



Release Notes for Catalyst 4000 Family Software Release 4.x

Current Release

4.5(13a)—February 7, 2002

Previous Releases

4.5(13), 4.5(12a), 4.5(12), 4.5(11), 4.5(10), 4.5(9), 4.5(8), 4.5(7), 4.5(6a), 4.5(6), 4.5(5), 4.5(4), 4.5(3), 4.5(2), 4.5(1), 4.4(1)

These release notes describe the features, modifications, and caveats for Catalyst 4000 family supervisor engine software release 4.x and all 4.x maintenance releases. The current 4.x release is supervisor engine software release 4.5(13a). These release notes apply to Catalyst 4000 family switches as well as to Catalyst 2948G series and Catalyst 4912G series switches running Catalyst 4000 family supervisor engine software.



Note

Although the software image in a new Catalyst 4000 family switch operates correctly, later software images containing the latest upgrades and modifications are released regularly to provide you with the most optimized software available. We strongly recommend that you check for the latest released software images at the World Wide Web locations listed in the [“Cisco.com” section on page 37](#).



Note

Release notes for prior Catalyst 4000 family software releases were accurate at the time of release. However, for information on the latest caveats and updates to previously released Catalyst 4000 family software releases, refer to the release notes for the latest maintenance release in your software release train. You can access all Catalyst 4000 family release notes at the World Wide Web locations listed in the [“Cisco.com” section on page 37](#).



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). Use 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.

Contents

This document consists of these sections:

- [Release 4.x Memory Requirements, page 2](#)
- [Product and Software Version Matrix, page 3](#)
- [Orderable Software Images, page 4](#)
- [New Features for Supervisor Engine Software Release 4.5, page 4](#)
- [New Features for Supervisor Engine Software Release 4.4, page 5](#)
- [Open and Resolved Caveats in Software Release 4.5\(13a\), page 5](#)
- [Open and Resolved Caveats in Software Release 4.5\(13\), page 6](#)
- [Open and Resolved Caveats in Software Release 4.5\(12a\), page 6](#)
- [Open and Resolved Caveats in Software Release 4.5\(12\), page 7](#)
- [Open and Resolved Caveats in Software Release 4.5\(11\), page 7](#)
- [Open and Resolved Caveats in Software Release 4.5\(10\), page 8](#)
- [Open and Resolved Caveats in Software Release 4.5\(9\), page 9](#)
- [Open and Resolved Caveats in Software Release 4.5\(8\), page 10](#)
- [Open and Resolved Caveats in Software Release 4.5\(7\), page 11](#)
- [Open and Resolved Caveats in Software Release 4.5\(6a\), page 12](#)
- [Open and Resolved Caveats in Software Release 4.5\(6\), page 13](#)
- [Open and Resolved Caveats in Software Release 4.5\(5\), page 15](#)
- [Open and Resolved Caveats in Software Release 4.5\(4\), page 16](#)
- [Open and Resolved Caveats in Software Release 4.5\(3\), page 18](#)
- [Open and Resolved Caveats in Software Release 4.5\(2\), page 20](#)
- [Open and Resolved Caveats in Software Release 4.5\(1\), page 22](#)
- [Open Caveats in Software Release 4.4\(1\), page 27](#)
- [Usage Guidelines, Restrictions, and Troubleshooting, page 30](#)
- [Documentation Updates for Software Release 4.4, page 35](#)
- [Additional Documentation, page 36](#)
- [Obtaining Documentation, page 36](#)
- [Obtaining Technical Assistance, page 37](#)

Release 4.x Memory Requirements

The 4.x Catalyst 4000 family supervisor engine software releases require a minimum of 32-MB RAM installed on your supervisor engine.

Product and Software Version Matrix

This section contains configuration matrixes to help you order Catalyst 4000 family products. [Table 1](#) lists the minimum supervisor engine version and the current recommended and default supervisor engine version for Catalyst 4000 family modules and chassis.

Table 1 Product and Software Version Matrix

Product Number (append with "=" for spares)	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
Supervisor Engine			
WS-X4012	Catalyst 4000 family Supervisor Engine I module	4.4(1)	4.5(13a)
Ethernet, Fast Ethernet, and Gigabit Ethernet			
WS-X4148-RJ	48-port 10/100 Fast Ethernet RJ-45	4.4(1)	4.5(13a)
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet		
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet	4.4(1)	4.5(13a)
WS-X4418-GB	18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet	4.5(1)	4.5(13a)
Gigabit Interface Converters (GBICs)			
WS-G5484=	1000BASE-SX GBIC	4.4(1)	4.5(13a)
WS-G5486=	1000BASE-LX/LH GBIC		
WS-G5487=	1000BASE-ZX GBIC	4.5(1)	4.5(13a)
Modular Chassis			
WS-C4003	Catalyst 4003 chassis (3-slot)	4.4(1)	4.5(13a)
Fixed-Configuration Chassis			
WS-C2948G	Catalyst 2948G with 2 1000BASE-X (GBIC) Gigabit Ethernet uplinks and 48 10/100 Fast Ethernet ports	4.5(1)	4.5(13a)
WS-C4912G	Catalyst 4912G with 12 1000BASE-X (GBIC) Gigabit Ethernet ports	4.5(1)	4.5(13a)

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the supervisor engine software.

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
Supervisor Engine I			
4.4(1)	cat4000.4-4-1.bin	SFC4K-4.4.1	SFC4K-4.4.1=
4.5(1)	cat4000.4-5-1.bin	SFC4K-4.5.1	SFC4K-4.5.1=
4.5(2)	cat4000.4-5-2.bin	SFC4K-4.5.2	SFC4K-4.5.2=
4.5(3)	cat4000.4-5-3.bin	SFC4K-4.5.3	SFC4K-4.5.3=
4.5(4)	cat4000.4-5-4.bin	SFC4K-4.5.4	SFC4K-4.5.4=
4.5(5)	cat4000.4-5-5.bin	SFC4K-4.5.5	SFC4K-4.5.5=
4.5(6a)	cat4000.4-5-6a.bin	SFC4K-4.5.6a	SFC4K-4.5.6a=
4.5(6)	cat4000.4-5-6.bin	SFC4K-4.5.6	SFC4K-4.5.6=
4.5(7)	cat4000.4-5-7.bin	SFC4K-4.5.7	SFC4K-4.5.7=
4.5 (8)	cat4000.4.5-8.bin	SFC4K-4.5.8	SFC4K-4.5.8=
4.5 (9)	cat4000.4.5-9.bin	SFC4K-4.5.9	SFC4K-4.5.9=
4.5 (10)	cat4000.4.5-10.bin	SFC4K-4.5.10	SFC4K-4.5.10=
4.5 (11)	cat4000.4.5-11.bin	SFC4K-4.5.11	SFC4K-4.5.11=
4.5 (12)	cat4000.4.5-12.bin	SFC4K-4.5.12	SFC4K-4.5.12=
4.5 (12a)	cat4000.4.5-12a.bin	SFC4K-4.5.12a	SFC4K-4.5.12a=
4.5 (13)	cat4000.4.5-13.bin	SFC4K-4.5.13	SFC4K-4.5.13=
4.5 (13a)	cat4000.4.5-13a.bin	SFC4K-4.5.13a	SFC4K-4.5.13a=

New Features for Supervisor Engine Software Release 4.5

This section describes the new features available in Catalyst 4000 family software release 4.5.

- Catalyst 4912G switch (WS-C4912)—The Catalyst 4912G switch is a fixed-configuration Gigabit Ethernet switch with 12 1000BASE-X Gigabit Interface Converter (GBIC) Gigabit Ethernet ports.
- 18-port server switching 1000BASE-X Gigabit Ethernet (WS-X4418-GB)—Catalyst 4000 family switching module with 2 1000BASE-X (GBIC) Gigabit Ethernet ports and 16 oversubscribed Gigabit Ethernet ports.
- 1000BASE-ZX GBIC (WS-G5487=)—Hot-swappable GBIC supporting Gigabit Ethernet transmission over distances up to 55 miles (90 km).

New Features for Supervisor Engine Software Release 4.4

This section describes the new features available in Catalyst 4000 family software release 4.4.

- Catalyst 4003 switch (WS-C4003)—Three-slot modular Gigabit Ethernet switch with optional redundant power supplies.
- Catalyst 4000 family Supervisor Engine I (WS-X4012)—Supervisor engine module for the Catalyst 4000 family switches.
- 6-port 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4306-GB)—Catalyst 4000 family switching module with six 1000BASE-X (GBIC) Gigabit Ethernet ports.
- 32-port 10/100 Fast Ethernet, plus two-port 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4232-GB-RJ)—Catalyst 4000 family switching module with 32 RJ-45 10/100 Fast Ethernet ports and two 1000BASE-X (GBIC) Gigabit Ethernet ports.
- 48-port 10/100 Fast Ethernet module (WS-X4148-RJ)—Catalyst 4000 family switching module with 48 RJ-45 10/100 Fast Ethernet ports.
- Catalyst 2948G switch (WS-C2948)—Fixed-configuration Gigabit Ethernet switch with 48 10/100-Mbps Fast Ethernet ports and two 1000BASE-X (GBIC) Gigabit Ethernet uplink ports.

Open and Resolved Caveats in Software Release 4.5(13a)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(13a):

- [Open Caveats in Software Release 4.5\(13a\), page 5](#)
- [Resolved Caveats in Software Release 4.5\(13a\), page 5](#)

Open Caveats in Software Release 4.5(13a)

There are no open caveats in Catalyst 4000 family software release 4.5(13a).

Resolved Caveats in Software Release 4.5(13a)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(13a).

- An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw67458>

This problem is resolved in software release 4.5(13a). (CSCdw67458)

- Some Cisco Catalyst switches, running certain Catalyst OS software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to crash and result in a switch reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack.

This vulnerability is documented as Cisco bug ID CSCdw19195. There are workarounds available to mitigate the vulnerability.

This advisory will be posted at this URL:

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

The following workarounds can be implemented.

- If ssh is available in the code base use ssh instead of Telnet and disable Telnet.

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

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

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

This problem is resolved in software release 4.5(13a). (CSCdw19195)

Open and Resolved Caveats in Software Release 4.5(13)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(13):

- [Open Caveats in Software Release 4.5\(13\), page 6](#)
- [Resolved Caveats in Software Release 4.5\(13\), page 6](#)

Open Caveats in Software Release 4.5(13)

There are no open caveats in Catalyst 4000 family software release 4.5(13).

Resolved Caveats in Software Release 4.5(13)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(13).

- 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. This problem is resolved in software release 4.5(13). (CSCdu10858)
- RMON history, events, and alarm entries are not saved after reloading a software image. This problem is resolved in software release 4.5(13). (CSCdu26550)

Open and Resolved Caveats in Software Release 4.5(12a)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(12a):

- [Open Caveats in Software Release 4.5\(12a\), page 6](#)
- [Resolved Caveats in Software Release 4.5\(12a\), page 7](#)

Open Caveats in Software Release 4.5(12a)

There are no open caveats in Catalyst 4000 family software release 4.5(12a).

Resolved Caveats in Software Release 4.5(12a)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(12a).

- An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw67458>

This problem is resolved in software release 4.5(12a). (CSCdw67458)

Open and Resolved Caveats in Software Release 4.5(12)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(12):

- [Open Caveats in Software Release 4.5\(12\), page 7](#)
- [Resolved Caveats in Software Release 4.5\(12\), page 7](#)

Open Caveats in Software Release 4.5(12)

There are no open caveats in Catalyst 4000 family software release 4.5(12).

Resolved Caveats in Software Release 4.5(12)

There are no resolved caveats in Catalyst 4000 family software release 4.5(12).

Open and Resolved Caveats in Software Release 4.5(11)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(11):

- [Open Caveats in Software Release 4.5\(11\), page 7](#)
- [Resolved Caveats in Software Release 4.5\(11\), page 7](#)

Open Caveats in Software Release 4.5(11)

There are no open caveats in Catalyst 4000 family software release 4.5(11).

Resolved Caveats in Software Release 4.5(11)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(11).

- If the **show crashdump mod** command is entered on a switch that has not crashed in the past, the switch may crash. The workaround is to avoid entering the **show crashdump mod** command in releases that are affected by this caveat. This problem is resolved in software release 4.5(11). (CSCds37453)

- Very rarely a switch might reset under a heavy load. To determine whether the reset is due to this rare condition, enter the **show crashdump 1** command after the switch reboots. If you observe that the switch crashed in Connection_onAckTimeout (a procedure in the image), you are probably experiencing this problem. This problem is resolved in software release 4.5(11). (CSCds84051)
- When a 10/100-Mbps port receives a runt packet (a packet of less than 64 bytes that has an FCS error), both the runt counter and the FCS-error counter are incremented. According to IEEE 802.3, undersized packets should not increment any other error counters, and each packet should typically be represented by a single counter. As a result, runt packets should be counted solely as runts and not as FCS-errors. CRC errors, alignment errors, jabbers, and fragments are now counted and displayed correctly. This problem is resolved in software release 4.5(11). (CSCdt15053)

Open and Resolved Caveats in Software Release 4.5(10)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(10):

- [Open Caveats in Software Release 4.5\(10\), page 8](#)
- [Resolved Caveats in Software Release 4.5\(10\), page 8](#)

Open Caveats in Software Release 4.5(10)

This section describes the open caveats in Catalyst 4000 family software release 4.5(10).

- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)

Resolved Caveats in Software Release 4.5(10)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(10).

- A series of unauthenticated Telnet attempts can cause the switch to fail to pass traffic or accept management connections until the system is rebooted or a power cycle is performed. This problem is resolved in software release 4.5(10). (CSCds66191)
- If a reverse Telnet session to the switch times out, press the space bar to reactivate the session, and you will be able to see the configuration of the switch. This situation affects the Catalyst 4000 family modules with a console port connected to a modem, communication server, or PC. This problem is resolved in software release 4.5(10). (CSCds08837)
- Non-alphanumeric characters are not valid in VTP domain names, but can be configured in certain cases. This problem is resolved in software release 4.5(10). (CSCds34927)
- To avoid high CPU utilization when using the **show logging buffer** command, do not display more than 20 messages when the screen length is set to 0, or more than 24 when using the **set length** command. This problem is resolved in software release 4.5(10). (CSCds05287)

- An incorrect value might be returned when SNMP uses `vlanTrunkPortVlansEnabled` to display VLANs enabled on the trunking ports. This problem is resolved in software release 4.5(10). (CSCds44309)
- The switch resets with a TLB exception when using the **show flash tftp: chips** command. This problem is resolved in software release 4.5(10). The system now returns a response indicating that the **chips** option is not valid with the **tftp:** option. (CSCds64917)
- When “.” is used as a filename for **copy** or **show file** commands, the system might reset. This problem is resolved in software release 4.5(10). (CSCds54945)

Open and Resolved Caveats in Software Release 4.5(9)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(9):

- [Open Caveats in Software Release 4.5\(9\), page 9](#)
- [Resolved Caveats in Software Release 4.5\(9\), page 9](#)

Open Caveats in Software Release 4.5(9)

This section describes the open caveats in Catalyst 4000 family software release 4.5(9).

- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the `portOperTxFlowControl` and `portOperRxFlowControl` objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)
- If a reverse Telnet session to the switch times out, press the space bar to reactivate the session, and you will be able to see the configuration of the switch. This situation affects the Catalyst 4000 family modules with a console port connected to a modem, communication server, or PC. This problem is resolved in software release 4.5(10). (CSCds08837)

Resolved Caveats in Software Release 4.5(9)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(9).

- SNMP requests for specific dynamically learned MAC addresses returns the same information as if the MAC address has never been learned by the switch. (CSCdr09715)
- The switch might display “Out of memory” messages, which causes VMPS to become inactive. This situation could be due to duplicate MAC addresses in the VMPS database. The workaround is to reboot the switch. This problem is resolved in software release 5.5(3). (CSCdr95115)
- When a Catalyst 4000 family or 2948G series has a large number (greater than 5000) of active paths, packets sometimes get reordered. An active path is a SA, DA pair. Reordered packets may cause SNA sessions to drop. There is no workaround. (CSCdr68833)
- In the presence of loopback cabling on ports forced to half-duplex mode, particular traffic patterns may cause the following message to be generated (CSCdr77637):

```
2000 Jun 02 00:20:30 cet +02:00 %SYS-4-P2_WARN:1/Blocked queue on gigaport 2
```

Open and Resolved Caveats in Software Release 4.5(8)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(8):

- [Open Caveats in Software Release 4.5\(8\), page 10](#)
- [Resolved Caveats in Software Release 4.5\(8\), page 10](#)

Open Caveats in Software Release 4.5(8)

This section describes open caveats in Catalyst 4000 family software release 4.5(8).

- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)

Resolved Caveats in Software Release 4.5(8)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(8).

- The Catalyst 4000 is unable to resolve DNS names if the DNS has more than 7 entries. This problem is resolved in software releases 4.5(8) and 5.5(2). (CSCdr808353)
- If you connect a Supervisor Engine III running software version 4.5 through Telnet and from there connect to another device through Telnet, displaying a large list or file can cause the Telnet session to hang. This problem is resolved in software releases 4.5(8), 5.4(4), and 5.5(2). (CSCdm79404, CSCdr40184)
- When large amounts of data are being displayed during a Telnet session, the Telnet session will sometimes hang. This usually happens if you have set the screen length to 0 and long **show** commands are being displayed or if you have cut and pasted several **show** commands onto the window.

The workaround for this problem is to avoid using cut and paste in a Telnet session and setting the screen length to nonzero. This problem is resolved in software releases 4.5(8), 5.4(4), and 5.5(2). (CSCdp47176, CSCdr40184)

- The statistics for transmitted broadcast packets are not correct on 10/100 ports. Broadcast packets received by the switch on a 10/100 port are counted both in the receive and the transmit statistics. Packets are forwarded correctly. (CSCdr51233)
- The GBIC type is reported as “unknown” for some SX GBICs. Port operation is not affected. (CSCdr52518)
- An invalid packet with a length less than 64 bytes received on a 10/100 port will cause both the Runts and FCS-Error counters to increment on the port. In order to determine the actual number of FCS-Errors on valid length packets received on the port, subtract the value of the port Runts counter from the value of the port FCS-Error counter. (CSCdr37645)
- In the presence of loopback cabling on ports forced to half-duplex mode, related ports may experience permanent receive or transmit failure. (CSCdp68027)

- A system reset might occur during SNMP polling of the switch ports (SWPoll64bCnt) if a module goes on- and offline frequently. This problem is resolved in software releases 4.5(8) and 5.4(3). (CSCdr41609)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- The Catalyst 2948G switch and Catalyst 4000 family switches may display this message:

```
2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Internal Event: ScxSwitchMan - ProtocolTable
Packet on address 00:00:01:76:01:00 arrived on unexpected port 2/37.
```

For more information on this error message, capture the output from the following commands *before you reset the switch* and provide this information to your TAC representative:

- **show ebminterposition 1**
- **show interposition 1**
- **show swinterposition 1**
- **path find 1 <dest-mac-addr>**

<dest-mac-addr> is the address in the error message.

- **show health 1**

After upgrading to software release 4.5(8), this error message is displayed:

```
Blocked queue on gigaport 4, ( 0 :10 )
```

For more information on this error message, capture the output from the following commands *before you reset the switch* and provide this information to your TAC representative:

(CSCdp93187)

Open and Resolved Caveats in Software Release 4.5(7)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(7):

- [Open Caveats in Software Release 4.5\(7\), page 11](#)
- [Resolved Caveats in Software Release 4.5\(7\), page 12](#)

Open Caveats in Software Release 4.5(7)

This section describes open caveats in Catalyst 4000 family software release 4.5(7).

- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)

- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key . (CSCdm11604)

- The Catalyst 2948G switch and Catalyst 4000 family switches may display this message:

```
2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Internal Event: ScxSwitchMan - ProtocolTable
Packet on address 00:00:01:76:01:00 arrived on unexpected port 2/37.
```

For more information on this error message, capture the output from the following commands *before you reset the switch* and provide this information to your TAC representative:

- **show ebminterposition 1**
- **show interposition 1**
- **show swinterposition 1**
- **path find 1 <dest-mac-addr>**
<dest-mac-addr> is the address in the error message.
- **show health 1**

(CSCdp93187)

Resolved Caveats in Software Release 4.5(7)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(7).

- If you save a configuration file from a switch, and then apply the saved configuration file to that same switch, it is safe to ignore messages about TRBRF and TRCRF VLANs. These messages are caused by the default Token Ring VLAN configuration, which is always present regardless of the specific configuration of the switch. This problem is resolved in software release 4.5(7). (CSCdm92714)
- After closing a Telnet session, the switch still shows the session as open. Using the **disconnect ip_address** command to disconnect a user and manually close the session does not close the session. This problem is resolved in software release 4.5(7). (CSCdp33649)

Open and Resolved Caveats in Software Release 4.5(6a)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(6a):

- [Open Caveats in Software Release 4.5\(6a\), page 12](#)
- [Resolved Caveats in Software Release 4.5\(6a\), page 13](#)

Open Caveats in Software Release 4.5(6a)

This section describes open caveats in Catalyst 4000 family software release 4.5(6a).

- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)

- The 2948G and 4000 family switches display this message:

```
2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Internal Event: ScxSwitchMan - ProtocolTable
Packet on address 00:00:01:76:01:00 arrived on unexpected port 2/37.
```

To provide more information on this error message, the development engineer will add a dump in software release 4.5(6), 5.4(2), and 6.2(1).

If you are on a switch that receives this message, capture the output from the following commands *before you reset the switch*.

- **show ebminterposition 1**
- **show interposition 1**
- **show swinterposition 1**
- **path find 1 <dest-mac-addr>**
<dest-mac-addr> is the address in the error message.
- **show health 1**

If you (TAC) can get into engineering mode, use **lcp 1 show vbuf**. (CSCdp93187)

- If you save a configuration file from a switch, and then apply the saved configuration file to that same switch, it is safe to ignore messages about TRBRF and TRCRF VLANs. These messages are caused by the default Token Ring VLAN configuration, which is always present regardless of the specific configuration of the switch. (CSCdm92714)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)
- After closing a Telnet session, the switch still shows the session as open. Using the **disconnect ip_address** command to disconnect a user and manually close the session does not close the session. (CSCdp33649)

Resolved Caveats in Software Release 4.5(6a)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(6a).

- An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw67458>

This problem is resolved in software release 4.5(6a). (CSCdw67458)

Open and Resolved Caveats in Software Release 4.5(6)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(6):

- [Open Caveats in Software Release 4.5\(6\), page 14](#)
- [Resolved Caveats in Software Release 4.5\(6\), page 14](#)

Open Caveats in Software Release 4.5(6)

This section describes open caveats in Catalyst 4000 family software release 4.5(6).

- The 2948G and 4000 family switches display this message:

```
2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Internal Event: ScxSwitchMan - ProtocolTable
Packet on address 00:00:01:76:01:00 arrived on unexpected port 2/37.
```

To provide more information on this error message, the development engineer will add a dump in software release 4.5(6), 5.4(2), and 6.2(1).

If you are on a switch that receives this message, capture the output from the following commands *before you reset the switch*.

- **show ebminterposition 1**
- **show interposition 1**
- **show swinterposition 1**
- **path find 1 <dest-mac-addr>**
<dest-mac-addr> is the address in the error message.
- **show health 1**

If you (TAC) can get into engineering mode, use **lep 1 show vbuf**. (CSCdp93187)

- If you save a configuration file from a switch, and then apply the saved configuration file to that same switch, it is safe to ignore messages about TRBRF and TRCRF VLANs. These messages are caused by the default Token Ring VLAN configuration, which is always present regardless of the specific configuration of the switch. (CSCdm92714)
- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)
- After closing a Telnet session, the switch still shows the session as open. Using the **disconnect ip_address** command to disconnect a user and manually close the session does not close the session. (CSCdp33649)

Resolved Caveats in Software Release 4.5(6)

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(6).

- By entering **reset <mod_num>** repeatedly and very quickly, you can cause the switch to reset. This does not happen in normal use. (CSCdp75494)

- Communication with the 10/100 ports can be lost under rare circumstances when the ports are busy transmitting traffic, and you reconfigure the port speed or duplex or disable the port. The modules affected are WS-X4148, WS-X4232, and 2948G. (CSCdp62955)

Open and Resolved Caveats in Software Release 4.5(5)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(5):

- [Open Caveats in Software Release 4.5\(5\), page 15](#)
- [Resolved Caveats in Software Release 4.5\(5\), page 16](#)

Open Caveats in Software Release 4.5(5)



Note

For a description of caveats resolved in software release 4.5(5), see the [“Resolved Caveats in Software Release 4.5\(5\)”](#) section on page 16.

This section describes open caveats in Catalyst 4000 family software release 4.5(5).

- If you save a configuration file from a switch, and then apply the saved configuration file to that same switch, it is safe to ignore messages about TRBRF and TRCRF VLANs. These messages are caused by the default Token-Ring VLAN configuration, which is always present regardless of the specific configuration of the switch. (CSCdm92714)
- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)
- After closing a Telnet session, the switch still shows the session as open. Using the **disconnect ip_address** command to disconnect a user and manually close the session does not close the session. (CSCdp33649)

Resolved Caveats in Software Release 4.5(5)



Note

Open caveats in software release 4.5(5) are listed in the [“Open Caveats in Software Release 4.5\(5\)” section on page 15](#).

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(5).

- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- When the **set snmp trap help** command is executed, the keyword **syslog** is not shown as an option. (CSCdp29969)
- If a VTP client and server in a VTP domain are separated from each other by a VTP transparent-mode switch that is not a member of any VTP domain, after a client is reset, it does not update its configuration after receiving a VTP update from the VTP server. (CSCdp05027)
- Telnet sessions to the switch are not properly released. (CSCdp15609)
- Multicast and broadcast traffic is not cleared correctly from the counters when the **clear counter** command is issued. (CSCdm94354)
- VTP clients do not learn new configurations from each other. When the update timer in one VTP client times out, it has to send a request advertisement but this request does not reach other clients and the requesting client remains stuck waiting for the rest of the configuration. Resetting the switch or changing the state of the switch enables the hung client to learn the configuration. (CSCdm90300)
- Trunk is going up and down when the channel is in channel-on mode and the trunk is in nonnegotiate mode. (CSCdp32703)
- When upgrading from any 4.x software release to software release 5.2(2), the SNMP trap receiver conversion causes SNMP trap receiver information to be lost and replaced with 10 incorrect SNMP trap receivers of 0.0.0.0. The workaround is to issue a **clear snmp trap all** command and reenter the valid SNMP trap receivers. (CSCdp44206)
- The LED remains on indicating link speed even when the link is down. (CSCdp42337)

Open and Resolved Caveats in Software Release 4.5(4)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(4):

- [Open Caveats in Software Release 4.5\(4\), page 17](#)
- [Resolved Caveats in Software Release 4.5\(4\), page 17](#)

Open Caveats in Software Release 4.5(4)



Note

For a description of caveats resolved in software release 4.5(4), see the [“Resolved Caveats in Software Release 4.5\(4\)” section on page 17](#).

This section describes open caveats in Catalyst 4000 family software release 4.5(4).

- If you save a configuration file from a switch, and then apply the saved configuration file to that same switch, it is safe to ignore messages about TRBRF and TRCRF VLANs. These messages are caused by the default Token-Ring VLAN configuration, which is always present regardless of the specific configuration of the switch. (CSCdm92714)
- In some cases, on a Catalyst 4000 family switch with an extremely heavy traffic load (such as from a traffic generator), modules that contain 10/100 Fast Ethernet ports might not come online after being reset. The workaround is to reduce the traffic load and reset the module. (CSCdk74166)
- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)

Resolved Caveats in Software Release 4.5(4)



Note

Open caveats in software release 4.5(4) are listed in the [“Open Caveats in Software Release 4.5\(4\)” section on page 17](#).

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(4).

- Under certain conditions, the switch can access an out-of-range memory location, causing the switch to reset. This problem is fixed in software release 4.5(4). (CSCdm81976)
- The command **set spantree portvlancost mod_num /port_num cost cost vlan** does not work properly following module reset (the portvlancost for all ports on module *mod_num* except port *port_num* will be incorrect following module reset). This problem is fixed in software release 4.5(4). (CSCdm93868)

- When using TACACS+, if you open a Telnet session to the switch and enter a username and close the Telnet session without entering a password, the TACACS+ session from the switch to the TACACS+ server remains open. This problem is fixed in software release 4.5(4). (CSCdp02341)
- Occasionally, you may see “%SPANTREE-3-PORTADD_DISABLE” messages. This message indicates that a port for a given VLAN has been added to the spanning tree in a disabled state. Examine the condition of the port. Contact your technical support representative. These messages have been moved to severity level 7 in software release 4.5(4). (CSCdp06238)
- Periodically, the switch reboots with an **MCP not responding** message. This problem is fixed in software release 4.5(4). (CSCdm90981)
- When you configure a permanent multicast CAM entry for multiple ports and you change the port VLAN membership for multiple ports, the supervisor engine receives an exception and reloads. Only the first port listed retains the new VLAN membership, and is removed from the permanent CAM entry. This problem is fixed in software release 4.5(4). (CSCdm91321)

Open and Resolved Caveats in Software Release 4.5(3)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(3):

- [Open Caveats in Software Release 4.5\(3\), page 18](#)
- [Resolved Caveats in Software Release 4.5\(3\), page 19](#)

Open Caveats in Software Release 4.5(3)



Note

For a description of caveats resolved in software release 4.5(3), see the [“Resolved Caveats in Software Release 4.5\(3\)”](#) section on page 19.

This section describes open caveats in Catalyst 4000 family software release 4.5(3).

- In some cases, on a Catalyst 4000 family switch with an extremely heavy traffic load (such as from a traffic generator), modules that contain 10/100 Fast Ethernet ports might not come online after being reset. The workaround is to reduce the traffic load and reset the module. (CSCdk74166)
- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- You can configure only one default gateway on the Catalyst 4000 family switches in software release 4.x. Multiple default gateways are not supported. (CSCdk70727)
- On IEEE 802.1Q trunk ports with a large number of active VLANs (several hundred), spanning tree convergence time can be delayed up to several minutes, depending on the number of active VLANs. The 802.1Q trunk port will eventually enter the correct spanning tree state for each active VLAN. (CSCdk70821)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)

- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- When you enable spanning tree PortFast on a port connected to a PC, if the first subsequent link-up received on the port is an IPX client attempting to autosense the frame type, the operation will fail. The workaround is to reset the module after you enable PortFast on the desired ports. (CSCdm62783)
- In some cases, the spanning tree convergence time is not decreased when UplinkFast is enabled on a Catalyst 4003 switch. If the uplink port is on one module (for example, module 2), hosts connected to the other module (for example, module 3) will not notice a decrease in convergence time. (CSCdm54393)

Resolved Caveats in Software Release 4.5(3)



Note

Open caveats in software release 4.5(3) are listed in the [“Open Caveats in Software Release 4.5\(3\)” section on page 18](#).

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(3).

- If the out-of-band management Ethernet (me1) interface is the only interface configured, the system name is not successfully retrieved through Domain Name System (DNS) even though DNS is configured and enabled. As a result, the system name (in the **show system** command output) and the command line prompt do not reflect the system name. This problem is fixed in software release 4.5(3). (CSCdk56988)
- If you configure an RMON threshold alarm on the switch and that alarm is triggered while a MIB walk is in progress, the MIB walking application might loop back to the first leaf of the MIB branch it is currently walking. The workaround is to disable RMON, not configure any RMON alarms on the switch, or increase the polling interval of the alarm (such as one poll every five minutes). This problem is fixed in software release 4.5(3). (CSCdm34091)
- In some situations, the “RxBPDUThresholdDrop” counter does not show the actual number of dropped frames. This problem is fixed in software release 4.5(3). (CSCdm56862)
- When you configure a port with a connected workstation as the SPAN destination port (with the **inpkts** option enabled) for a SPAN source port configured as a VLAN trunk, attempts to ping other devices in the network from the workstation fail. This problem is fixed in software release 4.5(3). (CSCdm48998)
- A PC equipped with a 3C905 NIC might fail to connect to Novell servers if the PC is configured for IPX auto-frame detection and the Novell servers do not use 802.2 framing. The problem only occurs on PCs when IPX is the only protocol stack bound to the NIC (the PC does not use IP or NetBEUI, for example). The workaround is to make sure Novell servers use 802.2 framing, or manually configure the PC to use the appropriate IPX framing. This problem is fixed in software release 4.5(3). However, a related caveat (CSCdm62783) is still open in software release 4.5(3). For more information, see the [“Open Caveats in Software Release 4.5\(3\)” section on page 18](#). (CSCdm53125)
- If you repeatedly delete and create an etherStatsEntry, you might be unable to access the counter MIB objects for the current etherStatsEntry. The workaround is to delete the problem etherStatsEntry and create a new one. This problem is fixed in software release 4.5(3). (CSCdm01166)

- If you configure an RMON threshold alarm on the switch and that alarm is triggered while a MIB walk is in progress, the MIB walking application might loop back to the first leaf of the MIB branch it is currently walking. The workaround is to disable RMON, not configure any RMON alarms on the switch, or increase the polling interval of the alarm (such as one poll every five minutes). This problem is fixed in software release 4.5(3). (CSCdm34091)
- A syslog message for a given facility is not sent to the syslog server if the syslog server severity level is set to a value equal to or greater than the message severity but the default severity level for that facility is set to a value less than the message severity. The workaround is to set the default facility severity level to a value equal to or greater than the configured syslog severity level. In release 4.5(3), syslog messages are sent to the syslog server if the syslog server severity level is equal to or greater than the message severity and the default facility severity level is equal to or greater than the message severity. (CSCdm71889)
- In some cases, when you clear the configuration using the **clear config all** command, not all routes are removed from the IP routing table. The workaround is to configure the in-band (sc0), out-of-band management Ethernet (me1), and SLIP (sl0) interfaces down using the **set interface {sc0 | me1 | sl0} down** command before clearing the configuration. This problem is fixed in software release 4.5(3). (CSCdm56746)
- Attempts to authenticate users on the switch using CiscoSecure NT might fail because the switch does not include the remote address (rem_addr) field in TACACS+ authentication packets. This problem is fixed in software release 4.5(3). (CSCdm60984)

Open and Resolved Caveats in Software Release 4.5(2)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(2):

- [Open Caveats in Software Release 4.5\(2\), page 20](#)
- [Resolved Caveats in Software Release 4.5\(2\), page 21](#)

Open Caveats in Software Release 4.5(2)



Note

For a description of caveats resolved in software release 4.5(2), see the [“Resolved Caveats in Software Release 4.5\(2\)”](#) section on page 21.

This section describes open caveats in Catalyst 4000 family software release 4.5(2).

- In some cases, on a Catalyst 4000 family switch with an extremely heavy traffic load (such as from a traffic generator), modules that contain 10/100 Fast Ethernet ports might not come online after being reset. The workaround is to reduce the traffic load and reset the module. (CSCdk74166)
- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- If the out-of-band management Ethernet (me1) interface is the only interface configured, the system name is not successfully retrieved through Domain Name System (DNS) even though DNS is configured and enabled. As a result, the system name (in the **show system** command output) and the command line prompt do not reflect the system name. (CSCdk56988)
- You can configure only one default gateway on the Catalyst 4000 family switches in software release 4.x. Multiple default gateways are not supported. (CSCdk70727)

- On IEEE 802.1Q trunk ports with a large number of active VLANs (several hundred), spanning tree convergence time can be delayed up to several minutes, depending on the number of active VLANs. The 802.1Q trunk port will eventually enter the correct spanning tree state for each active VLAN. (CSCdk70821)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- If you configure an RMON threshold alarm on the switch and that alarm is triggered while a MIB walk is in progress, the MIB walking application might loop back to the first leaf of the MIB branch it is currently walking. The workaround is to disable RMON, not configure any RMON alarms on the switch, or increase the polling interval of the alarm (such as one poll every five minutes). (CSCdm34091)
- A syslog message for a given facility is not sent to the syslog server if the syslog server severity level is set to a value equal to or greater than the message severity but the default severity level for that facility is set to a value less than the message severity. The workaround is to set the default facility severity level to a value equal to or greater than the configured syslog severity level. (CSCdm71889)

Resolved Caveats in Software Release 4.5(2)



Note

Open caveats in software release 4.5(2) are listed in the [“Open Caveats in Software Release 4.5\(2\)” section on page 20](#).

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(2).

- If you disconnect a Telnet session to the switch when the switch is at the More prompt (such as with **show** command output) or is waiting for user input (such as a Yes/No prompt), future Telnet sessions might stop accepting user input. This problem is resolved in software release 4.5(2). (CSCdk83562)
- Under certain traffic conditions characterized by a large number (greater than 64K) of unique source and destination address pairs, it is possible that the system will learn less than the maximum number of supported hosts. This problem is resolved in software release 4.5(2). (CSCdk87372)
- If DNS is enabled and none of the configured DNS servers is reachable, local password authentication can be excessively slow. This problem is resolved in software release 4.5(2). (CSCdm14239)
- In some cases, when the active link of an UplinkFast link pair is disconnected, the switch does not transmit broadcast frames on the secondary link. This problem is resolved in software release 4.5(2). (CSCdm23587)
- In some cases, when a switch receives frames with the BPDUs on a blocked port, the switch incorrectly floods the frames, causing spanning tree instability. This problem is resolved in software release 4.5(2). (CSCdm34970)

- In some cases, if the primary UplinkFast link goes down, when it comes back up it can take 20 to 25 seconds to begin forwarding traffic instead of the usual one to five seconds, depending on the remote hardware. The workaround is to connect to a different port on the remote device if the problem occurs. This problem is resolved in software release 4.5(2). (CSCdm26273)
- In some cases, UplinkFast does not function correctly between a Catalyst 5000 family switch and a Catalyst 4000 family switch, a Catalyst 2948G switch, or a Catalyst 5000 family Gigabit EtherChannel module (WS-X5410). This problem is resolved in software release 4.5(2). (CSCdm34341)
- In some cases, if you configure a port as a SPAN source port and subsequently configure the same port as the SPAN destination, the SPAN destination port might be unable to receive traffic if any other SPAN-related commands are executed on the port. To avoid the problem, disable SPAN before changing the SPAN configuration. If the problem occurs, reset the module with the problem SPAN port. This problem is resolved in software release 4.5(2). (CSCdm43384)
- If you delete the RMON alarmEntry or if you modify the alarmVariable of the RMON alarmEntry while that alarmVariable is being sampled, the switch might reset. This problem is resolved in software release 4.5(2). (CSCdm49575)
- If you configure the IP address of the in-band (sc0) interface with an address in subnet zero of a Class B address and 24 bits of subnet mask, IP traffic destined for other subnets in the same Class B network are not forwarded to the default gateway. For example, if the sc0 IP address is 172.20.0.10/24, a ping to any other address in the 172.20 Class B network (except for those in the 172.20.0 subnet) fails. However, a ping to an address in any other Class B network succeeds. This problem is resolved in software release 4.5(2). (CSCdm33248)
- In some situations, if the switch attempts to clear dynamic CAM table entries when the dynamic entries have not been cleared for an extended period of time (several days to several weeks), the switch resets. Events that cause the switch to clear dynamic CAM entries include:
 - Entering the **clear cam dynamic** command
 - A link-down on a switch port, causing the switch to clear entries learned on that port
 This problem is resolved in software release 4.5(2). (CSCdm33046)

Open and Resolved Caveats in Software Release 4.5(1)

This section describes the open and resolved caveats in Catalyst 4000 family software release 4.5(1):

- [Open Caveats in Software Release 4.5\(1\), page 22](#)
- [Resolved Caveats in Software Release 4.5\(1\), page 24](#)

Open Caveats in Software Release 4.5(1)



Note

For a description of caveats resolved in software release 4.5(1), see the [“Resolved Caveats in Software Release 4.5\(1\)” section on page 24](#).

This section describes open caveats in Catalyst 4000 family software release 4.5(1).

- In some cases, on a Catalyst 4000 family switch with an extremely heavy traffic load (such as from a traffic generator), modules that contain 10/100 Fast Ethernet ports might not come online after being reset. The workaround is to reduce the traffic load and reset the module. (CSCdk74166)

- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface. (CSCdk80415)
- If the out-of-band management Ethernet (me1) interface is the only interface configured, the system name is not successfully retrieved through Domain Name System (DNS) even though DNS is configured and enabled. As a result, the system name (in the **show system** command output) and the command line prompt do not reflect the system name. (CSCdk56988)
- You can configure only one default gateway on the Catalyst 4000 family switches in software release 4.x. Multiple default gateways are not supported. (CSCdk70727)
- On IEEE 802.1Q trunk ports with a large number of active VLANs (several hundred), spanning tree convergence time can be delayed up to several minutes, depending on the number of active VLANs. The 802.1Q trunk port will eventually enter the correct spanning tree state for each active VLAN. (CSCdk70821)
- If you disconnect a Telnet session to the switch when the switch is at the More prompt (such as with **show** command output) or is waiting for user input (such as a Yes/No prompt), future Telnet sessions might stop accepting user input. This problem is resolved in software release 4.5(2). (CSCdk83562)
- On 10/100-Mbps Fast Ethernet ports, SNMP incorrectly reports the status of the portOperTxFlowControl and portOperRxFlowControl objects as “disagree” instead of “off.” These ports are not capable of flow control. This problem does not affect the operation of the switch. (CSCdk78451)
- Under certain traffic conditions characterized by a large number (greater than 64K) of unique source and destination address pairs, it is possible that the system will learn less than the maximum number of supported hosts. This problem is resolved in software release 4.5(2). (CSCdk87372)
- Pressing **Control-C** at the More prompt (for example, when a **show** command is displaying multiple pages of output) does not interrupt the output and return the Console> prompt. The workaround is to press the **q** key. (CSCdm11604)
- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- In some situations, if the switch attempts to clear dynamic CAM table entries when the dynamic entries have not been cleared for an extended period of time (several days to several weeks), the switch resets. Events that cause the switch to clear dynamic CAM entries include:
 - Entering the **clear cam dynamic** command
 - A link-down on a switch port, causing the switch to clear entries learned on that port(CSCdm33046)

Resolved Caveats in Software Release 4.5(1)



Note

Open caveats in software release 4.5(1) are listed in the [“Open Caveats in Software Release 4.5\(1\)” section on page 22](#).

This section describes the caveats resolved in Catalyst 4000 family software release 4.5(1).

- In some cases, on a Catalyst 4000 family switch with a heavy traffic load, you might experience difficulty resetting a module that contains 10/100 Fast Ethernet ports. If you reset the module and some or all of the ports fail to come up, reset the module a second time. If ports still do not come up, remove and reinsert the module. This problem is resolved in software release 4.5(1). (CSCdk79232)
- The outDiscards Management Information Base (MIB) object might report an incorrect value. If there have been no transmit queue drops, the value is correct (no drops occurred). However, if there have been drops, the counter might show an incorrect nonzero number. In addition, the counter might decrement or display a very large number. This problem is resolved in software release 4.5(1). (CSCdk79523)
- Under very heavy load conditions, a switching module might not come online after hot swapping. To recover, reset the switch. This problem is resolved in software release 4.5(1). (CSCdk80446)
- If the out-of-band management Ethernet (me1) interface is the only interface configured, the **test snmp trap** command fails to send an Simple Network Management Protocol (SNMP) trap message. This problem is resolved in software release 4.5(1). (CSCdk75897)
- In some cases, if you change the VLAN assignment of ports in a Fast EtherChannel, some ports are placed in the “errdisable” state and the channel is not renegotiated. The correct behavior is that the channel is torn down and renegotiated. This problem is resolved in software release 4.5(1). (CSCdk32807)
- In ROM monitor mode, do not specify a repeat count greater than 16 when entering the **repeat** command. Specifying a repeat count greater than 16 might cause the ROM monitor to reset the system. This problem is resolved in software release 4.5(1). (CSCdk71931)
- On some Catalyst 4000 family switching modules, if you change the following configuration options on a four-port EtherChannel bundle, the change might appear to be applied to all four ports but actually, only the first two ports in the channel retain the configuration changes:
 - Spanning tree port priority (**set spantree portpri**)
 - Port speed (**set port speed**)
 - Port duplex (**set port duplex**)
 - Spanning tree PortFast (**set spantree portfast**)
 - Virtual LAN (VLAN) membership (**set vlan**)
 - Trunking admin status (**set trunk**)
 - Protocol filtering (**set port protocol**)

Some of these options (such as VLAN membership) affect all four ports while the channel is established, but if the channel breaks, the change is only retained on the first two ports.

The workaround is to turn off channeling on the ports, make the desired configuration changes, and then return the channeling configuration to its original state. This problem is resolved in software release 4.5(1). (CSCdk78961)

- If you configure port security on a port with user-configured static content-addressable memory (CAM) entries configured, and a frame with a nonsecure Media Access Control (MAC) address is received on the port (causing the port to shut down), the user-configured static CAM entries for the port display the X attribute, indicating that the entry is the secure port address, rather than the * attribute, indicating that the entry is user-configured. This problem does not affect the functionality of port security or the static CAM entries. This problem is resolved in software release 4.5(1). (CSCdk77138)
- If you configure a port as the Switched Port Analyzer (SPAN) destination port, and you power off the system and remove the module with the SPAN destination port, when you power on the system, the **show span** command output indicates that the SPAN destination port is a port on a module that does not exist. The workaround is to disable SPAN, power off the switch, remove the module, power on the switch, and enable SPAN. The problem does not occur if you remove the module with the power on. This problem is resolved in software release 4.5(1). (CSCdk77485)
- If you manually configure the in-band (sc0) interface with IP address 0.0.0.0, BOOTP/RARP will fail with this message the next time the switch is rebooted:

```
bootp_send: sendto 51
```

The workaround is to manually set the desired sc0 IP address. Alternately, you can clear the entire switch configuration using the **clear config all** command (make sure you back up your switch configuration before entering this command or your configuration will be lost). This problem is resolved in software release 4.5(1). (CSCdk71833)

- In some cases, entering the **show cdp neighbors detail** command causes the switch to reset. This problem is resolved in software release 4.5(1). (CSCdm02194)
- If you configure the in-band (sc0) and out-of-band management Ethernet (me1) interfaces with IP addresses in the same subnet, with the sc0 interface configured Up and the me1 interface configured Down, when you reboot the switch the subnet route for sc0 is not present, causing a loss of IP connectivity to the switch. The workaround is to configure a different IP address and subnet mask for the me1 interface. This problem is resolved in software release 4.5(1). (CSCdk77542)
- In some cases, if you change the IP address of the in-band (sc0) interface from an address that conflicts with the out-of-band management Ethernet (me1) interface address to one that does not conflict, the subnet route for me1 might be deleted, possibly resulting in a loss of IP connectivity to the switch. The workaround is to configure the me1 interface Down and then Up (using the **set interface** command). This problem is resolved in software release 4.5(1). (CSCdk77952)
- In some cases, if you configure the in-band (sc0) and out-of-band management Ethernet (me1) interfaces with IP addresses in the same subnet, the switch software fails to properly assign the subnet route to the correct interface (use the **show ip route** command to check to which interface a route is assigned). The workaround is to configure the unused interface Down and assign it an IP address in a different subnet. If subnet routes are still assigned to the wrong interface, manually configure the active interface Down and then Up (using the **set interface** command). This problem is resolved in software release 4.5(1). (CSCdk77912)
- If you configure the Catalyst 4000 family switch as a VTP client, and its only connection to the VTP server is through an IEEE 802.1Q trunk with its native VLAN other than VLAN 1, when you reset the system the trunk port might fail to enter trunking mode after the system comes online (the **show trunk** command output shows the trunk in the “inactive” state). The workaround is to set the native VLAN of the trunk port to VLAN 1 (permanently fixing the problem) or reset the module on which the trunk port is located (you will have to reset the module again each time the switch boots). This problem is resolved in software release 4.5(1). (CSCdk77956)

- If you specify a nonconnected port as a VLAN SPAN destination port and you later connect the port, packets transmitted or received in the monitored VLAN might not be mirrored to the SPAN destination port correctly. The workaround is to not specify a nonconnected port as a VLAN SPAN destination, or disable and reenable SPAN on the port once the port is connected. This problem is resolved in software release 4.5(1). (CSCdk73354)
- Under some circumstances, several ports might incorrectly be assigned the same ifIndex value (you can see the ifIndex values for ports using the **show port** command). If multiple ports share an ifIndex value, when you change the configuration on one port, other ports with the same ifIndex value might be affected. If this problem occurs, clear the entire switch configuration using the **clear config all** command (make sure you back up your switch configuration before entering this command or your configuration will be lost) and reset the switch. This problem is resolved in software release 4.5(1). (CSCdk74506)
- If you set a trunk port as a SPAN destination port, trunking on that port is turned off. However, the **show trunk** command output shows the port is still trunking. The correct trunking state is displayed for the port after a reset. This problem is resolved in software release 4.5(1). (CSCdk75806)
- When you set the out-of-band management Ethernet (me1) to a non-8-bit boundary subnet mask (such as 255.255.255.240), the system might incorrectly calculate the broadcast address. The workaround is to explicitly specify the broadcast address when you enter the **set interface** command when using a non-8-bit boundary subnet mask. This problem is resolved in software release 4.5(1). (CSCdk80885)
- If you reconnect a Sun Gigabit Ethernet Card 2.0 to the switch after the link was broken (for example, by disabling the port or disconnecting the cable), the output of the **show port status** command might indicate a “remfault” condition, even though the link is operational. This problem is resolved in software release 4.5(1). (CSCdk88589)
- In the output of the **show counters** command, the SymbolErrorsDuringCarrier counter is not included in the total CRCAlignErrors counter value on Fast Ethernet ports. The workaround is to add the SymbolErrorsDuringCarrier value to the CRCAlignErrors value to obtain the correct CRCAlignErrors value for the port. This problem is resolved in software release 4.5(1). (CSCdk83555)
- When you place a port that is forwarding traffic for a host into the **auto** protocol filtering mode, the traffic might be dropped instead of filtered according to the normal protocol filtering rules. The workaround is to clear the CAM table using the **clear cam dynamic** command after enabling protocol filtering or setting the protocol filtering mode of a port to **auto**. This problem is resolved in software release 4.5(1). (CSCdk89017)
- In certain circumstances, some traffic loss can occur with X-stream tests. This problem is resolved in software release 4.5(1). (CSCdm01120)
- If the switch learns the MAC address of a host advertising a MAC address of 00:00:00:00:00:00, when you enter the **show cam dynamic** command, the switch will reset. This MAC address is illegal, but some noncompliant hardware might advertise this address. The workaround is to not enter the **show cam dynamic** command if a MAC address of all zeroes has been learned. This problem is resolved in software release 4.5(1). (CSCdm05261)

Open Caveats in Software Release 4.4(1)

This section describes open caveats in Catalyst 4000 family software release 4.4(1).

- In some cases, on a Catalyst 4000 family switch with a heavy traffic load, you might experience difficulty resetting a module that contains 10/100 Fast Ethernet ports. If you reset the module and some or all of the ports fail to come up, reset the module a second time. If ports still do not come up, remove and reinsert the module. This problem is resolved in software release 4.5(1). (CSCdk79232)
- In some cases, on a Catalyst 4000 family switch with an extremely heavy traffic load (such as from a traffic generator), modules that contain 10/100 Fast Ethernet ports might not come online after being reset. The workaround is to reduce the traffic load and reset the module. (CSCdk74166)
- The outDiscards Management Information Base (MIB) object might report an incorrect value. If there have been no transmit queue drops, the value is correct (no drops occurred). However, if there have been drops, the counter might show an incorrect nonzero number. In addition, the counter might decrement or display a very large number. This problem is resolved in software release 4.5(1). (CSCdk79523)
- On some Catalyst 4000 family switching modules, if you change the following configuration options on a four-port EtherChannel bundle, the change might appear to be applied to all four ports but actually, only the first two ports in the channel retain the configuration changes:
 - Spanning tree port priority (**set spantree portpri**)
 - Port speed (**set port speed**)
 - Port duplex (**set port duplex**)
 - Spanning tree PortFast (**set spantree portfast**)
 - Virtual LAN (VLAN) membership (**set vlan**)
 - Trunking admin status (**set trunk**)
 - Protocol filtering (**set port protocol**)

Some of these options (such as VLAN membership) affect all four ports while the channel is established, but if the channel breaks, the change is only retained on the first two ports.

The workaround is to turn off channeling on the ports, make the desired configuration changes, and then return the channeling configuration to its original state. This problem is resolved in software release 4.5(1). (CSCdk78961)

- Do not set the out-of-band management Ethernet (me1) interface status to Up unless the interface has a valid IP address configured. Communication over the in-band interface might be lost. (CSCdk80415)
- Under very heavy load conditions, a switching module might not come online after hot swapping. To recover, reset the switch. This problem is resolved in software release 4.5(1). (CSCdk80446)
- If the out-of-band management Ethernet (me1) interface is the only interface configured, the system name is not successfully retrieved through Domain Name System (DNS) even though DNS is configured and enabled. As a result, the system name (in the **show system** command output) and the command line prompt do not reflect the system name. (CSCdk56988)
- If the out-of-band management Ethernet (me1) interface is the only interface configured, the **test snmp trap** command fails to send a Simple Network Management Protocol (SNMP) trap message. This problem is resolved in software release 4.5(1). (CSCdk75897)

- If you configure port security on a port with user-configured static content-addressable memory (CAM) entries configured, and a frame with a nonsecure Media Access Control (MAC) address is received on the port (causing the port to shut down), the user-configured static CAM entries for the port display the X attribute, indicating that the entry is the secure port address, rather than the * attribute, indicating that the entry is user-configured. This problem does not affect the functionality of port security or the static CAM entries. This problem is resolved in software release 4.5(1). (CSCdk77138)
- In some cases, if you change the VLAN assignment of ports in a Fast EtherChannel, some ports are placed in the “errdisable” state and the channel is not renegotiated. The correct behavior is that the channel is torn down and renegotiated. This problem is resolved in software release 4.5(1). (CSCdk32807)
- If you configure a port as the Switched Port Analyzer (SPAN) destination port, and you power off the system and remove the module with the SPAN destination port, when you power on the system, the **show span** command output indicates that the SPAN destination port is a port on a module that does not exist. The workaround is to disable SPAN, power off the switch, remove the module, power on the switch, and enable SPAN. The problem does not occur if you remove the module with the power on. This problem is resolved in software release 4.5(1). (CSCdk77485)
- You can configure only one default gateway on the Catalyst 4000 family switches in software release 4.x. Multiple default gateways are not supported. (CSCdk70727)
- If you manually configure the in-band (sc0) interface with IP address 0.0.0.0, BOOTP/RARP will fail the next time the switch is rebooted, and this message will appear:

```
bootp_send: sendto 51
```

The workaround is to manually set the desired sc0 IP address. Alternately, you can clear the entire switch configuration using the **clear config all** command (make sure you back up your switch configuration before entering this command or your configuration will be lost). This problem is resolved in software release 4.5(1). (CSCdk71833)

- If you configure the in-band (sc0) and out-of-band management Ethernet (me1) interfaces with IP addresses in the same subnet, with the sc0 interface configured Up and the me1 interface configured Down, when you reboot the switch the subnet route for sc0 is not present, causing a loss of IP connectivity to the switch. The workaround is to configure a different IP address and subnet mask for the me1 interface. This problem is resolved in software release 4.5(1). (CSCdk77542)
- On IEEE 802.1Q trunk ports with a large number of active VLANs (several hundred), spanning tree convergence time can be delayed up to several minutes, depending on the number of active VLANs. The 802.1Q trunk port will eventually enter the correct spanning tree state for each active VLAN. (CSCdk70821)
- In some cases, if you configure the in-band (sc0) and out-of-band management Ethernet (me1) interfaces with IP addresses in the same subnet, the switch software fails to properly assign the subnet route to the correct interface (use the **show ip route** command to check to which interface a route is assigned). The workaround is to configure the unused interface Down and assign it an IP address in a different subnet. If subnet routes are still assigned to the wrong interface, manually configure the active interface Down and then Up (using the **set interface** command). This problem is resolved in software release 4.5(1). (CSCdk77912)
- In some cases, if you change the IP address of the in-band (sc0) interface from an address that conflicts with the out-of-band management Ethernet (me1) interface address to one that does not conflict, the subnet route for me1 might be deleted, possibly resulting in a loss of IP connectivity to the switch. The workaround is to configure the me1 interface Down and then Up (using the **set interface** command). This problem is resolved in software release 4.5(1). (CSCdk77952)

- If you configure the Catalyst 4000 family switch as a VTP client and its only connection to the VTP server is through an IEEE 802.1Q trunk with its native VLAN other than VLAN 1, when you reset the system the trunk port might fail to enter trunking mode after the system comes online (the **show trunk** command output shows the trunk in the “inactive” state). The workaround is to set the native VLAN of the trunk port to VLAN 1 (permanently fixing the problem) or reset the module on which the trunk port is located (you will have to reset the module again each time the switch boots). This problem is resolved in software release 4.5(1). (CSCdk77956)
- In ROM monitor mode, do not specify a repeat count greater than 16 when entering the **repeat** command. Specifying a repeat count greater than 16 might cause the ROM monitor to reset the system. This problem is resolved in software release 4.5(1). (CSCdk71931)
- Under some circumstances, several ports might incorrectly be assigned the same ifIndex value (you can see the ifIndex values for ports using the **show port** command). If multiple ports share an ifIndex value, when you change the configuration on one port, other ports with the same ifIndex value might be affected. If this problem occurs, clear the entire switch configuration using the **clear config all** command (make sure you back up your switch configuration before entering this command or your configuration will be lost) and reset the switch. This problem is resolved in software release 4.5(1). (CSCdk74506)
- If you specify a nonconnected port as a VLAN SPAN destination port and you later connect the port, packets transmitted or received in the monitored VLAN might not be mirrored to the SPAN destination port correctly. The workaround is to not specify a nonconnected port as a VLAN SPAN destination, or disable and reenable SPAN on the port once the port is connected. This problem is resolved in software release 4.5(1). (CSCdk73354)
- If you set a trunk port as a SPAN destination port, trunking on that port is turned off. However, the **show trunk** command output shows the port is still trunking. The correct trunking state is displayed for the port after a reset. This problem is resolved in software release 4.5(1). (CSCdk75806)
- When you set the out-of-band management Ethernet (me1) to a non-8-bit boundary subnet mask (such as 255.255.255.240), the system might incorrectly calculate the broadcast address. The workaround is to explicitly specify the broadcast address when you enter the **set interface** command when using a non-8-bit boundary subnet mask. This problem is resolved in software release 4.5(1). (CSCdk80885)
- If the switch learns the MAC address of a host advertising a MAC address of 00:00:00:00:00:00, when you enter the **show cam dynamic** command, the switch will reset. This MAC address is illegal, but some noncompliant hardware might advertise this address. The workaround is to not enter the **show cam dynamic** command if a MAC address of all zeroes has been learned. This problem is resolved in software release 4.5(1). (CSCdm05261)
- You cannot clear a specific user-configured dynamic CAM entry using the **clear cam mac_addr** command. The workaround is to clear all dynamic CAM entries using the **clear cam dynamic** command, or wait for the entry to age out (if no traffic from that address is received by the switch). (CSCdk48841)
- In some situations, if the switch attempts to clear dynamic CAM table entries when the dynamic entries have not been cleared for an extended period of time (several days to several weeks), the switch resets. Events that cause the switch to clear dynamic CAM entries include:
 - Entering the **clear cam dynamic** command
 - A link-down on a switch port, causing the switch to clear entries learned on that port
 (CSCdm33046)

Usage Guidelines, Restrictions, and Troubleshooting

These sections provide usage guidelines, restrictions, and troubleshooting information for Catalyst 4000 family switch hardware and software:

- [System and Supervisor Engine, page 30](#)
- [Modules and Switch Ports, page 30](#)
- [Spanning Tree, page 32](#)
- [VTP, VLANs, and VLAN Trunks, page 34](#)
- [EtherChannel, page 34](#)
- [SPAN, page 35](#)
- [Multicast, page 35](#)
- [MIBs, page 35](#)

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.

- Setting the out-of-band management Ethernet (me1) interface status to Up without a valid IP address configured can disrupt communication over the in-band (sc0) interface.
- If you need to download configuration files to many switches in a network topology with redundant EtherChannel links, download the configuration at each switch manually using the **configure network** command. Otherwise, in some situations, a broadcast storm can occur.
- Under certain conditions, etherHistoryUtilization is not reported correctly if the counter value wraps between the two consecutive samples. The workaround is to reduce the sample interval.
- If your configuration produces thousands of CAM entries, ensure that your screen length is set to a value greater than 0 before entering the **show cam dynamic** command.
- The LrnDiscard counter (displayed by entering the **show mac** command) indicates the number of times a CAM entry is replaced with a newly learned address when the CAM table is full. The counter value is not maintained for each port; instead, the value is maintained for the entire switch.
- Although the **show spantree** command displays the PortFast feature as enabled on a trunk port, spanning tree PortFast has no effect on trunk ports. Do not use the **set portfast** command on a trunk port. In addition, designating a port as a trunk port ignores the PortFast feature for the port.
- The CLI command **show cam dynamic** and the SNMP query “getmany community@vlan dot1dTpFdbAddress” are sometimes not synchronized.

Modules and Switch Ports

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

- When hot inserting a module into a Catalyst 4000 family chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Incorrectly inserting a module can cause unexpected behavior. For proper module installation instructions, refer to the *Catalyst 4003 Series Installation Guide*.

- When connecting end stations (such as Windows 95/98/NT workstations) to Catalyst 4000 family 10/100-Mbps switch ports, use the following configuration if the end stations are using DHCP or IPX. If you use a different configuration, you might have problems obtaining an IP address using BOOTP/DHCP or getting an IPX login using IPX.
 - Spanning tree PortFast enabled
Use the **set spantree portfast *mod_num/port_num* enable** command to enable PortFast on a port.
 - Trunking off
Use the **set trunk *mod_num/port_num* off** command to disable trunking on a port.
 - Channeling off
Use the **set port channel *port_list* off** command to disable channeling on a port.



Note You must specify a valid port range when entering the **set port channel** command. You cannot specify a single port.

This example shows how to configure a port for end station connectivity:

```
Console> (enable) set spantree portfast 2/2 enable
```

```
Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc. to
a fast start port can cause temporary spanning tree loops. Use with caution.
```

```
Spantree port 2/2 fast start enabled.
```

```
Console> (enable) set trunk 2/2 off
```

```
Port(s) 2/2 trunk mode set to off.
```

```
Console> (enable) set port channel 2/1-2 off
```

```
Port(s) 2/1-2 channel mode set to off.
```

```
Console> (enable)
```

- When you replace a module (other than the supervisor engine) with a module of a different type, or when you insert a module (other than the supervisor engine) in an empty slot, enter the command **clear config *mod_num*** to clear the module configuration information in the supervisor engine and obtain the correct spanning tree parameters.
- Whenever you connect a Catalyst 4000 family 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 Catalyst 4000 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.
- If a port fails the physical-medium-dependent (PMD) loopback test (port LED is flashing orange) after the Catalyst 4000 family switch is reset, you must reset the affected module to recover.
- If a module fails to come online, reset the module by entering the **reset *mod_num*** command.
- If the Catalyst 4000 family switch detects a port-duplex misconfiguration, the misconfigured switch port is disabled and placed in the “errdisable” state. Reconfigure the port-duplex setting and use the **set port enable** command to reenable the port.
- 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.

- On Catalyst 4000 family modules that contain 10/100 Fast Ethernet ports, the Carri-Sen counter (in the output of the **show port** command) might erroneously show a value of 1 indicating an error occurred, even though in most cases, a carrier sense error did not occur. (CSCdk69054)
- Some ports on the Catalyst 4000 family oversubscribed Gigabit Ethernet modules do not reliably autonegotiate Ethernet operational modes with some Sun Gigabit Ethernet NICs. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

These Sun Gigabit Ethernet NICs are affected (the problem occurs only on some hardware revisions):

- Sbus Gigabit Ethernet NIC (part number X1140A)
- PCI Gigabit Ethernet NIC (part number X1141A)

The workaround is to use the following configuration:

Catalyst 4000 Family Ports		Sun Gigabit Ethernet NIC	
Configuration	Command	Configuration	Command
Autonegotiation disabled	set port negotiation <i>mod_num/port_num</i> disable	Autonegotiation disabled	ndd -set /dev/ge adv_1000autoneg_cap 0
N/A	N/A	Half-duplex off	ndd -set /dev/ge adv_1000hdx_cap 0
Send flow control on ¹	set port flowcontrol <i>mod_num/port_num</i> send on	Send flow control off	ndd -set /dev/ge adv_pauseTX 0
Receive flow control desired ¹	set port flowcontrol <i>mod_num/port_num</i> receive desired	Receive flow control on	ndd -set /dev/gs adv_pauseRX 1

1. Default setting

- (CSCdm38405)

Spanning Tree

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, the Catalyst 4000 family switch receives spanning tree bridge protocol data units (BPDUs) periodically from the 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 two seconds). If a Catalyst 4000 family 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.

The following usage guidelines, restrictions, and troubleshooting information apply to spanning tree:

- On your Catalyst 4000 family switch, ensure that the total number of logical ports across all instances of spanning tree for different VLANs does not exceed the number allowed for the supervisor engine. You can use the **show spantree summary** command and this formula to compute the total number of logical ports on the switch:

$$\text{sum of all logical ports} \leq (\text{number of trunks on the switch} * \text{number of active VLANs on those trunks}) + \text{number of nontrunking port on the switch}$$

where the *sum of all logical ports* equals 1500 for Catalyst 4000 family Supervisor Engine I.



Caution

If you enable numerous memory-intensive features concurrently (such as VTP pruning, VMPS, EtherChannel, and RMON), or if there is switched data traffic on the management VLAN, the maximum number of supported logical ports is reduced.



Note

Count each port in an EtherChannel port bundle independently (do not count the bundle as a single port).

- A Catalyst family switch should be the root for all VLANs, especially VLAN 1. In order to recover from an extended broadcast storm caused by a faulty device in a network, Catalyst family switches reset blocked ports. To ensure recovery, all Catalyst family switches in the network should perform this function at the same time by sending synchronization packets on VLAN 1. These synchronization packets are only sent by a Catalyst family switch if it is the root bridge.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk can potentially cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If you plan to disable spanning tree in an 802.1Q environment, disable spanning tree on every VLAN in the network and ensure a loop-free topology exists.
- Use these commands to monitor blocked spanning tree ports:
 - **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, make sure that the Rcv-Frms and Rcv-Multi counters are incrementing continuously. If the Rcv-Frms counter stops incrementing, the port is not receiving any frames, including BPDUs. If the Rcv-Frms counter is incrementing but the Rcv-Multi counter is not, then this port is receiving nonmulticast frames but is not receiving any 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 the 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.
- Do not use spanning tree PortFast on a trunk port. Although the **show spantree** command displays PortFast as enabled on a trunk port, PortFast has no effect on trunk ports.

VTP, VLANs, and VLAN Trunks

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

- Although the Dynamic Trunk Protocol (DTP) is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems, follow these guidelines:
 - For ports connected to nonCatalyst family devices in which trunking is not being used, configure trunk-capable Catalyst 4000 family switch ports to **off** by entering the **set trunk mod_num/port_num off** command.
 - When trunking 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.
- With Cisco IOS software release 12.0, the Catalyst 8510 campus switch router (CSR) does not process untagged packets (packets on the native VLAN) received on an IEEE 802.1Q trunked interface (all such packets are dropped). If you configure Catalyst 8510 CSR subinterfaces to trunk using 802.1Q encapsulation, traffic cannot be carried successfully on the native VLAN for the trunk configured on the Catalyst 4000 family switch.

The workaround is to create an unused VLAN and assign that VLAN as the native VLAN for the 802.1Q trunk on the Catalyst 4000 family switch. Verify the native VLAN assignment for the trunk using the **show trunk** command.

This problem is tracked as a defect against the Catalyst 8510 CSR software (CSCdk77676).

EtherChannel

This section contains usage guidelines, restrictions, and troubleshooting information that apply to Fast and Gigabit EtherChannel.

- With a large number of channels, trunks, or VLANs, or a change of channel configuration (for example, **off** to **auto**), or upon Fast EtherChannel module reboot, ports might take up to five minutes to form a channel and to participate in spanning tree. (During this interval, the port does not appear in **show spantree** command output.) If it takes more than ten minutes for a channel to form and appear on spanning tree, disable and reenabte the ports. In addition, it might take up to two minutes to unbundle a channel after changing the channel mode.
- When using Fast EtherChannel, if a “SPANTREE-2: Channel misconfig - x/x-x will be disabled” or similar syslog message is displayed, it indicates a mismatch of Fast EtherChannel modes on the connected ports. We recommend that you correct the configuration and reenabte the ports by entering the **set port enable** command. Valid EtherChannel configurations include:

Port Channel Mode	Valid Neighbor Port Channel Mode(s)
desirable	desirable or auto
auto	desirable or auto¹
on	on
off	off

1. If both the local and neighbor ports are in **auto** mode, an EtherChannel bundle will not form.

SPAN

This section contains usage guidelines, restrictions, and troubleshooting information that apply to the Switch Port Analyzer (SPAN).

- Incoming traffic on the SPAN destination port is disabled by default. You can enable it using the **set span** command with the **inpkts enable** keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the SPAN destination port to an unused VLAN.
- A SPAN destination port receives flooded unicasts and broadcasts for the VLAN of the source SPAN port.

Multicast

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

- Due to a conflict with the Hot Standby Router Protocol (HSRP), Cisco Group Management Protocol (CGMP) leave processing is disabled by default.

To enable CGMP leave processing, enter the **set cgmp leave enable** command.



Note If both HSRP and CGMP leave processing are enabled, you might experience some unicast packet flooding.

- When CGMP leave processing is enabled, the Catalyst 4000 family switch learns router ports through PIM-v1, HSRP, and CGMP self-join messages. When CGMP leave processing is disabled, the Catalyst 4000 family switch learns router ports through CGMP self-join messages only.
- CGMP does not prune multicast traffic for any IP multicast address that maps into the Media Access Control (MAC) address range of 01-00-5E-00-00-00 to 01-00-5E-00-00-FF. The reserved IP multicast addresses, in the range 224.0.0.0 to 224.0.0.255, are used to forward local IP multicast traffic in a single Layer 3 hop.

MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (<http://www.cisco.com/public/mibs/>). For information on the specific MIBs supported by the Catalyst 4000 family switches, refer to the Catalyst 4000 MIB Support List located at <ftp://ftp.cisco.com/pub/mibs/supportlists/wsc4000/wsc4000-supportlist.html>

Documentation Updates for Software Release 4.4

This section describes caveats for the Catalyst 4000 family software release 4.4 documentation. These changes will be included in the next update to the documentation.

In the January 1999 version of the *Catalyst 2948G Installation Guide*, in the “Console Port” section in the “Specifications” appendix, the statement “Data Terminal Ready (DTR) and Data Set Ready (DSR) handshake signals are supported” on the console port is incorrect. The console port does not support this function.

Additional Documentation

The following documents are available for the Catalyst 4000 family switches:

- *Catalyst 4000 Family Installation Guide*
- *Software Configuration Guide—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*
- *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*
- *System Message Guide—Catalyst 6000 Family, Catalyst 5000 Family, Catalyst 4000 Family, Catalyst 2926G Series, Catalyst 2948G, and Catalyst 2980G Switches*
- *Layer 3 Services Software Configuration Guide—Catalyst 5000 Family, Catalyst 4000 Family, Catalyst 2926G Series, Catalyst 2948G, and Catalyst 2980G Switches*

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 Cisco.com 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, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
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 documents listed in the “Additional Documentation” section on page 36.