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

Current Release
6.2(2)—June 12, 2001
Previous Releases: 6.1(4), 6.1(3), 6.1(2), 6.1(1d), 6.1(1c), 6.1(1b), 6.1(1a)

Note The most current version of these release notes can be found at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_11235.htm

Note 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 miminum boot ROM required for software release 6.2(2) and later releases is 6.1(3).

Note The supervisor engine boot ROM versions must be identical in redundant systems. For boot ROM upgrade information, refer to "Upgrading the Boot ROM on the Catalyst 6000 Family Supervisor Engine" at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_10142.htm

Note For information on the latest caveats and updates for the Cisco 7600 Optical Services Router (OSR), refer to the Cisco IOS Release 12.1(7a)E1 or later MSFC release notes at 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 75.

CISCO SYSTEMS

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

Contents

This document consists of these sections:

Release 6.*x* 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*.

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_2/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-S2-MSFC2	Supervisor Engine 2, dual 1000BASE-X GBIC uplinks, fabric-enabled[1], CEF, PFC2, and MSFC2 QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	6.1(1d)	6.1(4)
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)	6.1(4)
Supervisor Engine 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)	5.5(5)
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	5.5(5)
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	5.5(5)
WS-X6K-SUP1A-2GE	Supervisor Engine 1A, dual 1000BASE-X GBIC uplinks QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.3(1a)CSX	5.5(5)
WS-X6K-SUP1-2GE	Supervisor Engine 1, dual 1000BASE-X GBIC uplinks QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	5.5(5)
Switch Fabric Module			
WS-C6500-SFM	Switch Fabric Module to support fabric-enabled modules	6.1(1d)	6.1(4)
WS-X6500-SFM 2	Switch Fabric Module version 2	6.2(2)	6.2(2)
Ethernet, Fast Ethernet, and Gigabit Ethernet			
WS-X6516-GBIC	16-port Gigabit Ethernet GBIC switching module, fabric-enabled QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	6.1(1d)	6.1(4)
WS-X6416-GBIC	16-port Gigabit Ethernet GBIC switching module QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.4(2)	5.5(5)
WS-X6416-GE-MT	16-port Gigabit Ethernet MT-RJ QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.3(5a)CSX	5.5(5)
WS-X6316-GE-TX	16-port 1000BASE-TX RJ-45 Gigabit Ethernet QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.4(2)	5.5(5)
WS-X6408A-GBIC	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**	5.3(1a)CSX	5.5(5)

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-X6408-GBIC	8-port Gigabit Ethernet GBIC QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	5.5(5)
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)	5.5(5)
WS-X6224-100FX-MT	24-port 100FX Multimode MT-RJ QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	5.5(5)
WS-X6348-RJ-45 WS-X6348-RJ-45V	48-port 10/100TX 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: 5.5(5) With WS-F6K-VPWR: 5.5(5)
WS-F6K-VPWR	Inline-power field-upgrade module mounts on the 48-port 10/100TX RJ-45 module	5.5(1)	5.5(5)
WS-X6248-RJ-45	48-port 10/100TX RJ-45 QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.1(1)CSX	5.5(5)
WS-X6248A-TEL	48-port 10/100TX RJ-21 with 128K per-port packet buffers QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.3(2)CSX	5.5(5)
WS-X6248-TEL	48-port 10/100TX RJ-21 QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.2(1)CSX	5.5(5)
WS-X6024-10FL-MT	24-port 10BASE-FL MT-RJ QoS port architecture (Rx/Tx): **1q4t/2q2t**	5.3(3)CSX	5.5(5)
Voice Modules			
WS-X6224-FXS	24-port FXS analog interface module	5.5(1)	5.5(5)
WS-X6608-T1 WS-X6608-E1	8-port T1/E1 PSTN interface modules	5.5(1)	5.5(5)
FlexWan Module[2]			
WS-X6182-2PA	FlexWAN Module	5.4(2)	5.5(5)
Intrusion Detection System Module[3]			
WS-X6381-IDS	Intrusion Detection System Module	6.1(1d)	6.1(4)
Network Analysis Module[4]			
WS-X6380-NAM	Network Analysis Module	5.5(1)	5.5(5)
ATM[5]			
WS-X6101-OC12-SMF	Single-port single-mode OC-12 ATM	5.3(2)CSX	5.5(5)
WS-X6101-OC12-MMF	Single-port multimode OC-12 ATM	5.3(2)CSX	5.5(5)

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
Multilayer Switch Module (MSM)[6]			
WS-X6302-MSM	Multilayer Switch Module	5.2(1)CSX	5.5(5)
Optical Services Module[7]			
OSM-2OC12-POS-MM	2-port OC-12c/STM-4c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-2OC12-POS-SI	2-port OC-12c/STM-4c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-2OC12-POS-SL	2-port OC-12c/STM-4c POS Optical Services Module, SM-LR[8], with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-4OC12-POS-MM	4-port OC-12c/STM-4c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-4OC12-POS-SI	4-port OC-12c/STM-4c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-4OC12-POS-SL	4-port OC-12c/STM-4c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-8OC3-POS-MM	8-port OC-3c/STM-1c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-8OC3-POS-SI	8-port OC-3c/STM-1c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-8OC3-POS-SL	8-port OC-3c/STM-1c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-16OC3-POS-MM	16-port OC-3c/STM-1c POS Optical Services Module, MM, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-16OC3-POS-SI	16-port OC-3c/STM-1c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-16OC3-POS-SL	16-port OC-3c/STM-1c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(2)	6.1(4)
OSM-10C48-POS-SS	1-port OC-48c/STM-16c POS Optical Services Module, SM-SR, with 4 Gigabit Ethernet ports	6.1(3)	6.1(4)
OSM-10C48-POS-SI	1-port OC-48c/STM-16c POS Optical Services Module, SM-IR, with 4 Gigabit Ethernet ports	6.1(3)	6.1(4)
OSM-10C48-POS-SL	1-port OC-48c/STM-16c POS Optical Services Module, SM-LR, with 4 Gigabit Ethernet ports	6.1(3)	6.1(4)

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
Power Supplies			
WS-CAC-1000W	1000W AC power supply	5.1(1)CSX	5.5(5)
WS-CAC-1300W	1300W AC power supply	5.1(1)CSX	5.5(5)
WS-CDC-1300W	1300W DC power supply	5.1(1)CSX	5.5(5)
WS-CAC-2500W	2500W AC power supply	5.4(2)	5.5(5)
WS-CDC-2500W	2500W DC power supply	5.4(2)	5.5(5)
WS-CAC-4000W	4000W AC power supply	6.1(3)	6.1(4)
Modular Chassis			
WS-C6513	Catalyst 6513 chassis (13-slot)	6.2(2)	6.2(2)
WS-C6509	Catalyst 6509 chassis (9-slot)	5.1(1)CSX	5.5(5)
WS-C6509-NEB	Catalyst 6509-NEB chassis (9 vertically-oriented slots)	5.4(2)	5.5(5)
WS-C6009	Catalyst 6009 chassis (9-slot)	5.1(1)CSX	5.5(5)
WS-C6506	Catalyst 6506 chassis (6-slot)	5.2(1)CSX	5.5(5)
WS-C6006	Catalyst 6006 chassis (6-slot)	5.2(1)CSX	5.5(5)

1. Switch Fabric Module
2. Refer to the *Catalyst 6000 Family FlexWAN Module Installation and Configuration Note*
3. Refer to the *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note*
4. Refer to the *Network Analysis Module Installation and Configuration Note*
5. Refer to the *ATM Configuration Guide and Command Reference*
6. Refer to the *Multilayer Switch Module Release Notes*
7. Refer to the *Optical Services Module Installation and Configuration Note*
8. 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.

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number[1]
Supervisor Engine 2		
6.2(2) Flash image	cat6000-sup2.6-2-2.bin	SC6K-SUP2-6.2.2
6.2(2) Flash image (CiscoView)[2]	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)[2]	cat6000-sup2cvk9.6-2-2.bin	SC6K-SUP2CVK9-6.2.2
6.1(4) Flash image	cat6000-sup2.6-1-4.bin	SC6K-SUP2-6.1.4
6.1(4) Flash image (CiscoView)[2]	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)[2]	cat6000-sup2cvk9.6-1-4.bin	SC6K-SUP2CVK9-6.1.4
6.1(3) Flash image	cat6000-sup2.6-1-3.bin	SC6K-SUP2-6.1.3
6.1(3) Flash image (CiscoView)[2]	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)[2]	cat6000-sup2cvk9.6-1-3.bin	SC6K-SUP2CVK9-6.1.3
6.1(2) Flash image	cat6000-sup2.6-1-2.bin	SC6K-SUP2-6.1.2
6.1(2) Flash image (CiscoView)[2]	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)[2]	cat6000-sup2cvk9.6-1-2.bin	SC6K-SUP2CVK9-6.1.2
6.1(1d) Flash image	cat6000-sup2.6-1-1d.bin	SC6K-SUP2-6.1.1
6.1(1d) Flash image (CiscoView)[2]	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)[2]	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)[2]	cat6000-sup2cvk9.6-1-1c.bin	not orderable
6.1(1b) Flash image[3]	cat6000-sup2.6-1-1b.bin	not orderable
6.1(1b) Flash image (CiscoView)[2]	cat6000-sup2cv.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell[4])	cat6000-sup2k9.6-1-1b.bin	not orderable
6.1(1b) Flash image (Secure Shell and CiscoView)[2]	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[5])[2]	cat6000-sup2cv.6-1-1a.bin	not orderable
Supervisor Engine 1		
6.2(2) Flash image	cat6000-sup.6-2-2.bin	SC6K-SUP-6.2.2
6.2(2) Flash image (CiscoView)[2]	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)[2]	cat6000-supcvk9.6-2-2.bin	SC6K-SUPCVK9-6.2.2
6.1(4) Flash image	cat6000-sup.6-1-4.bin	SC6K-SUP-6.1.4
6.1(4) Flash image (CiscoView)[2]	cat6000-supcv.6-1-4.bin	SC6K-SUPCV-6.1.4

Table 2 Orderable Software Images (continued)

Software Version	Filename	Orderable Product Number[1]
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)[2]	cat6000-supcvk9.6-1-4.bin	SC6K-SUPCVK9-6.1.4
6.1(3) Flash image	cat6000-sup.6-1-3.bin	SC6K-SUP-6.1.3
6.1(3) Flash image (CiscoView)[2]	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)[2]	cat6000-supcvk9.6-1-3.bin	SC6K-SUPCVK9-6.1.3
6.1(2) Flash image	cat6000-sup.6-1-2.bin	SC6K-SUP-6.1.2
6.1(2) Flash image (CiscoView)[5,2]	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)[5,2]	cat6000-supcvk9.6-1-2.bin	SC6K-SUPCVK9-6.1.2
6.1(1c) Flash image (Secure Shell)	cat6000-supk9.6-1-1c.bin	SC6K-SUPK9-6.1.1
6.1(1c) Flash image (Secure Shell and CiscoView)[2]	cat6000-supcvk9.6-1-1c.bin	SC6K-SUPCVK9-6.1.1
6.1(1b) Flash image	cat6000-sup.6-1-1b.bin	not orderable
6.1(1b) Flash image (CiscoView)[6,2]	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)[5,2]	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[4])[2]	cat6000-supcv.6-1-1a.bin	not orderable

1. Installed on System; append with "=" for spare on floppy media.
2. CiscoView images are available approximately 2 weeks after the flash images are released.
3. Software release 6.1(1b) contains the fix for CSCds67513.
4. This release has been deferred due to caveat CSCds85763.
5. The 6.1(1a) CiscoView (CV) release and later releases require JPI (Java Plug-in) 1.3 in the browser. This release is incompatible with the 5.5(3) CV and earlier releases that require JPI 1.2.2. See the "Usage Guidelines and Restrictions" section on page 22 for caveats associated with JPI 1.3.
6. The cat6000-supcv.6-1-1.bin and cat6000-supcv.6-1-2.bin images are affected by CSCdu25881. See the "Open and Resolved Caveats in Software Release 6.1(2)" section on page 42 for more information about CSCdu25881.

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)

- Supervisor Engine 2
  - 6.1(3) and 6.1(4)

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)

Note 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 6.2

These sections describe the features in software release 6.2:

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

Software Release 6.2 Hardware Features

Software release 6.2 provides initial support for these modules:

- WS-C6513
  Catalyst 13-slot chassis

- WS-X6500-SFM 2
  Switch Fabric Module version 2

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.

- Muticast 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 13
- Software Release 6.1 Software Features, page 14

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 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
- 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 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.
- 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.
  - IOS ACLs that are mapped to a primary VLAN will get mapped to the associated secondary VLANs.
  - 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.
- IOS-like ping—The **-s** argument in the 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 15
- Software Release 5.5 Software Features, page 16

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 10/100TX 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

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 10/100TX 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 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:

- 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:

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 miminum boot ROM required for software release 6.2(2) and later releases is 6.1(3).
- IPX Layer 3 switched traffic with an encapsulation change from Service Advertisement Protocol (SAP) to non-SAP 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 rare corner cases, 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:

- 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 10/100TX 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 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)

Quality of Service

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

- 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, a Gigabit EtherChannel can contain ports with both strict-priority queues and ports without strict-priority queues. With QoS enabled, a Gigabit EtherChannel cannot contain both port types. If you enable QoS, ports drop out of any Gigabit 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 protocls and traffic on the switch:

- 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.
- In rare circumstances, multicast traffic might be blocked due to a mismatch between hardware and software entries. (CSCdp81324)

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)

Access Control

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

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

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

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

  The VACL description is as follows:

  – 1, 2. Allow IPX between client and server.

  – 3. The router needs to see the RIP/SAP packets.

  – 4. If packets are dropped during a connection, the client tries to find another route to the server by sending out RIP requests to IPX network 0.ffff.ffff.ffff. Not doing this results in a lost connection after packet drop.

  – 5. Upon startup, a client sends its first packets to 0.ffff.ffff.ffff and uses 0.ffff.ffff.ffff as its one IPX address.

  – 6. When a server connection socket is timed out, the client reconnects by sending a request to its local network to find its server.

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

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

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

High Availability

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

- 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)

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/mib

- 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 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 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)

CiscoView

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

CiscoView Images

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

- The supported client platform/browser/plugin 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 plugin/browser on the client machine.
- If CiscoView does not work after resizing the browser window on 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)

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), page 30
- Resolved Caveats in Software Release 6.2(2), page 33

Open Caveats in Software Release 6.2(2)

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

- The Catalyst 6000 CiscoView (CV) images do not support the Carrier Alarm Led for WAN modules. (CSCdt52011)
- If you configure the switch using the Catalyst 6000 CiscoView (CV) images, you may be unable to delete a primary VLAN after unbinding the secondary VLAN.

  Workaround: 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
  ```

  Workaround: Close and reopen the dialog and the correct error message will display. (CSCdt65530)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to create a policy name and then try to delete the policy name, the following incorrect error message appears:

  ```
  Unable to set row status
  ```

  (CSCdu11333)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to add an IP ACL, then select the **Add/Edit ACE** option, select an entry and make some changes, and then either click **Cancel** or **OK** ,and the configuration fails due to misconfigurations when you select **OK**, the previously entered values will appear as defaults when you attempt to edit your configuration.

  Workaround: you can overwrite the values in the fields if necessary.

  (CSCdu05678 and CSCdu15066)
- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management to add or edit an IP/IPX/MAC ACL, no buttons are available to move ACE entries up and down.

Workaround: Select the entry that needs to be moved and click on **Edit** and select **OK**. This entry is then moved to the bottom of the ACE list. (CSCdu64023)

- With the Catalyst 6000 CiscoView (CV) images, if you use QoS Device Management and select **Policy Selection** then **Add/Edit Policies** >**Change** then select a policy and click OK, selecting **Cancel** when the confirmation window displays will not cancel the operation. The policy will still be added to the Policy Selection.

  Workaround: Delete the policy selection entry that was added.

  (CSCdu43690)

- With the Catalyst 6000 CiscoView (CV) images, if you select **Configure** >**Interface** all fields show as N/A or with wrong values for the MultiChannel DS3 PA installed on a WS-X6182-PA module. (CSCdr39591)
- 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. (CSCdu25856)
- 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)
- ATM traffic is not forwarded through a WS-X6101 module after the module is reset. (CSCdu11300)
- 802.1x configuration allows incorrect command syntax. (CSCdu27021)
- WCCP Layer 2 redirection and IOS Firewall cannot be enabled at the same time on systems with Supervisor Engine 2 systems running supervisor engine software release 6.2(2) and IOS release 12.1(6)E1 through 12.1(7a)E1. The features work independently. (CSCdu25221)
- In a system with a Switch Fabric Module installed, the ACL capture feature does not work unless the one of the following conditions are met.

  – Traffic that is captured and exits on a nonfabric-enabled module port

  or

  – Traffic that 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)

- 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)
- 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 port status as "not-connected." This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays "Compact mode" for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics and fails to come online following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- 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)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
  - A 64-byte packet should be counted as 4 but is counted as 3
  - 65- to 79-byte packets are correctly counted as 4
  - An 80-byte packet should be counted as 5 but is counted as 4
  - 81- to 95-byte packets are correctly counted as 5
  - A 96-byte packet should be counted as 6 but is counted as 5

  (CSCdr56784)
- If you download a COPS ACL containing a policer to the switch and the switch cannot support the exact rate/burst supplied by the policer, no message informs you that the rate/burst was rounded off to the nearest value that the hardware could support. (CSCdr28715)
- If 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)
- 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 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)
- 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 the with 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 CiscoView browser window on a Solaris/Netscape Communicator client with Java plugin 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 an ISL trunk port is connected 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 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(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 34
- Resolved Caveats in Software Release 6.1(4), page 36

Open Caveats in Software Release 6.1(4)

This section describes open caveats in supervisor engine software release 6.1(4):

- 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)
- 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 an ISL trunk port is connected 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)
- On the 24-port FXS analog interface module (WS-X6624-FXS), the **show spantree** command displays port status as "not-connected." This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays "Compact mode" for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
  - A 64-byte packet should be counted as 4 but is counted as 3
  - 65- to 79-byte packets are correctly counted as 4
  - An 80-byte packet should be counted as 5 but is counted as 4
  - 81- to 95-byte packets are correctly counted as 5
  - A 96-byte packet should be counted as 6 but is counted as 5

  (CSCdr56784)
- 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)
- 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)
- 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 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)

- 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 circumtances 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(3)

These sections describe open and resolved caveats in supervisor engine software release 6.1(3):

- Open Caveats in Software Release 6.1(3), page 36
- Resolved Caveats in Software Release 6.1(3), page 38

Open Caveats in Software Release 6.1(3)

This section describes open caveats in supervisor engine software release 6.1(3):

- The CiscoView that is embedded in the cat6000-supcv_6-1-1b.bin and cat6000-supcv_6-1-2.bin images no longer works 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)

- 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)
- When an ISL trunk port is connected 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 port status as "not-connected." This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays "Compact mode" for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
  - A 64-byte packet should be counted as 4 but is counted as 3
  - 65- to 79-byte packets are correctly counted as 4
  - An 80-byte packet should be counted as 5 but is counted as 4
  - 81- to 95-byte packets are correctly counted as 5
  - A 96-byte packet should be counted as 6 but is counted as 5

  (CSCdr56784)
- 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)
- 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)

- 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 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)
- 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 IOS release 12.1(4)E2 are reset every 9 minutes by the Supervisor Engine 2. This problem is resolved in IOS releases 12.1(5a)E3 and later. (CSCdt02646)
- WS-X6101 ATM modules running IOS release 12.1(5a)E3 do not support high availability for Supervisor Engine 2. This problem is resolved in IOS releases 12.1(6)E and later. (CSCdt29354)
- If you configure large IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same IOS ACL and share the same label before might not be able to do so any more. As a result the 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

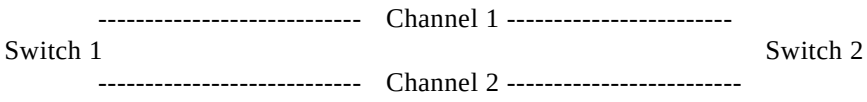
  If the multicast receiver sends an IGMPv2 leave for a multicast group, the IGMPv2 leave is forwarded to the external router which responds with a group-specific query. Switch A then forwards this query to Switch B, which starts to build a "MAC-based" general query to determine if any additional receivers 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 crash 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 crash. 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 crash. 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)

- Very rarely, 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(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 42
- Resolved Caveats in Software Release 6.1(2), page 44

Open Caveats in Software Release 6.1(2)

This section describes open caveats in supervisor engine software release 6.1(2):

- 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.

- 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)
- VLAN 2035 cannot be used for a Voice VLAN due to an incorrect LTL index mapping. (CSCds64624)
- WS-X6101 ATM modules running IOS release 12.1(4)E2 are reset every 9 minutes by the Supervisor Engine 2. (CSCdt02646)
- WS-X6101 ATM modules running IOS release 12.1(5a)E3 do not support HA for Supervisor Engine 2. (CSCdt29354)
- When an ISL trunk port is connected 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 IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same IOS ACL and share the same label before might not be able to do so any more. As a result the 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 port status as "not-connected." This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays "Compact mode" for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets that have a size evenly divisible by 16:
  - A 64-byte packet should be counted as 4 but is counted as 3
  - 65- to 79-byte packets are correctly counted as 4
  - An 80-byte packet should be counted as 5 but is counted as 4
  - 81- to 95-byte packets are correctly counted as 5
  - A 96-byte packet should be counted as 6 but is counted as 5

  (CSCdr56784)
- The 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)
- 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; and as a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)
- 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)
- 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 there is an error in installing any COPS policy, a successful commit is sent to the PDP even though 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 with the error condition and might result in a switch reset. (CSCdp66572)
- 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 steps 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 spanntree** 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 re-enable 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 re-enable 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)
- Very rarely, 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 re-enabled. 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)
- Very rarely, 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. CSCdr 50405 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(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 50
- Resolved Caveats in Software Release 6.1(1d), page 52

Open Caveats in Software Release 6.1(1d)

This section describes open caveats in supervisor engine software release 6.1(1d):

- If you configure large IOS ACLs on the MSFC, after a redundant MSFC switchover or a supervisor engine high-availability switchover, interfaces that were configured with the same IOS ACL and share the same label before might not be able to do so any more. As a result the 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 an ISL trunk port is connected 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 port status as “not-connected.” This error does not affect operation. (CSCds00575)

- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays “Compact mode” for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets whose size is evenly divisible by 16:
  - A 64-byte packet should be counted as 4, but is counted as 3
  - 65- to 79-byte packets are correctly counted as 4
  - An 80-byte packet should be counted as 5, but is counted as 4
  - 81- to 95-byte packets are correctly counted as 5
  - A 96-byte packet should be counted as 6, but is counted as 5

  (CSCdr56784)
- The 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)
- 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, and as a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)
- 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)
- 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 there is an error in installing any COPS policy, a successful commit is sent to the PDP even though 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 with the error condition and might result in a switch reset. (CSCdp66572)
- 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

    or

  – 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 52
- Resolved Caveats in Software Release 6.1(1c), page 56

Open Caveats in Software Release 6.1(1c)

This section describes open caveats in supervisor engine software release 6.1(1c).

- 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 an ISL trunk port is connected 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)
- Very rarely, 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 port status as **not-connected**. This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays “Compact mode” for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- 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)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)

- The broadcast suppression counter undercounts packets whose size is 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
  - Etc.

  (CSCdr56784)
- 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)
- 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)

- The 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, and as a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)
- 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)
- When a Cisco IP Phone 7960 is connected 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 will remain up but the phone will be down. Note that 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)
- In some situations, if there is an error in installing any COPS policy, a successful commit is sent to the PDP even though the policy was not correctly installed. In such situations, any modifications to the port's role combination will not install the correct policy on the port with the error condition. This might result in a switch reset. (CSCdp66572)
- 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 Cisco 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), page 57
- Resolved Caveats in Software Release 6.1(1b), page 61

Open Caveats in Software Release 6.1(1b)

This section describes open caveats in supervisor engine software release 6.1(1b).

- 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 an ISL trunk port is connected 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)
- Very rarely, 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 port status as "not-connected." This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays "Compact mode" for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)
- 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)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets whose size is 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
  - Etc.

  (CSCdr56784)
- 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)
- 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)
- The 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, and as a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)
- 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)
- When a Cisco IP Phone 7960 is connected 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 will remain up but the phone will be down. Note that 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)
- In some situations, if there is an error in installing any COPS policy, a successful commit is sent to the PDP even though the policy was not correctly installed. In such situations, any modifications to the port's role combination will not install the correct policy on the port with the error condition. This might result in a switch reset. (CSCdp66572)
- 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 61
- Resolved Caveats in Software Release 6.1(1a), page 66

Open Caveats in Software Release 6.1(1a)

This section describes open caveats in supervisor engine software release 6.1(1a).

- 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 an ISL trunk port is connected 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)
- Very rarely, 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 port status as “not-connected.” This error does not affect operation. (CSCds00575)
- Entering the **show fabric channel switchmode** command in a switch that has all fabric-enabled switching modules displays “Compact mode” for all switching modules and a single-port OC-12 ATM module (WS-X6101-OC12-SMF or WS-X6101-OC12-MMF) fails diagnostics following online insertion. To put the ATM module into service, enter the **reset** *slot_number* command. (CSCds12349)

- 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)
- When you enable UplinkFast, the EtherChannel port path cost (set with the **set channel cost** command) for a four-port 10/100 EtherChannel is less than the port path cost of a parallel Gigabit Ethernet link. This situation causes the slower four-port EtherChannel to forward and the Gigabit Ethernet link to block. (CSCds22895)
- The broadcast suppression counter undercounts packets whose size is 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
  - Etc.

  (CSCdr56784)
- 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.

- 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)
- The 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, and as a result, there is no indication to the user that the WRED minimum specified in the COPS policy was not used. (CSCdr28819)
- 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)
- When a Cisco IP Phone 7960 is connected 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 will remain up but the phone will be down. Note that 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)
- 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.

- In some situations, if there is an error in installing any COPS policy, a successful commit is sent to the PDP even though the policy was not correctly installed. In such situations, any modifications to the port's role combination will not install the correct policy on the port with the error condition. This might result in a switch reset. (CSCdp66572)
- 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-availablility versioning, you can have active and standby supervisor engines run different images as long as both images are release 5.4(1)or later.

The high availability versioning feature and Catalyst software upgrade should only be used when applying a maintenance release of CatOS 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 7 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 Clear the current boot variable.

```
Console_A> (enable) clear boot system all
```

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 system boot flash bootflash:cat6000-sup2.old.bin
```

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 20,000 (with or without the high availability feature enabled).
- With Supervisor Engine 2 configured for PVST+ and MISTP, ensure that the sum of the logical ports across all instances of spanning tree for different VLANs does not exceed 12,000 (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 50,000 (40,000 without HA).
- With Supervisor Engine 1 configured for PVST+ or PVST+ and MISTP, 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 or channels on the switch times the number of active VLANs on that trunk, 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 6000 Family Quick Software Configuration*
- *Catalyst 6000 Family Installation Guide*
- *Catalyst 6000 Family Module Installation Guide*
- *Catalyst 6000 Family Software Configuration Guide*
- *Catalyst 6000 Family Command Reference*
- *System Message Guide—Catalyst 6000 Family, 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980G Switches*
- *ATM Configuration Guide and Command Reference*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered CCO users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the *Catalyst 6000 Family Software Configuration Guide* and the *Catalyst 6000 Family Command Reference* publications.