



Text Part Number: OL-4923-01

Release Notes for the Catalyst 2900 Series XL Cisco IOS Release 11.2(8.3)SA3

February 12, 1999

These release notes describe the features and caveats for Cisco IOS Release 11.2(8.3)SA3. Changes since the 11.2(8.3)SA3 release are marked with change bars.

Catalyst 2900 series XL switches are supported by a special release of Cisco IOS software that is not released on the same eight-week maintenance cycle that is used for other platforms. As maintenance releases and future Cisco IOS releases become available, they will be posted to CCO in the Cisco IOS software area.

The product documentation for the Catalyst 2900 series XL switches and the Catalyst 2900 series XL modules is as follows:

Catalyst 2900 Series XL Installation and Configuration Guide

Catalyst 2900 Series XL Modules Installation Guide

Catalyst 2900 Series XL Command Reference (online only)

Quick Start: Catalyst 2900 Series XL Cabling and Setup

Release Notes for the Catalyst 2900 Series XL Cisco IOS 11.2(8)SA

Release Notes for the Catalyst 2900 Series XL Cisco IOS 11.2(8)SA1

Release Notes for the Catalyst 2900 Series XL Cisco IOS 11.2(8)SA2

Corporate Headquarters

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

Copyright © 1998
Cisco Systems, Inc.
All rights reserved.

Important Notes

Please review the subjects in this section before you begin using the switch.

Supported Browsers and Operating Systems

To ensure full functionality of the Cisco Visual Switch Manager Software and Cisco Switch Network View software, use the browser and operating system versions listed in Table 1 and Table 2.

Table 1 Browser Requirements for Cisco Visual Switch Manager Software

Operating System	Netscape Communicator	Microsoft Internet Explorer
Windows 95 Service Pack 1, Windows 98	4.03 or higher	4.01 Service Pack 1 (SP1)
Windows NT (Service Pack 3 recommended)	4.03 or higher	4.01 Service Pack 1 (SP1)
Solaris 2.5.1 or higher, with the SUN recommended patch cluster for that operating system and Motif library patch 103461-24.	4.03 or higher	–

Table 2 Browser Requirements for Cisco Switch Network View

Operating System	Netscape Communicator	Microsoft Internet Explorer
Windows 95 Service Pack 1 (SP1), Windows 98	4.06 or higher	4.01 Service Pack 1 (SP1)
Windows NT, (Service Pack 3 recommended)	4.06 or higher	4.01 Service Pack 1 (SP1)
Solaris 2.5.1 or higher, with the SUN recommended patch cluster for that operating system and Motif library patch 103461-24.	4.06 or higher	–

Browser Notes

Cisco Visual Switch Manager, hereafter referred to as the manager software, and Cisco Switch Network View, hereafter referred to as the network view, both check the browser version before they start. If the browser version is not supported, a message is displayed. If the browser version is supported for the manager software but not for the network view, a separate message displays, and the network view does not start.

When using Internet Explorer version 4.01, only edge devices connected to the primary switch are displayed in the network view. Internet Explorer does not support horizontal scroll bars; however, all other functionality is similar to that offered for Netscape Communicator.

You can download Netscape Communicator from <http://www.netscape.com>.

You can download Microsoft Internet Explorer from <http://www.microsoft.com/ie/download>.

Operating System Notes

Solaris 2.5.1 must be running the recommended patch cluster for that operating system and Motif library patch 103461-24 available from Sun Microsystems at <http://www.sun.com>.

Windows NT servers and workstations must be running Service Pack 3.

Windows 95 must be running Service Pack 1.

Minimum Screen Resolution

To operate the network view, you need a minimum screen resolution of 1024x768 pixels. Up to 256 colors are supported.

Network View Tested Configurations

The network view was tested using the following configurations:

PC	Sun Workstation
Pentium processor running at 230 MHz	Sun Ultra 1 running at 143 MHz
64-MB RAM	64-MB RAM
Operating systems: Windows 95, Windows NT, and Windows 98	Operating systems: Solaris 2.5.1 with all minimum recommended Sun patches
Browsers: Netscape 4.06, Netscape 4.5 B1 and Internet Explorer 4.0 (SP1)	Browsers: Netscape 4.06, Netscape 4.5 B

Configuring Netscape Communicator

Follow these steps to configure Netscape Communicator:

- Step 1** Start Netscape Communicator 4.03 or higher.
- Step 2** From the menu bar, select **Edit>Preferences**.
- Step 3** In the Preferences window, click **Advanced**.
 - (a) Select the **Enable Java**, **Enable JavaScript**, and **Enable Style Sheets** check boxes.
 - (b) Click **OK** to return to the browser home page.
- Step 4** From the menu bar, select **Edit>Preferences**.
 - (a) In the Preferences window, click **Advanced Cache**, and select **Every time**.
 - (b) Click **OK** to return to the browser home page.

Configuring Microsoft Internet Explorer

Follow these steps to configure Microsoft Internet Explorer:

- Step 1** Start Internet Explorer 4.01.
- Step 2** From the menu bar, select **View>Internet Options**.
- Step 3** In the Internet Options window, click **Advanced**.
 - (a) Scroll through the list of options until you see Java VM. Select the **Java JIT compiler enabled** and **Java logging enabled** check boxes.
 - (b) Click **Apply**.
 - (c) Click **General**. In the Temporary Internet Files section, click **Settings**. The Settings window opens.
- Step 4** Click **Every visit to the page**, and click **OK**.

- Step 5** In the Internet Options window, click **Security**.
- In the Zone drop-down list, select **Trusted Sites Zone**.
 - In the Trusted Sites Zone section, click **Custom**.
 - Click **Settings**.
- Step 6** Select **Java>Java Permissions** section, and select **Custom**.
Click **Java Custom Setting**, which appears at the bottom of the window.
- Step 7** In the Trusted Sites Zone window, click **Edit Permissions**.
- If the buttons under **Run Unsigned Content** are grayed out, select either **Medium** or **Low** security at the bottom of the window in the Reset Java Permissions list box. Click **Reset**.
 - Under **Run Unsigned Content**, select **Enable**, and click **OK**.
- Step 8** In the Security Settings window, click **OK**.
- Step 9** In the Internet Options window, click **Security**.
- Verify that the Zone drop-down list is set to **Trusted Sites Zone**.
 - In the Trusted Sites Zone section, click **Add Sites**.
- Step 10** In the Trusted Sites Zone window, deselect the **Require server verification** check box.
- In the **Add this Web site to the Zone** field, enter the switch IP address.
For example, enter: **http://172.20.130.40**
 - Click **Add**, and then click **OK**.

Note You must enter all stack-switch IP addresses as trusted sites, or you will not be able to retrieve device and link reports for those devices. You do not need to enter edge-device IP addresses.

- Step 11** In the Internet Options window, click **Apply**, and then click **OK**.

Upgrading to New Releases of Cisco IOS Software

You can use the Cisco IOS Release 11.2(8.3)SA3 to upgrade the switch firmware and HTML pages from the web-based Cisco Visual Switch Manager Software. However, to upgrade to Release 11.2(8.3)SA3, you need to use the Cisco IOS command-line interface (CLI) via Telnet or the console port. This section describes the procedure for upgrading to Release 11.2(8.3)SA3. The procedure includes the following steps:

- Downloading the IOS image and Switch Manager HTML files from Cisco Connection Online (CCO).
- Using the CLI to upgrade your switch to the new image and HTML files.

Note You must enable SNMP and set the community string to public for the network view software to work properly.

Downloading Files from CCO

Follow these steps to download a new version of Catalyst 2900 software:

- Step 1** Enter the following URL in your browser Go To field:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL>
- Step 2** Click on the Cisco IOS image file and the Switch Manager HTML tar file to download them.

Upgrading Switch Software by Using Telnet

After you have downloaded the new files to your PC or workstation, you can use Telnet and the switch CLI to perform a TFTP transfer of the files to the switch. You can also connect a PC or workstation to the console port and transfer the files via XMODEM.

The procedure that follows includes the commands to address the following issues:

- To avoid a conflict with users accessing manager software pages during the software upgrade, you need to delete the existing HTML files and disable access to the HTML pages before you upgrade the software.
- Because the switch Flash memory can hold only one software image file, you need to change the name of the *current* image file to the name of the *new* file you are copying. You then replace the old file with the new file when you copy it into Flash memory.

Follow these steps to upgrade the switch software by using a TFTP transfer:

- Step 1** If your PC or workstation cannot act as a TFTP server, copy the files to a TFTP server to which you have access.
- Step 2** Start a Telnet session on your PC or workstation, and display the switch CLI by entering the following command:

```
server% telnet switch_ip_address
```

- Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

- Step 4** Display the name of the current (default) image file. The following example shows the current name in *italic*:

```
switch# show boot
BOOT path-list:    flash:current_image
Config file:      flash:config.text
Enable Break:     1
Manual Boot:      no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

- Step 5** Rename the current image file to the name of the new image. This does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

- Step 6** Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:
Directory of flash:
-rwx      910426   Mar 06 1993 23:47:28  new_image
-rwx       4800   Mar 01 1993 00:04:14  html
-rwx        159   Jan 01 1970 00:00:34  env_vars
-rwx       1121   Mar 01 1993 18:46:01  config.text
```

- Step 7** Remove the manager software HTML files:

```
switch# del flash:html/*.*
```

Press the Enter key to confirm the deletion of each file. Do not press any other keys during this process.

- Step 8** Enter terminal configuration mode:

```
switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 9** Disable access to the switch HTML pages:

```
switch(config)# no IP http server
```

- Step 10** Change the name of the default image file:

```
switch(config)# boot system flash:new_image
```

- Step 11** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 12** Verify that the name of the default image file is correct:

```
switch# show boot
BOOT path-list:    flash:new_image
Config file:      flash:config.text
Enable Break:     1
Manual Boot:      no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

- Step 13** Use the name of the new image file when you copy it from the TFTP server to the Flash memory:

```
switch# copy tftp://server_ip_address//path/new_image.bin flash:new_image
Source IP address or hostname [server_ip_address]?
Source filename [path/filename.bin]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

- Step 14** Create a directory on the switch Flash memory to be used for the HTML files.

```
switch# mkdir flash:html/Snmp
```

Make sure the “S” in “Snmp” is uppercase.

- Step 15** Enter the following command to copy the HTML file from the TFTP server to the switch Flash memory:

```
switch# tar /x tftp://server_ip_address//path/filename.tar flash:html
Loading /path/filename.tar from server_ip_address (via!)
extracting advanced.gif (2648 bytes)
extracting amber.gif (530 bytes)!
extracting bar.gif (4156 bytes)!
extracting cool.gif (530 bytes)
extracting daytona.gif (1470 bytes)
extracting duplgn.gif (639 bytes)!
. . .
```

Depending on the TFTP server being used, you might only need to enter one slash (/) after the *server_ip_address* in the tar command.

- Step 16** Reload the new software with the following command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

- Step 17** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets. Restart Telnet as described at the beginning of this procedure.

- Step 18** Enter terminal configuration mode:

```
switch(config)# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 19** Reenable access to the switch HTTP pages:

```
switch(config)# IP http server
```

- Step 20** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 21** Save the running configuration as the startup configuration:

```
switch# copy running-config startup-config
```

You do not need to restart the switch to begin using the new HTML pages.

Using Previous Releases of Cisco IOS Software

The minimum software release for hardware revision (board ID **0x0c**) is Cisco IOS Release 11.2(8)SA2. To check the hardware revision of your switch, follow these steps:

Step 1 Start a Telnet session on your PC or workstation, and display the switch CLI by entering the following command:

```
server% telnet switch_ip_address
```

Step 2 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Step 3 Display the current version of the switch with the **show ver** command:

```
switch># show ver

Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-H-M), Version 11.2(0.0.68)SA2,
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 02-Jun-98 10:52 by rm
Image text-base: 0x00003000, data-base: 0x001C7948

ROM: Bootstrap program is C2900XL boot loader

switch uptime is 2 days, 22 hours, 0 minutes
System restarted by reload
Running default software

cisco WS-C2916M-XL (PowerPC403GA) processor (revision 0x11) with
4096K/1024K by.
Board ID 0x0c
18 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:E0:1E:9F:4C:40
Configuration register is 0xF
```

The Board ID identifies the hardware revision in hexadecimal notation. Table 3 lists the Cisco IOS software that you can load on the available versions of Catalyst 2900 series XL.

Note In Table 3, different versions of the Catalyst 2916M XL hardware are shown by different board IDs.

Table 3 Possible Combinations of Cisco IOS and Catalyst 2900 Series XL Switches

Board ID	Switch	Supported Software
0x04	Catalyst 2908 XL	Cisco IOS Release 11.2(8)SA Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2 Cisco IOS Release 11.2(8.3)SA3
0x07	Catalyst 2924 XL	Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2 Cisco IOS Release 11.2(8.3)SA3
0x09	Catalyst 2924C XL	Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2 Cisco IOS Release 11.2(8.3)SA3

Board ID	Switch	Supported Software
0x06	Catalyst 2916M XL	Cisco IOS Release 11.2(8)SA Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2 Cisco IOS Release 11.2(8.3)SA3
0x0C	Catalyst 2916M XL	Cisco IOS Release 11.2(8)SA2 Cisco IOS Release 11.2(8.3)SA3

Using BOOTP to Assign IP Address Information

You can use BOOTP to assign IP information to a Catalyst 2900 series XL switch. A database with a list of physical MAC addresses and corresponding IP addresses must be set up on the BOOTP server. Other information, such as the corresponding subnet masks and default gateway addresses can also be stored in the database but are optional. The switch must be able to access the BOOTP server through one of its ports.

If the switch starts and no IP address has been assigned, it transmits a BOOTP broadcast request to all of its ports having a physical connection, requesting a mapping for its physical MAC address. A valid response includes the IP address, which is mandatory, and the subnet mask and the default gateway, which are optional.

The reception of a valid BOOTP response immediately activates the rest of the system protocol suite, without requiring a system reset. The running configuration is set, but the saved configuration in Flash memory is not automatically updated. To save the IP information in the saved-configuration file, log in to the command-line interface and enter the **write memory** command. The IP information is then preserved, and the switch does not issue BOOTP messages the next time it resets.

Current Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(8.3)SA3.

- There is no connectivity to a Novell server after client power-up or reboot. The Ethernet link to the switch is active, but the client failed to find a Novell server and cannot log into it.

The workaround is to configure the switch port to operate at a fixed speed and specify the duplex mode. For example, you can choose 100 Mbps and half duplex. This disables autonegotiation on the switch port and allows the link between the client and the switch to be set up faster. Then the initial broadcast frames from the client searching for the Novell server are forwarded through the switch more quickly. [CSCdj57531]

- When a switch is attached to a network with heavy broadcast or multicast traffic, newly connected interfaces can stay in spanning-tree listening state and not move to learning and then forwarding. This broadcast or multicast traffic is also forwarded to switch CPU. The CPU can be so overwhelmed processing this network traffic that spanning tree does not run.

A network that is producing this much broadcast or multicast traffic is not operating correctly and is so saturated that it is useless for normal network traffic. However, if the traffic that is saturating the network is broadcast traffic, broadcast storm control can be used to slow down traffic to the switch CPU. Similarly, if the traffic is multicast and the multicast address can be identified, it can be added as a static address. These frames are not forwarded to the CPU. [CSCdj87200]

- If a Fast EtherChannel port group is destination-address based, only one port in the group should be selected as a destination interface. If multiple ports are selected, duplicate frames will be forwarded into the group.

If the group is source-address based, all the ports in the group should be selected as destinations because source addressing filters the destination down to a single port in the group. If all the interfaces in the group are not selected as destinations some frames will not be forwarded into the group, depending upon source address. [CSCdk23822]

- When the switch receives an Spanning-Tree Protocol (STP) topology change notification, the Cisco Group Management Protocol (CGMP) tables should be purged for the virtual LAN (VLAN) in which it was received.

If an incorrect topology is maintained in the CGMP tables, the entry or entries can be cleared with the command: **clear cgmp [vlan *vlan-id*] group [group-mac-address]**. This will cause CGMP to relearn with the up-to-date topology. To view the CGMP tables, use the **show cgmp** command. [CSCdk31459]

- When running on Solaris, Netscape Communicator 4.03 or greater crashes or core dumps when displaying pages for the Visual Switch Manager or when running the Switch Network View.

Improvements were seen when the Solaris system was updated with the Sun OS Recommended patch cluster. [CSCdk35650]

- When using Netscape on the device and link reports, CPU utilization goes to 100 percent on all tested platforms and will not go back down until Netscape is closed.

The workaround is to let the device and link-report applets completely load before closing the window or starting the same report on the same device again. The CPU problem is less likely to happen on Microsoft Internet Explorer 4.01 SP1 and Netscape Communicator 4.0. [CSCdk36977]

- Multi-VLAN ports should not be connected to other switch ports. Multi-VLAN ports should be connected to only end stations or routers. [CSCdk18776]

- Netscape 4.03 crashes with a core dump when running on Solaris. The workaround is to install the Solaris patch 103461-24. [CSCdk24534]

- On the web interface Address Management page, the Aging Time can be temporarily displayed as 15 seconds, when the configured aging time is some other value. This happens when the Spanning-Tree Protocol (STP) is reconfiguring. To display the correct value, wait for STP to reconfigure and reload the Address Management page. [CSCdk24622]

- The following link can present special problems: Switch A at 10, half-duplex is connected to switch B set to Auto, Auto.

In this link, A and B achieve link, with B autonegotiating to 10, half-duplex. Link is stable at 10, half-duplex. If the user then reconfigures A to 100, half-duplex, the link at A drops because B is sending 10Mbps Link pulses, but not at B. This is because A is now sending 100Mbps Fast Idles, which have frequency components that correspond to 10 Mbps link pulses. Thus, as far as B is concerned, the link has not dropped and there is no reason to reautonegotiate the link parameters.

The workaround is to either physically remove the link and reinsert it, or to force the link down on B by setting it to 100, auto and then back to auto, auto, if desired. You could also workaround the problem by setting A to 100, auto and then back to 100, half if desired. The main thing is to force a reautonegotiate on the link so that B can figure out how it should operate. [CSCdk28412]

- If you attempt to upgrade the HTML pages on a Catalyst 2900 switch by using the tar command in the command line interface (CLI), the switch can issue the following error message:

```
%Error opening flash:html/source.html.gz(Device or resource busy)
```

This happens when HTML pages are being accessed while attempting to upgrade the HTML pages or the switch image file.

The workaround is to prevent access to the HTML pages when upgrading the HTML pages or the switch image file. Before upgrading the switch firmware (HTML files and image file) via the command line interface, enter the following configuration command:

no ip http server

After upgrading the HTML pages or image file, enter the following command to restore access to the HTML pages:

ip http server

[CSCdk29204]

- If a user is on the second page of Spanning Tree Protocol and goes to a page such as the VLAN Configuration page, clicking on Back results in a data-missing error message. The user is unable to go back to the second page of spanning tree.

The workaround is to always go back to the parent page of the Spanning-Tree Configuration. From there you may navigate to other pages and click Back and Forward as usual. [CSCdk29466]

- In Switch Network View, device X is connected to devices Y and Z, and we call the links between X and Y, XY and between X and Z, XZ. In crowded topologies, Z can appear on link XY with link XZ completely on link XY, leading to ambiguous displays of the network.

The workaround is to drag Z away from the link between X and Y. [CSCdk32530]

- Running the Switch Network View application with Netscape Communicator uses all available real and virtual memory and can cause the computer to become unusable or unstable.

The workaround is to reduce the number of open windows while you are running Switch Network View. Also, do not leave Switch Network View running for long periods of time: close and restart the application. [CSCdk39494]

- If you use Visual Switch Manager to change the STP protocol setting to IBM or DEC, the protocol setting does not take effect. To change the STP protocol setting to IBM or DEC, use the CLI. [CSCdk42398]
- Software version 11.2(8.3)SA3 mistakenly saves the keyword of the spanning-tree configuration command as hello time whenever the spanning tree protocol is specified as IBM or DEC. This hello time keyword is rejected as illegal when the configuration is reloaded, causing the configuration command to be ignored. This prevents the user from saving a non-default STP hello time value when IBM or DEC protocol is being used. However, there should be no problem saving the hello time if the default IEEE protocol is in use.

If you want to use the IBM or DEC STP protocol and save a non-default hello-time parameter, use the following workaround:

- (a) Set the hello-time parameter as desired.
 - (b) Save the running configuration.
 - (c) Use TFTP to copy the running configuration to a remote server.
 - (d) On the remote server, edit the configuration file to change the hello time value.
 - (e) Use TFTP to copy the corrected configuration back to the C2900XL.
- [CSCdk42610]

- If SNMP is used to change an STP parameter, the change takes effect but is lost when the system is rebooted. The workaround is to use the command line interface to change STP parameters. [CSCdk42666]

Cisco IOS 11.2(8)SA2 Caveats/Release 11.2(8.3)SA3 Modifications

This section describes Cisco IOS Release 11.2(8)SA2 caveats that were resolved with Cisco IOS Release 11.2(8.3)SA3.

- From the login prompt, it is possible to recover fragments of lines typed by the previous user of the same physical or virtual terminal line. This can represent a security exposure. A complete description of this problem can be found at this URL:
<http://www.cisco.com/warp/public/770/ioshist-pub.shtml>. (CSCdk43920)
- In certain cases, when using type-1 station cabling, if a balun is disconnected the transceiver CAN loop the port back on itself. In this environment the switch fails to put the port into blocking mode and a loop condition occurs. (CSCdk33396)
- In certain cases a Catalyst 2924XL switch running Cisco IOS 11.2(8.3)SA3 CAN lose IP connectivity. This problem appears to be due to a loss of input packet buffers for the IP input to the switch CPU. This can be verified by using **show buffers**. If the output for the Interface buffer pool CPU6 indicates that there are 0 in the free list, then this condition might be present. (CSCdk67379)
- Secure addresses on a module port show up on a different port.

Dynamic module insertion and extraction is not supported in this release. Reboot the system after a new module is inserted. [CSCdj52749]

- The set function of c2900PortUsageApplication MIB object is not supported.
Use web-based interface or the CLI to set the corresponding port application parameters. [CSCdj66180]
- The CISCO-C2900-MIB object c2900InfoVisualIndicatorMode is a read-only object.
Do not set this object. [CSCdj66193]
- The CISCO-C2900-MIB object c2900PortUsageApplication cannot be set. To control the port application, use the Cisco IOS CLI. [CSCdj69900]
- If the user has not configured a path cost, the spanning-tree path cost for a Fast EtherChannel port group is calculated based on the aggregate bandwidth of the ports in the group. This aggregate bandwidth is used as the path cost for STP to elect the network root switch, designated bridges, and designated ports.

When the interface in the Fast EtherChannel port group that is carrying STP information loses the link, another interface is chosen to carry the STP information. When this backup interface takes over, the path cost used for the Fast EtherChannel port group is based on the bandwidth of just that interface.

If this path cost adversely affects the desired convergence of spanning tree, there are three options:

- Reenable the link on the interface which lost the link.
- Use the web interface or CLI to remove the down interface from the group.
- Manually configure the path cost for the group.

Any one of these remedies will make the Fast EtherChannel port group use a path cost that reflects the aggregate bandwidth. [CSCdj74531]

- BOOTP client sets the wrong default gateway.
The workaround is to make certain that the BOOTP server can forward packets to the correct default gateway. Alternatively, the default gateway can be placed in the local configuration file. [CSCdj79384]

- Under some circumstances, the counters in the **show interface** command can display erroneous information.

There is no workaround at this time. [CSCdj88171]

- By default, the switch will not accept an IP address-netmask pair that would result in using the subnet zero.

The workaround is to first enter the **ip subnet-zero** command, and then set the IP address and netmask. [CSCdj89742]

- The following MIB objects are added to determine the port duplex mode, duplex status, and the data rate via the CISCO-C2900-MIB private MIB:

c2900PortDuplexState

OBJECT-TYPE SYNTAX INTEGER { fullduplex(1), halfduplex(2), auto-negotiate(3) }
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION

- Set to fullduplex(1) to operate in full-duplex mode, port will allow simultaneous transmit and receive, which can double its bandwidth.
- Set to halfduplex(2) to operate in half-duplex mode.
- Set to auto-negotiate(3) to allow the switch to negotiate with the other end of the connection.

The status of duplex mode on a port is available with c2900PortDuplexStatus object. DEFVAL {auto-negotiate} ::= {c2900PortEntry 31}

c2900PortDuplexStatus

OBJECT-TYPE SYNTAX INTEGER { fullduplex(1), halfduplex(2) }
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

The status of duplex mode on this port. This shows the result of full-duplex autonegotiation when c2900PortDuplexState is set to autonegotiate." ::= {c2900PortEntry 32}

c2900PortAdminSpeed

OBJECT-TYPE SYNTAX INTEGER { autoDetect(1), s10000000(10000000), -- 10 Mbps
 s100000000(100000000) -- 100 Mbps }
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION

The object controls the speed of the port. The current operational speed of the port can be determined from ifSpeed." DEFVAL {autoDetect} ::= {c2900PortEntry 33} [CSCdj92712]

- Pings to or from a switch can receive duplicate responses.

If STP has blocked a port due to duplicate paths in a network, ICMP packets can still be sent and received on the blocked port. Note that this bug only affects traffic going to or from the switch CPU itself; it does not affect traffic going through the switch. So, blocked ports will not transmit any packets received from any other port on the switch, and packets received on any blocked port will not be forwarded to any other ports on the switch.

There is no workaround. [CSCdk05329]

- The c2916M-XL console condition can hang if the banner contains eight or more full lines of text and a laptop hyperterm is activated while connected to the console port. The workaround is to activate the laptop hyperterm prior to connecting to console. [CSCdk06196]
- Form submissions (the Apply button) did not work when the browser was configured to use a proxy server. There is no workaround, short of not using a proxy server. [CSCdk06332]
- It is possible for a port to lock up under some jabber conditions on ports configured for 10 Mbps half-duplex operation and only happens on units with a board ID of 4 or 6.

To determine the board ID see the section “Using Previous Releases of Cisco IOS Software” in this document. [CSCdk11524]

- The following MIB object is added to CISCO-C2900-MIB to find out main board type:

```
c2900InfoBoardIdentifier
OBJECT-TYPE SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
```

Returns the identifier of the main board on which the firmware resides. ::= {c2900SysInfo 10} [CSCdk14232]

- The tar command does not automatically create subdirectories within a tar archive while extracting the contents of the archive.

The workaround is to update the Cisco IOS software to a newer version before extracting the contents of a tar archive. You could also extract the contents of an archive, paying attention to errors brought about by directories not being created. The directories can then manually be created with the mkdir command; the contents of the archive will have to be extracted once more to get all the files that were missed the first time. [CSCdk18396]
- Spanning-tree topology can be incorrect because the message-age timer is incorrect. The workaround is to use ports 1 or 2 as uplink ports to other switches. [CSCdk18443]
- If a user disables one of the ports on the C2900XL and another device attempts to ping the C2900XL CPU through the disabled port, the ping is successful. To stop the ping from being successful, enter a **clear mac** command. [CSCdk28344]
- In certain cases when using type-1 station cabling, if a balun is disconnected, the transceiver might loop the port back on itself. In this environment, the switch fails to put the port into blocking mode and a loop condition occurs. [CSCdk33396]

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

This document is to be used in conjunction with the *Catalyst 2900 Series XL Installation and Configuration Guide*.

AccessPath, Any to Any, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratum, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn and Empowering the Internet Generation are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9808R)

Copyright © 1997-1999, Cisco Systems, Inc.
All rights reserved. Printed in USA.