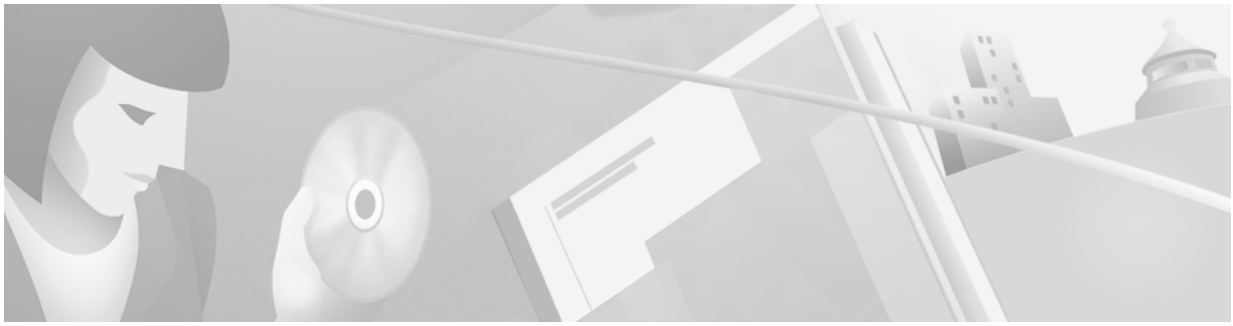

Release Notes for Catalyst 4000 Family Software Release 6.*x*

Current Release:
6.2(1) - April 12, 2001

Previous Releases
6.1(1), 6.1(1c), 6.1(2)

These release notes describe the features, modifications, and caveats for Catalyst 4000 family supervisor engine software release 6.*x* and all 6.*x* maintenance releases. The most current 6.*x* release is supervisor engine software release 6.2(1). These release notes apply to Catalyst 4000 family switches as well as to Catalyst 2948G and 2980 series switches running Catalyst 4000 family supervisor engine software.

Note For the most recent information on open caveats, refer to the most recent version of these release notes located at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/78_11318.htm

Caution We strongly recommend that you read these release notes before using your switch or upgrading your switch 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 location listed in the "Cisco.com" section on page 29.

CISCO SYSTEMS

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

78-11318-03

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 location listed in the "Cisco.com" section on page 29.

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). A software downgrade will *always* cause the configuration to be lost. 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:

System Requirements

This section describes the system requirements for the Catalyst 4000 family switches and contains the following sections:

Power Supply Requirements

The Catalyst 4006 switch requires dual power supplies.

Release 6.*x* Memory Requirements

The Catalyst 4000 family supervisor engine software release 6.*x* requires a minimum of 64-MB DRAM installed on your supervisor engine.

If your supervisor engine has less than 64-MB DRAM, you can add more memory by ordering the 32-MB DRAM upgrade (Cisco product number MEM-C4K-32-RAM=) for the Catalyst 4000 family Supervisor Engine I.

Product and Software Version Support Matrix

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

Table 1 Product and Supervisor Engine 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	4.5(8)	4.5(10)
WS-X4013	Catalyst 4006 Supervisor Engine I module	5.4(2)	5.5(5)
Ethernet, Fast Ethernet, and Gigabit Ethernet			
WS-X4148-RJ	48-port 10/100 Fast Ethernet RJ-45	4.5(8)	4.5(10)
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet		
WS-X4148-RJ45V	48-port inline power 10/100BASE-TX switching module	6.1(1)	6.1(1)

Table 1 Product and Supervisor Engine Software Version Matrix (continued)

Product Number (append with "=" for spares)	Product Description	Minimum Supervisor Engine Software Version	Recommended Supervisor Engine Software Version
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45	5.1(1)	5.5(5)
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet	4.5(8)	5.5(5)
WS-X4418-GB	18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet	4.5(8)	4.5(10)
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet switching module	5.4(2)	5.5(5)
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet switching module	5.4(2)	5.5(5)
WS-X4148-RJ21	48-port 10/100-Mbps Fast Ethernet switching module	5.4(2)	5.5(5)
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet switching module	6.2(1)	6.2(1)
Uplink Modules			
WS-U4504-FX-MT	4-port 100BASE-FX MT-RJ	5.1(1)	5.5(5)
Gigabit Interface Converters (GBICs)			
WS-G5484=	1000BASE-SX GBIC	4.5(8)	4.5(10)
WS-G5486=	1000BASE-LX/LH GBIC		
WS-G5487=	1000BASE-ZX GBIC	4.5(8)	4.5(10)
Modular Chassis			
WS-C4003	Catalyst 4003 chassis (3-slot)	4.5(8))	4.5(10)
WS-C4006-S2	Catalyst 4006 chassis (6-slot)	5.4(2)	5.5(5)
Fixed-Configuration Chassis			
WS-C2948G	Catalyst 2948G with two 1000BASE-X (GBIC) Gigabit Ethernet uplinks and 48 10/100 Fast Ethernet ports	4.5(8)	4.5(10)
WS-C4912G	Catalyst 4912G with 12 1000BASE-X (GBIC) Gigabit Ethernet ports	4.5(8)	4.5(10)
WS-C2980G	Catalyst 2980 with 80 10/100 Fast Ethernet ports and 2 1000BASE-X ports	5.4(2)	5.5(5)
WS-C2980G-A	Catalyst 2980 with 80 10/100 Fast Ethernet ports and 2 1000BASE-X ports	6.1(1)	6.1(1)

Release 6.*x* Orderable Software Images

Table 2 lists the software versions and applicable ordering information for Catalyst 4000 family supervisor engine software release 6.*x*.

Table 2 Release 6.x Orderable Software Image Matrix

Software Version	Filename	Orderable Product Number Flash on System	Orderable Product Number Spare Upgrade (Floppy Media)
Supervisor Engine I			
6.1(1)	cat4000.6-1-1.bin	SC4K-SUP-6.1.1	SC4K-SUP-6.1.1=
6.1(1) Kerberos	cat4000k4.6-1-1.bin	SC4K-SUPK4-6.1.1	SC4K-SUPK4-6.1.1=
6.1(2)	cat4000.6-1-2.bin	SC4K-SUP-6.1.2	SC4K-SUP-6.1.2=
6.1(2) Kerberos	cat4000k4.6-1-2.bin	SC4K-SUPK4-6.1.2	SC4K-SUPK4-6.1.2=
6.2(1)	cat4000.6-2-1.bin	SC4K-SUP-6.2-1	SC4K-SUP-6.2-1=
6.2(1) Kerberos	cat4000k4.6-2-1.bin	SC4K-SUPK4-6.2-1	SC4K-SUPK4-6.2-1=
Supervisor Engine II			
6.1(1)	cat4000.6-1-1.bin	SC4K-SUP-6.1.1	SC4K-SUP-6.1.1=
6.1(1) Cisco View[1]	cat4000-cv.6-1-1.bin	SC4K-SUPCV-6.1.1	SC4K-SUPCV-6.1.1=
6.1(2)	cat4000.6-1-2.bin	SC4K-SUP-6.1.2	SC4K-SUP-6.1.2=
6.1(2) Cisco View[1]	cat4000-cv.6-1-2.bin	SC4K-SUPCV-6.1.2	SC4K-SUPCV-6.1.2=
6.2(1)	cat4000.6-2-1.bin	SC4K-SUP-6.2-1	SC4K-SUP-6.2-1=

1. The 6.*x* CiscoView (CV) releases require JPI (Java Plug-in) 1.3.0 in the browser. This version is incompatible with the 5.5(3) CV and earlier releases, which require JPI 1.2.2. Software releases 5.5(4) CV and later work with JPI 1.3.0. Subsequent versions of the Java Plug-in are incompatible with software releases 5.5(4) CV and 6.*x* CV.

New Features for Supervisor Engine Software Release 6.2

This section describes the new hardware and software features available in software release 6.2.

Hardware Features

The following hardware features are new to release 6.2:

- 48-port 100BASE-FX Fast Ethernet switching module (WS-X4148-FX-MT)

Software Features

The following software features are new to software release 6.2:

- Dynamic VLAN support for VVID

  Prior to software release 6.2(1), dynamic ports could only belong to one VLAN. You could not enable the dynamic port VLAN feature on ports that carried a native VLAN and an auxiliary VLAN. With software releases 6.2(1) and later, the dynamic ports can belong to two VLANs. The switch port configured for connecting an IP phone can have separate VLANs configured for carrying the following traffic:

  – Voice traffic to and from the IP phone (auxiliary VLAN)

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

- BPDU packet filtering

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

- BPDU skew detection and syslog

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

- Loop guard

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

- IEEE 802.1x

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

- Local command accounting

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

- RSM/MSFC Autodisable

  The auto state feature shuts down (or brings up) Layer 3 interfaces and subinterfaces on the MSFC and the multilayer switch module (MSM) when port configuration changes occur on the switch.

- Private VLANs

  Private VLANs are sets of ports that have the features of normal VLANs and also provide some Layer 2 isolation from other ports on the Catalyst 4000 family switch.

- Layer 2 Traceroute

  The Layer 2 Traceroute utility allows you to identify the physical path that a packet takes when going from a source to a destination. The Layer 2 Traceroute utility determines the path by looking at the forwarding engine tables of the switches in the path.

- Multiple Instance Spanning Tree Protocol (MISTP)

  MISTP allows you to group multiple VLANs under a single instance of spanning tree. MISTP combines the Layer 2 load-balancing benefits of PVST+ with the lower CPU load of IEEE 802.1Q.

- MAC address filtering

  You can filter traffic based on a host's MAC address so that packets that are tagged with that specific source MAC address are discarded. When you specify a MAC address filter, incoming traffic from that host MAC address will be dropped and packets addressed to that host will not be forwarded.

- HC-RMON media independent table

  Provides information for full- and half-duplex links as well as high-capacity links.

- Support for the following MIBs:
  - CISCO-PRIVATE-VLAN-MIB
  - CISCO-CATOS-ACL-QOS-MIB
  - CISCO-QOS-POLICY-MIB
  - CISCO-STACK-MIB enhancement
  - CISCO-STP-EXTENSIONS-MIB enhancement
  - CISCO-VTP-MIB enhancement

New Features for Supervisor Engine Software Release 6.1

This section describes the new hardware and software features available in software release 6.1.

Hardware Features

The following hardware features are new to release 6.1:

- Power entry module (WS-X4095-PEM)
- External power shelf (WS-P4603)
- External power supply (WS-X4608)
- 48-port inline power 10/100BASE-TX switching module (WS-X4148-RJ45V)

Software Features

The following software features are new to software release 6.1:

- Ability to limit console and Telnet login attempts

  You can specify how many console and Telnet login attempts to allow and the duration of the lockout after the switch has denied a login attempt.

- Secure Shell encryption

  The Secure Shell encryption feature provides security for Telnet sessions to the switch. Secure Shell encryption supports the DES and 3DES encryption methods and can be used in conjunction with RADIUS and TACACS+ authentication.

- Spanning tree root guard

  The root guard feature forces a port to become a designated port, so that no switch on the other end of the link can become a root switch.

- **write tech-support** command

  The **write tech-support** command allows you to generate a report with status information about your switch that you can upload to a TFTP server and send to Cisco TAC.

- IOS-like ping

  The **-s** argument in the IOS-like **ping** command allows you to configure the number of packets to ping, the packet size, and the wait time before timing out a response. The wait time can be set as low as 0, which would produce a continuous ping.

- Reduced MAC address usage

  The MAC address reduction feature is used to enable extended-range VLAN identification. When MAC address reduction is enabled on Catalyst 4000 family switches, it disables the pool of MAC addresses used for the VLAN spanning tree, leaving a single MAC address that identifies the switch.

- Configuration file text search
- At the --more-- prompt during a **show** command, enter a forward slash character ("/") followed by a text string to search for text.
- Globally disable EtherChannel

  To disable all EtherChannels on the switch, you can enter the **set port channel all mode off** command. To disable all trunks on the switch, enter the **set trunk all off** command.

- Enhanced support for scripting

  The switch assumes a positive ("yes") answer to all the confirmation prompts when configured from a configuration file.

- SNMP group access context

  When defining the access rights of an SNMP group, you can specify a context string and the method to match the context string.

- System warnings—error counters

  When the count differs from the previous poll, selected debug port counters are polled at a fixed interval and warnings are generated.

Open and Resolved Caveats in Software Release 6.2(1)

This section describes the open and resolved caveats in supervisor engine software release 6.2(1):

- Open Caveats in Software Release 6.2(1), page 8
- Resolved Caveats in Software Release 6.2(1), page 10

Open Caveats in Software Release 6.2(1)

This section describes open caveats in software release 6.2(1):

Note For the most recent information on open caveats, refer to the most recent version of these release notes located at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/78_11318.htm

- Multicast and broadcast traffic on the WS-X4013 module might experience lost packets when hosts join or leave a multicast/broadcast group. (CSCdp38859)
- The 1000BASE-T ports on the WS-X4412-2GB-T module may take up to two minutes to come online.

  Workaround: Connect the port to another device and then reconnect to the desired device. As a final option, you can reset the module. (CSCdp90760)
- In some cases, a switch port connected to an Intel Pro100+ management adapter might lose and regain a link independent of any action that would cause such behavior. The problem occurs intermittently and for a short period. There is no workaround. (CSCdm76616)
- If protocol filtering is enabled and you have set some protocols to be filtered on a port, such as the IPX protocol with the **set port protocol 2/3 ipx off** command, and then you change the port to a trunk port with the **set trunk** command, the trunk port will have the same settings as it did before it was an access port. However, when you enter the **show port protocol** command, the display shows that all protocols are allowed. (CSCds05967)

  Workaround: If protocol filtering is enabled on the switch, and a port that had some protocol filtering configured on it is changed to a trunk port, explicitly configure the trunk port to allow all protocols by entering one of the following commands for each protocol:

  – **set port protocol** *mod_num*/*port_num* **ipx on**

  – **set port protocol** *mod_num*/*port_num* **ip on**

  – **set port protocol** *mod_num*/*port_num* **group on**
- Some Sun Gigabit Ethernet NICs do not reliably autonegotiate flow control with some ports on the Catalyst 4000 family oversubscribed Gigabit Ethernet modules. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

  These Sun Gigabit Ethernet NICs are affected:

  – X1140A Sun Gigabit Ethernet Sbus Adapter 2.0

  – X1141A PCI Gigabit Ethernet PCI Adapter 2.0

  Workaround: Use the following configuration:

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

1. Default setting

(CSCdm38405)

Resolved Caveats in Software Release 6.2(1)

This section describes resolved caveats in software release 6.2(1):

- On a Catalyst 4006 switch with a Supervisor Engine II, switch ports in the same VLAN may lose connectivity with one another. This loss of connectivity results in a VLAN appearing to be partitioned into several isolated segments. A host may be able to ping one set of devices in its VLAN, but it cannot ping another set of devices in the same VLAN.

  This loss of connectivity is independent of the slot a module is installed in. The same set of ports on a module are affected regardless of the slot that the module is installed in. This problem is resolved in software release 6.2(1). (CSCdt80707)

- If the native VLAN for a port is cleared from the port's trunk allowed range, this port does not appear to be in the native VLAN in the configuration file. This problem is resolved in software release 6.2(1). (CSCdr31412)

- Occasionally removing and reinserting a module can cause a memory leak which can impair functionality or crash the switch. This problem is resolved in software release 6.2(1). (CSCds55847)

- The switch might reset if you attempt to delete a nonexistent VLAN through the SNMP vtpVlanEditTable. This problem is resolved in software release 6.2(1). (CSCdt38160)

- The **show ip permit** command might cause the switch to reset. This problem is resolved in software release 6.2(1). (CSCdt55237)

- When the system runs out of memory, the following messages are printed when you execute a **show** command:

  ```
  Failed to allocate session block.

  Error: can't find scp/slp buffer slot for show command:29.
  ```

  These messages are printed because the **show** command cannot allocate the required memory for the **show** command process. Add more memory to the system or disable some features to free up existing memory. This problem is resolved in software release 6.2(1). (CSCdr74107)

- If you force a new root in an IEEE spantree by using the **set spantree priority** command, the port may appear as a type inconsistent (type-pvid-inconsistent). This problem is resolved in software release 6.2(1). (CSCds68230)

- Disabling spanning tree on a native VLAN on a non-root switch may result in the switch attempting to become a root on VLAN 1. This is not a problem when disabling spanning tree in other VLANs. This problem is resolved in software release 6.2(1). (CSCds23433)

- On IEEE 802.1Q trunk ports with several hundred active VLANs, spanning tree convergence time might be delayed up to several minutes when the last trunk goes down or the first trunk comes up, depending on the number of active VLANs. The 802.1Q trunk port will eventually enter the correct spanning tree state for each active VLAN. This problem is resolved in software release 6.2(1). (CSCds06965)

- Some 10/100 ports flap link with no cables connected to them. This has been observed only when the port is forced to 10 Mbps and half duplex. This problem is resolved in software release 6.2(1). (CSCdt39972)

- If you run a script that contains any **show** command followed by several **Ctrl-C** characters, the switch may crash. This problem is resolved in software release 6.2(1). (CSCdt30178)

- When configured as an NTP client, the Catalyst 4000 family switch incorrectly reports summertime. The reported summertime end time is advanced by one year. The **show ntp** command displays the following information:

```
Console> (enable) show ntp

 Current time: Tue Feb 13 2001, 20:50:21 NZDT
 Timezone: 'NZST', offset from UTC is 12 hours
 Summertime: 'NZDT', enabled
   Start : Sun Oct 1 2000, 02:00:00
   End   : Sun Mar 17 2002, 03:00:00      <========= Here is the problem
   Offset: 60 minutes
 Last NTP update: Tue Feb 13 2001, 20:49:27
```

  This problem is resolved in software release 6.2(1). (CSCdt43350)

- When you upgrade the supervisor engine software on a WS-X4013 supervisor engine module, the supervisor engine may hang and require a manual reset. When this happens, often this last message is displayed:

```
Upgrade NVRAM successful.
```

  This problem can occur when upgrading to any 5.4(*x*) release, any 5.5(*x*) release prior to 5.5(7), or any 6.1(*x*) release prior to 6.2(1). This fix also covers all cases described in CSCdr96136. This problem is resolved in software release 6.2(1). (CSCdt69490)

Open and Resolved Caveats in Software Release 6.1(2)

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

- Open Caveats in Software Release 6.1(2), page 11
- Resolved Caveats in Software Release 6.1(2), page 13

Open Caveats in Software Release 6.1(2)

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

Note For the most recent information on open caveats, refer to the most recent version of these release notes located at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/78_11318.htm

- Disabling spanning tree on a native VLAN on a non-root switch may result in the switch attempting to become a root on VLAN 1. This situation is not a problem when disabling spanning tree in other VLANs. (CSCds23433)
- Multicast and broadcast traffic on the WS-X4013 module might experience lost packets when hosts join or leave a multicast/broadcast group. (CSCdp38859)
- If you force a new root in an IEEE spanning tree by using the **set spantree priority** command, the port may appear as a type inconsistent (type-pvid-inconsistent). This problem is resolved in software release 6.2(1). (CSCds68230)
- The 1000BASE-T ports on the WS-X4412-2GB-T modules may take up to two minutes to come online.

Workaround: Connect the port to another device and then reconnect to the desired device. As a final option, you can reset the module. (CSCdp90760)

- In some cases, a switch port connected to an Intel Pro100+ management adapter might lose and regain a link independent of any action that would cause such behavior. The problem occurs intermittently and for a short period. There is no workaround. (CSCdm76616)
- On IEEE 802.1Q trunk ports with several hundred active VLANs, spanning tree convergence time when the last trunk goes down or the first trunk comes up might 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. (CSCds06965)
- Some Sun Gigabit Ethernet NICs do not reliably autonegotiate flow control with some ports on the Catalyst 4000 family oversubscribed Gigabit Ethernet modules. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

  These Sun Gigabit Ethernet NICs are affected:

  – X1140A Sun Gigabit Ethernet Sbus Adapter 2.0

  – X1141A PCI Gigabit Ethernet PCI Adapter 2.0

  Workaround: Use the following configuration:

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

1. Default setting

(CSCdm38405)

- If protocol filtering is enabled and you have set some protocols to be filtered on a port, such as the IPX protocol with the **set port protocol 2/3 ipx off** command, and then you change the port to a trunk port with the **set trunk** command, the trunk port will have the same settings as it did before it was an access port. However, when you enter the **show port protocol** command, the display shows that all protocols are allowed. (CSCds05967)

  Workaround: If protocol filtering is enabled on the switch, and a port that had some protocol filtering configured on it is changed to a trunk port, explicitly configure the trunk port to allow all protocols by entering one of the following commands for each protocol:

  – **set port protocol** *mod_num*/*port_num* **ipx on**

  – **set port protocol** *mod_num*/*port_num* **ip on**

  – **set port protocol** *mod_num*/*port_num* **group on**

Resolved Caveats in Software Release 6.1(2)

This section describes resolved caveats in software release 6.1(2):

- Occasionally, an SNMP mibwalk on a very busy switch can crash the switch. This problem only exists in software release 5.5(4) and has been resolved in software release 6.1(2). (CSCds79550)
- 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. (CSCds84051)
- The WS-X4124-FX-MT and WS-U4504-FX-MY modules will sometimes produce the following error message if the traffic the module receives traffic on one of its ports while booting:

  ```
  SYS-3-MON_MINORFAIL:Minor problem in module #
  ```
  In this case, some or all of the 100-FX ports will be faulty. (CSCds25826)
- If you configure the SPAN after entering the **clear config all** command, the SPAN configuration will be erased during the next system reboot. (CSCds54788)
- Prior to software releases 4.5(10), 5.5(5) and 6.1(2), SNMP processed UDP packets with the destination port 0. (CSCds65753).
- The Catalyst 4000 family switches declare that a host is flapping if it moves locations twice in 15 seconds. As a response to the host flap, the switch suppresses all traffic destined to the host for up to 15 seconds. If you have a configuration where a host can briefly (one packet) appear on a different port, this will cause problems.

  In software releases 6.1(2), 6.2(1), and 5.5(4), the algorithm has been made less aggressive. A host must move at least 4 times in 15 seconds before being declared to be flapping. As a response to the host flap, the switch still suppresses all traffic destined to and from that host for up to 15 seconds. (CSCds05573).
- Under certain circumstances, changing the auxiliary VLAN of one of the ports belonging to a channel on the WS-X4148-RJ45V module places the port in errdisable mode. (CSCdr88895)
- If you change management VLAN (VLAN assigned to the sc0 interface) on the supervisor engine, no ports remain connected on the old management VLAN. The old management VLAN corresponds to an interface on the WS-X4232-L3_module. This interface was in the up state before management VLAN changed, then the interface does not go to the shutdown state but stays in the up state. Using the Auto Port State feature, the module should have gone down. Traffic that used to go to the old management VLAN is dropped by the switch after passing through the WS-X4232-L3 module, and the ICMP “host unreachable” message will not be sent. (CSCds36572)
- When using the redundant power supply alone, the Catalyst 4912 and Catalyst 2948G switches report the AC power supply as faulty. (CSCdm68030)
- IPX clients may be unable to connect to a server during bootup. (CSCds27476)
- A crash log is not appended to the **show log** command output. Use the **show crashdump** command to display the crash log. (CSCdp38333)
- If you configure level 2 system logging and a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values, and sometimes a reload might occur. (CSCds23497)
- 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. (CSCds08837)

- When you enter the **clear config all** command and reset the system, the ifIndex does not reset. The problem also occurs after a switchover from the active supervisor engine to the redundant supervisor engine. This problem appears in software releases 5.4(1) and later. (CSCds34328)
- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90 percent, some **show** commands might not work, and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) show version
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  (CSCds30395)
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a "bad value" error message. The problem exists in software releases 5.*x* and 6.1(1). (CSCds22815)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)
- After resetting a WS-X4604-GWY module, but before it has come online (that is, its status shows as "other" in the **show module** command), the **show sprom** command resets the Catalyst 4000 switch. (CSCds33864).

Open and Resolved Caveats in Software Release 6.1(1c)

This section describe the open and resolved caveats in supervisor engine software release 6.1(1c):

- Open Caveats in Software Release 6.1(1c), page 14
- Resolved Caveats in Software Release 6.1(1c), page 16

Open Caveats in Software Release 6.1(1c)

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

Note For the most recent information on open caveats, refer to the most recent version of these release notes located at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/78_11318.htm

- Multicast and broadcast traffic on the WS-X4013 module might experience lost packets when hosts join or leave a multicast/broadcast group. (CSCdp38859)
- The 1000BASE-T ports on the WS-X4412-2GB-T modules may take up to two minutes to come up.

  Workaround: Connect the port to another device and then reconnect to the desired device. As a final option, you can reset the module. (CSCdp90760)
- In some cases, a switch port connected to an Intel Pro100+ management adapter might lose and regain a link independent of any action that would cause such behavior. The problem occurs intermittently and for a short period. There is no workaround. (CSCdm76616)

- If you configure level 2 system logging and if a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. (CSCds23497)
- Some Sun Gigabit Ethernet NICs do not reliably autonegotiate flow control with some ports on the Catalyst 4000 family oversubscribed Gigabit Ethernet modules. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

  These Sun Gigabit Ethernet NICs are affected:

  – X1140A Sun Gigabit Ethernet Sbus Adapter 2.0

  – X1141A PCI Gigabit Ethernet PCI Adapter 2.0

  Workaround: Use the following configuration:

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

1. Default setting

  (CSCdm38405)

- On the Catalyst 4000 family switch, SNMP mibwalks of the dynamically learned hosts are very slow. (CSCds30442)
- Under certain circumstances, changing the auxiliary VLAN of one of the ports belonging to a channel places the port in errdisable mode. (CSCdr88895)

  Workaround: If you need to change the auxiliary VLAN of a port, verify that the port is not part of a channel. If the port is part of a channel, remove it from the channel. This should not be a limitation because the auxiliary VLAN is used when connecting the Cisco IP phone to the port, which will not be part of a channel.
- 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. (CSCds08837)
- On IEEE 802.1Q trunk ports with several hundred active VLANs, spanning tree convergence time when the last trunk goes down or the first trunk comes up might 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. (CSCds06965)
- After resetting a WS-X4604-GWY module, but before it has come online (its status shows as "other" in the **show module** command), the **show sprom** command resets the Catalyst 4000 switch. (CSCds33864).

  Workaround: Wait until the module is online before issuing the **show sprom** command.

- If protocol filtering is enabled and you have set some protocols to be filtered on a port, such as the IPX protocol with the **set port protocol 2/3 ipx off** command, and then you change the port to a trunk port with the **set trunk** command, the trunk port will have the same settings as it did before it was an access port. However, when you enter the **show port protocol** command, the display shows that all protocols are allowed. (CSCds05967)

  Workaround: If protocol filtering is enabled on the switch, and a port that had some protocol filtering configured on it is changed to a trunk port, explicitly configure the trunk port to allow all protocols by entering one of the following commands for each protocol:

  – **set port protocol** *mod_num*/*port_num* **ipx on**

  – **set port protocol** *mod_num*/*port_num* **ip on**

  – **set port protocol** *mod_num*/*port_num* **group on**

- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a “bad value” error. The problem exists in software releases 5.x and 6.1(1).

  Workaround: Use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. (CSCds22815)

- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)

- When you enter the **clear config all** command and reset the system, the ifIndexdoes not reset. The problem also occurs after a switchover from the active supervisor engine to the standby supervisor engine. This problem appears in software releases 5.4(1) and later. (CSCds34328)

- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90 percent, some **show** commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) show ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  Workaround: If most of the memory was used by RMON buckets, use one of the following workarounds:

  – Reduce the number of buckets for each entry.

  – Reduce the number of control entries.

  – Disable the RMON feature.

  (CSCds30395)

Resolved Caveats in Software Release 6.1(1c)

This section describes resolved caveats in software release 6.1(1c):

- Non-SSH connection attempts to an enabled SSH service on a Catalyst 4000 family switch might cause a “protocol mismatch” error, resulting in a supervisor engine failure. The supervisor engine failure causes the switch to fail to pass traffic and reboots the switch. This problem is resolved in software release 6.1(1c). (CSCds85763)

Open and Resolved Caveats in Software Release 6.1(1)

This section describe the open and resolved caveats in supervisor engine software release 6.1(1):

Open Caveats in Software Release 6.1(1)

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

Note For the most recent information on open caveats, refer to the most recent version of these release notes located at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/78_11318.htm

- Multicast and broadcast traffic on the WS-X4013 module might experience lost packets when hosts join or leave a multicast/broadcast group. (CSCdp38859)
- The 1000BASE-T ports on the WS-X4412-2GB-T modules may take up to two minutes to come online.

  Workaround: Connect the port to another device and then reconnect to the desired device. As a final option, you can reset the module. (CSCdp90760)
- In some cases, a switch port connected to an Intel Pro100+ management adapter might lose and regain a link independent of any action that would cause such behavior. The problem occurs intermittently and for a short period. There is no workaround. (CSCdm76616)
- Under certain circumstances, changing the auxiliary VLAN of one of the ports belonging to a channel places the port in errdisable mode. (CSCdr88895)

  Workaround: If you need to change the auxiliary VLAN of a port, verify that the port is not part of a channel. If the port is part of a channel, removed it from the channel. This should not be a limitation because the auxiliary VLAN is used when connecting the Cisco IP phone to the port, which will then not be part of a channel.
- If you configure level 2 system logging and if a native VLAN mismatch occurs on 802.1Q trunks, the system log messages contain incorrect module and port values and sometimes a reload might occur. (CSCds23497)
- Some Sun Gigabit Ethernet NICs do not reliably autonegotiate flow control with some ports on the Catalyst 4000 family oversubscribed Gigabit Ethernet modules. The 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet module (WS-X4418-GB) is affected.

  These Sun Gigabit Ethernet NICs are affected:
  - X1140A Sun Gigabit Ethernet Sbus Adapter 2.0
  - X1141A PCI Gigabit Ethernet PCI Adapter 2.0

Workaround: Use the following configuration:

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

1. Default setting

(CSCdm38405)

- 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. (CSCds08837)
- On IEEE 802.1Q trunk ports with a large number of active VLANs (several hundred), spanning tree convergence time when the last trunk goes down or the first trunk comes up might 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. (CSCds06965)
- After resetting a WS-X4604-GWY module, but before it has come online (its status shows as "other" when you enter the **show module** command), the **show sprom** command resets the Catalyst 4000 family switch. (CSCds33864).

  Workaround: Wait until the module is online before entering the **show sprom** command.
- If protocol filtering is enabled and you have set some protocols to be filtered on a port, such as the IPX protocol with the **set port protocol 2/3 ipx off** command, and then you change the port to a trunk port with the **set trunk** command, the trunk port will have the same settings as it did before it was an access port. However, when you enter the **show port protocol** command, the display shows that all protocols are allowed. (CSCds05967)

  Workaround: If protocol filtering is enabled on the switch, and a port that had some protocol filtering configured on it is changed to a trunk port, explicitly configure the trunk port to allow all protocols by entering one of the following commands for each protocol:

  – **set port protocol** *mod_num*/*port_num* **ipx on**

  – **set port protocol** *mod_num*/*port_num* **ip on**

  – **set port protocol** *mod_num*/*port_num* **group on**
- The switch does not allow you to create a second etherStatsEntry with the same ifIndex for an interface. When you try to create the second etherStatsEntry with the same interface in etherStatsDataSource as one of the existing entries, the switch returns a "bad value" error. The problem exists in software releases 5.x and 6.1(1a).

  Workaround: Use the existing etherStatsEntry for the interface or create a new one after deleting the existing entry that has the same ifIndex. (CSCds22815)

- On the Catalyst 4000 family switch, SNMP mibwalks of the dynamically learned hosts are very slow. (CSCds30442)
- Allocating too many buckets in RMON might cause memory allocation errors. When system memory usage reaches 90 percent, some **show** commands might not work and new Telnet sessions might not be allowed. An example follows:

```
Console> (enable) show ver
 Failed to allocate session block.
 Error: can't find scp/slp buffer slot for show command: 10.
Console> (enable)
```

  Workaround: If most of the memory was used by RMON buckets, use one of the following workarounds:

  – Reduce the number of buckets for each entry.

  – Reduce the number of control entries.

  – Disable the RMON feature.

  (CSCds30395)
- Setting ntpAuthenticationSecretKey from SNMP does not have any effect. (CSCdk75107)
- When you enter the **clear config all** command and reset the system, the ifIndexdoes not reset. The problem also occurs after a switchover from the active supervisor engine to the redundant supervisor engine. This problem appears in software releases 5.4(1) and later. (CSCds34328)

Resolved Caveats in Software Release 6.1(1)

This section describes resolved caveats in software release 6.1(1):

- The hcRMONCapabilities MIB object is not supported in the supervisor engine RMON software. RMON applications, such as TrafficDirector that depend on the hcRMONCapabilities MIB value, might fail to discover the HC-RMON capability of a device. (CSCdr89597)
- For normal UDLD the recommended default interval is 15 seconds. Caveat CSCdr50206 requires that you follow these configurations:

  – When you enable aggressive UDLD, the recommended default is 30 seconds.

  – Do not use UDLD, with the ON - AUTO trunk combination; however, UDLD can be used with any other valid trunk combination. (CSCdr50206)
- When a 10/100 port receives an invalid packet with a length of less than 64 bytes, both the Runts and FCS-Error counters increment on the port. The correct operation is to increment only the Runts counter when receiving an undersized or invalid packet. 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)

Usage Guidelines, Restrictions, and Troubleshooting

This section provide usage guidelines, restrictions, and troubleshooting information for Catalyst 4000 family switch hardware and software.

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:

- The Catalyst 4006 switch requires dual power supplies. Refer to the *Catalyst 4003 and 4006 Switch Installation Guide* for detailed information about power requirements for the Catalyst 4000 family switches.
- In supervisor engine software release 5.2 and later, the **show config**, **write terminal**, and **copy config** commands return only the nondefault configuration (that is, only commands that change the default configuration are displayed). Use the **all** keyword to display both the default and nondefault configuration (for example, **show config all**).
- 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.

  Workaround: 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 causes the PortFast feature to be ignored 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:

- This message indicates a problem with hardware:

  ```
  2000 Feb 15 16:15:28 %SYS-4-P2_WARN: 1/Blocked queue on gigaport 5 ( 15 : 1 )
  ```

  In this case, the gigaport number is 5. If you receive this message, contact your technical support representative.

- When you connect end stations (such as Windows 95, 98, or NT workstations) to Catalyst 4000 family 10/100-Mbps switch ports, we recommend this configuration:
  - Spanning tree PortFast enabled
  - Trunking off
  - Channeling off

  In supervisor engine software release 5.2 and later, you can use the **set port host** command to optimize the port configuration for host connections. This command automatically enables PortFast and sets the trunking and channeling modes to **off**.

  In software releases prior to release 5.2, you can optimize the port configuration for host connections as follows:

  - Use the **set spantree portfast** *mod_num/port_num* **enable** command to enable PortFast on a port.
  - Use the **set trunk** *mod_num/port_num* **off** command to disable trunking on a port.
  - 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 using the **set port host** command:

```
Console> (enable) set port host 2/1

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 2/1 fast start enabled.
Port(s) 2/1 trunk mode set to off.
Port(s) 2/1 channel mode set to off.

Console> (enable)
```

This example shows how to manually 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 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 and 4006 Switch Installation Guide*.
- 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, entering the command **clear config** *mod_num* clears the module configuration information in the supervisor engine and obtains the correct spanning tree parameters.
- If a module fails to come online, reset the module by entering the **reset** *mod_num* command.
- If a port fails the physical-medium-dependent (PMD) loopback test (that is, if a port LED is flashing orange) after the Catalyst 4000 family switch is reset, you must reset the affected module.
- 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 speed is set to **auto** and is 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.
- Whenever you connect a Catalyst 4000 family port that is set to autonegotiate an end station or another networking device, make sure that the other device also is configured for autonegotiation. 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.
- Do not enable protocol filtering on the switch if you have configured port security on any ports and set the violation mode to **restrict**. There is no restriction if the violation mode is set to **shutdown**; you can enable protocol filtering on the switch.
- The following restrictions apply when configuring port security:
  - You cannot configure dynamic, static, or permanent CAM entries on a secure port.
  - When you enable port security on a port, any static or dynamic CAM entries associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.
- If you configure a secure port to restrictive mode and a station is connected to the port whose MAC address is already configured as a secure MAC address on another port on the switch, the port in restrictive mode will shut down rather than restrict traffic from that station. For example, if you configure MAC-1 as the secure MAC address on port 2/1 and MAC-2 as the secure MAC address on port 2/2, and you then connect the station with MAC-1 to port 2/2 when port 2/2 is configured for restrictive mode, port 2/2 will shut down instead of restricting traffic from MAC-1.

- 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.

Spanning Tree

This section contains usage guidelines, restrictions, and troubleshooting information that apply to 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 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.
- If the STP parameters are reduced in value, be sure that the number of STP instances are also reduced proportionally in order to avoid spanning tree loops in the network.
- On your Catalyst 4000 family switch, be sure that the total number of logical ports across all instances of spanning tree for different VLANs does not exceed the number allowed for your supervisor engine.

  You can use the **show spantree summary** command and the following formula to compute the sum of logical ports on the switch:

  (number of trunks on the switch × number of active VLANs on those trunks) + number of nontrunking ports on the switch

  The sum of all logical ports, as calculated with the formula above, should be less than or equal to 1500 for the Catalyst 4000 family Supervisor Engine I and II.

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 sent by a Catalyst family switch only if it is the root bridge.
- Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk may 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 it on every VLAN in the network to ensure that a loop-free topology exists.

- To monitor blocked spanning tree ports, use the following commands:
  - Use the **show port** command to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs.
  - Use the **show mac** command if the Inlost counter increments continuously or a 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, ensure that the trunk configuration is valid on both sides of the link.
- On trunk ports, ensure 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 such ports.

VTP, VLANs, and VLAN Trunks

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

- The VLAN numbers are always ISL VLAN identifiers and not 802.1Q VLAN identifiers.
- 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 non-Catalyst 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 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 a trunk using 802.1Q encapsulation, traffic cannot be carried successfully on the native VLAN for the trunk configured on a Catalyst 4000 family switch.

  Workaround: Create an unused VLAN and assign it 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)

- A VTP transparent switch with no VTP domain name configured might not relay VTP requests received from VTP client and server switches. Therefore, VTP client and server switches might not synchronize if they are separated by a VTP transparent switch with no domain name configured.

  Workaround: Configure a VTP domain name on the VTP transparent switch.

- IEEE 802.1Q trunks with several hundred active VLANs take a few minutes to become operational. The time increases with the number of VLANs on the trunk. During this time, you may see unexpected behavior, such as the console hanging or other ports not going into forwarding. After the trunks become operational, the unexpected behavior disappears and operation returns to normal. The operation remains normal as long as the trunks remain operational.

EtherChannel

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

- 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 reenable the ports by entering the **set port enable** command. Valid EtherChannel configurations include:

Port Channel Mode	Valid Neighbor Port Channel Modes
desirable	**desirable** or **auto**
auto	**desirable** or **auto**[1]
on	**on**
off	**off**

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

- 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 reenable the ports. In addition, it might take up to two minutes to unbundle a channel after changing the channel mode.

SPAN

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

- By default, incoming traffic on the SPAN destination port is disabled. 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:

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

CiscoView Images

The CiscoView 6.*x* release requires Java Plug-in 1.3.0 in the browser. This version is incompatible with the CiscoView 5.5(3) and earlier releases which require the Java Plug-in 1.2.2. Cisco View software releases 5.5(4) and later work with Java Plug-in 1.3.0. Subsequent versions of the Java Plug-in are incompatible with software releases 5.5(4) CV and 6.*x* CV.

Software Documentation Updates for Release 6.1

This section describes caveats for the Catalyst 4000 family software release 6.1 documentation. These changes will be included in the next update to the documentation.

- Refer to the online versions of the *Command Reference—Catalyst 5000 Family, Catalyst 4000 Family, Catalyst 2926G, Catalyst 2948G, Catalyst 2980G Switches* for software releases 5.5, and 5.4 and the *Command Reference—Catalyst 4000 Family, Catalyst 2926G, Catalyst 2948G, Catalyst 2980G Switches* for software release 6.1 for information about these two commands supported in software release 5.4(1) and later:

  set traffic monitor *threshold*
  show traffic

- The *Software Configuration Guide—Catalyst 4000 Family, 2948G, and 2980 Switches* for software release 6.1 incorrectly lists the following two restrictions for aggressive UDLD:
  - When enabling aggressive UDLD, the recommended default is 30 seconds.
  - We recommend that you do not use UDLD or aggressive UDLD with the ON - AUTO trunk combination. UDLD and aggressive UDLD can be used with any other valid trunk combination.

  Refer to the online version of the *Software Configuration Guide—Catalyst 4000 Family, 2948G, and 2980 Switches* for a current version of this publication at

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/rel_6_1/config/index.htm
- Refer to the online versions of the *System Message Guide—Catalyst 6000, 5000, 4000, 2948G, 2926G and 2926 Series Switches* for releases 5.4, 5.5, and 6.1 for information on the following system log error messages:

  ```
  SYS-5-SYS_HITRFC: [dec] traffic load exceeded threshold on switching bus
  SYS-5-HITRFC3: [dec] traffic load exceeded threshold on switching bus [chars]
  SYS-3-SYS_MEMLOW: [chars][dec]
  SYS-3-SYS_MEMERR: Out of range while freeing address [chars]
  SYS-3-INBAND_NORESOURCE: Inband resource error warning [dec]
  SYS-3-INBAND_SPRINTR: inband spurious interrupt occurred [dec]
  SYS-3-PORT_ERR: port [dec]/[dec] swBusResultEvent [dec]
  SYS-3-PORT_WARN: port [dec]/[dec] dmaTxFull [dec] dmaRetry [dec]
  IP-3-UDP_SOCKOVFL: UDP socket overflow [dec]
  IP-3-TCP_SOCKOVFL: TCP socket overflow [dec]
  IP-3-UDP_BADCKSUM: UDP bad checksum [dec]
  IP-3-TCP_BADCKSUM: UDP bad checksum [dec]
  SPANTREE-5-PORTLISTEN: Port [dec]/[dec] state in VLAN 1 changed to listening
  SPANTREE-5-TR_PORTLISTEN: Trcrf 101 in trbrf 102 state changed to listening
  ```

Related Documentation

The following documents are available for Catalyst 4000 family switches:

- *Catalyst Family Switch Installation Guide*
- *Catalyst 4912G Installation Guide*
- *Software Configuration Guide—Catalyst 4000 Family, 2948G, and 2980 Switches*
- *Layer 3 Switching Software Configuration Guide—Catalyst 5000 Family, 4000 Family, 2926G Series, and 2948G Switches*
- *Command Reference—Catalyst 4000 Family, 2948G Series, and 2980 Switches*
- *System Message Guide—Catalyst 6000 Family, Catalyst 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980 Switches*
- *Troubleshooting Tips—Catalyst 5000 Family, 4000 Family, 2926G Series, and 2948G Switches*
- *Enterprise MIB User Quick Reference* (online only)

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.

P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 27.