information about the following two commands supported in software release 5.4(1) and later:

  set traffic monitor *threshold*
  show traffic

  Refer to the online version of the *System Message Guide—Catalyst 6000, 5000, 4000, 2948G, and 2926G and 2926 Series Switches* for releases 5.4, 5.5, and 6.1 for information about the following system log error messages:

  ```
  SYS-5-SYS_HITRFC:[dec] traffic load exceeded threshold on switching bus
  SYS-5-HITRFC3:[dec] traffic load exceeded threshold on switching bus [chars]
  SYS-3-SYS_MEMLOW:[chars][dec]
  SYS-3-SYS_MEMERR:Out of range while freeing address [chars]
  SYS-3-INBAND_NORESOURCE:Inband resource error warning [dec]
  SYS-3-INBAND_SPRINTR:inband spurious interrupt occurred [dec]
  SYS-3-PORT_ERR:port [dec]/[dec] swBusResultEvent [dec]
  SYS-3-PORT_WARN:port [dec]/[dec] dmaTxFull [dec] dmaRetry [dec]
  IP-3-UDP_SOCKOVFL:UDP socket overflow [dec]
  IP-3-TCP_SOCKOVFL:TCP socket overflow [dec]
  IP-3-UDP_BADCKSUM:UDP bad checksum [dec]
  IP-3-TCP_BADCKSUM:UDP bad checksum [dec]
  SPANTREE-5-PORTLISTEN:Port [dec]/[dec] state in vlan 1 changed to listening
  SPANTREE-5-TR_PORTLISTEN:Trcrf 101 in trbrf 102 state changed to listening
  ```

- The *Catalyst 6000 Family Software Configuration Guide Release 6.1*and the *Catalyst 6000 Family Command Reference Release 6.1* incorrectly omit the restriction that the **session** keyword for the **set port channel** command is supported only with Supervisor Engine 2 and PFC2.
- The *Catalyst 6000 Family Software Configuration Guide Release 6.1*, incorrectly lists the following two restrictions for aggressive UDLD:
  - When enabling aggressive UDLD, the recommended default is 30 seconds (this recommendation is invalid: the default is 15 seconds).
  - We recommend that you do not use UDLD or aggressive UDLD with the ON - AUTO trunk combination. UDLD and aggressive UDLD can be used with any other valid trunk combination (this recommendation is invalid: you can use UDLD or aggressive UDLD with the ON - AUTO trunk combination).

Additional Documentation

The following documents are available for the Catalyst 6000 family 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*
- *System Message Guide—Catalyst 6500 Series, Catalyst 4500 Series, 2948G, and 2980G Switches*
- *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/techsupport

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- 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 205.