



Doc. No. 78-4923-05

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

July 30, 1998

These release notes describe the features and caveats for Cisco IOS Release 11.2(8)SA2.

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

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.

Class A Warnings

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Loading Previous Releases of Cisco IOS Software

This Catalyst 2900 Series XL switch is shipped with Cisco IOS Release 11.2(8)SA2. If you want to load a previous release of the software, there might be some restrictions. See the section “Using Previous Releases of Cisco IOS Software” for more information.

Using BOOTP to Assign IP Address Information

You can use BOOTP to assign IP information to a Catalyst 2900 series XL switch. A database containing 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.

Downloading New Catalyst 2900 Series XL Software

This release of Cisco IOS software can be downloaded from Cisco Connection Online (CCO) at the following URLs:

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

Catalyst 2900 series XL software consists of a binary file and an HTML file. You can copy these files from CCO to your PC or workstation with an FTP transfer or as an e-mail attachment. You might need to register to download the new files.

Renaming the Software Image File when Upgrading Switch Software

Caveat CSCdj68326 in the section “Cisco IOS 11.2(8)SA1 Caveats/Release 11.2(8)SA2 Modifications” describes a need to rename the switch software-image file when you download it. If you are running Cisco IOS Release 11.2(8)SA1 or Cisco IOS Release 11.2(8)SA, you need to rename the image file when you download it.

However, if you purchased a switch running Cisco IOS Release 11.2(8)SA2, you do not have to rename the image file if you upgrade to a later release. The switch searches Flash memory and boots the image that it finds.

Reading LEDs for FastEtherchannel Port Groups

Because Fast Etherchannel port groups act as a single logical port, one port status LED in a port group is green, and all other port status LEDs in the group are amber. This has no effect on packet forwarding, and all ports in the port group share the same forwarding characteristics and STP status changes.

Connecting FastEtherchannel Port Groups to a Router

During normal operation, Fast EtherChannel load balancing distributes traffic among all ports in a port group. This load balancing does not work when connecting a port group to routers. Routers are single-MAC-address devices, and the switch forwards all traffic over one port instead of over all ports in the group.

Upgrading Switch Software by Using Telnet

After you have downloaded the new image files to your PC or workstation, you can use Telnet and the switch command-line interface (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.

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 EXEC mode:

```
switch> enable  
switch#
```

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

```
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** Enter terminal configuration mode:

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

- Step 8** Change the name of the default image file:

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

- Step 9** 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 10** 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
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 11** 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 duplgnd.gif (639 bytes)!
...
```

- Step 12** The new image file loads the next time you reset the switch. You can load the new software with the following command:

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

- Step 13** Press Return to confirm the reload. Your Telnet session ends when the switch resets.

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 command-line interface (CLI) by entering the following command:

```
server% telnet switch_ip_address
```

Step 2 Enter 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 indicates the hardware revision in hexadecimal notation. Table 1 lists the Cisco IOS software that you can load on the available versions of Catalyst 2900 Series XL.

Note In Table 1, different versions of the Catalyst 2916M XL hardware are indicated by different board IDs.

Table 1 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
0x07	Catalyst 2924 XL	Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2
0x09	Catalyst 2924C XL	Cisco IOS Release 11.2(8)SA1 Cisco IOS Release 11.2(8)SA2
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
0x0C	Catalyst 2916M XL	Cisco IOS Release 11.2(8)SA2

Current Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(8)SA2.

- The value of MIB object `c2900PortRxSuppressBcastFrames` is always zero.

The MIB object `c2900PortRxSuppressBcastFrame` is not supported. It is used to count the broadcast frames received that were discarded because of the threshold-based broadcast suppression. [CSCdj48447]

- The `c2900PortVisualIndicator` object in the `CISCO-C2900-MIB` always returns the state of the LED in port status mode.

This MIB object will only indicate the LED color in the `portStatus` mode. Therefore, make sure that the `c2900InfoVisualIndicatorMode` is `portStatus` before relying on the validity of the `c2900PortVisualIndicator` object. The LED colors can also be determined by looking at the front of the Catalyst 2900 series XL switch. [CSCdj49195]

- Switch resets when extracting a module.

The modules cannot be dynamically installed and removed while the switch is running. First turn off the switch, and then remove the module. [CSCdj52719]

- Secure addresses on a module port show up on a different port. After a module is removed from one module slot and a new module is inserted into a different module slot, the secure addresses assigned or learned on ports of the extracted module show up on ports of the newly inserted module.

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

- The `CISCO-C2900-MIB` objects `c2900PortFrameAge`, `c2900PortBufferCongestionControl`, and `c2900PortBufferCongestionThresholdPercent` should be treated as read-only objects. An error is returned if you attempt to set this object. [CSCdj65469]

- The set function of `c2900PortUsageApplication` MIB object is not supported. Use the web interface or command-line interface (CLI) to set the corresponding port application parameters. [CSCdj66180]

- The switch unreliably responds to continuous pings from another workstation.

This could be due to a network transmitting broadcast traffic at 500 frames per second and thus containing a misconfigured or faulty device. In this case, fix or remove the faulty device. It could also be a duplex mismatch. See the *Catalyst 2900 Series XL Installation and Configuration Guide* for instructions on how to troubleshoot duplex mismatches. [CSCdj60660]

- The input/output packet rate and bit rate counters do not update themselves.

Do not rely on the packet/bit rate counters to provide an indication of the traffic through a given interface. SNMP/RMON or the LED flashing frequency can be used to provide this information. [CSCdj76674]

- A multicast group address cannot be added to the address table after slots in the self-address table are freed.

This problem occurs when the switch receives a CGMP-join for a group-address port and the self-address table is full. When space in the self-address table is freed, that group-address port is still not added to the table when another join message is received. A possible workaround would be to clear that group from CGMP so that the group can be re-populated by CGMP Joins. The command to clear the group from CGMP is **clear ip igmp group-mac-address** [CSCdj80234]

Cisco IOS 11.2(8)SA1 Caveats/Release 11.2(8)SA2 Modifications

This section describes Cisco IOS Release 11.2(8)SA1 caveats that were resolved with Cisco IOS Release 11.2(8)SA2.

- Cannot use the CDP name to connect to the CDP neighbor from the CDP HTML page. The workaround is to register the CDP name to a domain name server before trying to connect to it from the CDP HTML page. [CSCdj31392]

- Switch does not send a trap for an address security violation.

View the security violation messages on the console, or configure the switch to send syslog messages to a server, and examine them on that server. [CSCdj35909]

- Broadcast storm control miscounts the input broadcast frame rate. The workaround is to not rely on the “Current” field of the output of **show port storm-control**. [CSCdj37018]

- There are some commands that are not disabled, but that do nothing. For example, the configuration command **ip routing** can be entered from the command line without error. This command, however, can affect IP connectivity. Do not enter router-based Cisco IOS commands such as **ip routing**. [CSCdj43070]

- CGMP cannot be disabled. There is no workaround. [CSCdj44323]

- A message appears on the console shortly after booting:

```
% Illegal subtree oid: c2900MibNotificationsPrefix.1 XCRS% Illegal subtree oid:
c2900MibNotificationsPrefix.2
```

No workaround is necessary. The unit is working properly, and the above messages can be ignored. [CSCdj44968]

- If the user uses ? when entering a command-line interface (CLI) command to find out the available module numbers, the help prompt displays the incorrect module number (interface number). Depending on whether the system has no modules, one module, or two modules, the available module numbers are 0, 0–1, or 0–2. [CSCdj47044]

- Inconsistent port numbering for dot1dStpPort and dot1dTpFdbPort.

For dot1dStpPort, the range of system board port numbers is from 1–32, the range of module 1 port numbers is from 33–64, and the range of module 2 port numbers is 33–64.

For dot1dTpFdbPort, the range of system board port numbers is from 1–64, the range of module 1 port numbers is from 65–128, and the range of module 2 port numbers is from 129–193.

Use the above port-numbering scheme to match dot1dStpPort port number and dot1dFdbPort port number to module and port numbers on the system. [CSCdj47348]

- If the speed of a switch port is set to autonegotiate and the user tries to set full duplex on the port, the port can lose link. The workaround is to set the port speed to 10 Mbps or 100 Mbps before setting full duplex on the port. [CSCdj47637]

- c2900PortNumberOfLearnedAddresses and c2900PortNumberOfDroppedAddresses MIB objects are not currently supported. No workaround is available. [CSCdj48438]

- Bandwidth Group objects in Cisco C2900 MIB are not updated. These MIB objects are not implemented and therefore always return the default values. Use statistics in the interface group of the MIB-II to derive bandwidth values. [CSCdj48441]

- Turning on Port Fast on ports in a Fast EtherChannel port group might cause a loss of connectivity between switches. The workaround is to not turn on Port Fast on ports in a Fast EtherChannel port group. [CSCdj48602]

- Error messages are returned when the user tries to set the following CISCO-C2900-MIB objects:
c2900PortBroadcastRisingThreshold, c2900PortFloodUnknownUnicasts,
c2900PortFloodUnknownMulticasts, c2900PortFrameAge, c2900PortMayForwardFrames,
c2900PortBufferCongestionControl, c2900PortGroupIndex, c2900PortUsageApplication,
c2900PortBufferCongestionThresholdPercent, c2900InfoVisualIndicatorMode, and
c2900PortClearAddresses

These C2900 MIB objects are not supported in this release. Use the corresponding command-line interface (CLI) commands to set these variables. [CSCdj49182]
- In the C2900PortEntry table, four objects are not maintained:
c2900PortNumberOfDroppedAddresses, c2900PortFloodUnknownMulticasts,
c2900PortAddrSecureAddrViolations, and c2900PortNumberOfLearnedAddresses

When retrieving these MIB objects, the values returned are always zero.

These objects are not currently supported. The values returned by these four objects should be ignored. [CSCdj49186]
- The c2900ConfigAddressViolationAction and c2900PortFrameAge objects in the CISCO-C2900-MIB always return their default values.

If the default values for these MIB objects are altered, do not rely on their current values to be returned by the MIB. [CSCdj49197]
- All ports are amber when the switch is in utilization mode.

This is normal behavior, as the amber LEDs indicate a *high-usage mark*. All LEDs up to the LED that represents the highest utilization reached in the last 24-hours are colored amber. Then, all LEDs up to the LED that represents the current utilization are colored green. This high-usage mark display is reset every 24 hours, unless changed to a different PeakBandwidthInterval by SNMP management. [CSCdj49279]
- On the Port Security HTML page, security action cannot be configured by choosing the security action and clicking **Apply**. The workaround is to disable port security, click **Apply**, and then reenables port security and set the security action before clicking **Apply**. [CSCdj49285]
- The historyControlIndex in the RMON MIB can be greater than 65535. No workaround is necessary; the switch functions properly regardless of the historyControlIndex value. To comply with the RMON MIB, do not specify a historyControlIndex value greater than 65535. [CSCdj49296]
- The count of input broadcast frames does not include the count of multicast frames nor the count of broadcast frames and multicast frames dropped due to forwarding decisions.

Enter **show controllers ethernet-controller interface** at the CLI to display a complete table of statistics for an interface. This can then be used to determine the complete number of broadcast frames, including multicast and unforwarded frames. [CSCdj49315]
- The RMON monitoring of ifIndex.1 does not work properly.

The ifIndex.1 interface refers to the internal, or CPU, interface to the network. Because this is an internal interface, RMON monitoring of this interface is not supported. This interface should not be specified in the historyControlDataSource. [CSCdj49324]
- The ACT and COL LEDs shown on the HTML home page are not working.

The ACT and COL LEDs displayed on the front panel of the HTML home page should be marked 1 and 2. They are LEDs that display module status on the real system. These LEDs on the HTML page are not supported. [CSCdj50013]

- The MAC Address aging time can be set to less than 10 seconds. Because the IEEE 802.1d specification states that the aging time for MAC addresses should be in the 10 to 1000000 range, do not configure the MAC aging time with a value between 0 and 9. (CSCdj50275)
- When the user enters the **reload** command to reboot the system, there is no prompt for saving configuration changes into NVRAM.
Either use a **write mem** command before using **reload** to reboot the system, or avoid using the **clear** command to modify the system configuration. [CSCdj50400]
- Creating an RMON event table entry from the CLI with a duplicate eventIndex writes over the previous entry.
When creating entries in the RMON event table from the CLI, be sure to choose unique event numbers for each entry. [CSCdj50799]
- The user cannot add a static address through the web interface if no output port is specified.
Add the static address by using the CLI command **mac-address-table static hwaddr input-port**. [CSCdj50857]
- Creating RMON event table entries with large eventIndex fields will cause CPUHOG messages on the console.
When creating entries in the RMON event table, choose small numbers for the eventIndex value. Sequential numbers starting with 1 will work best. [CSCdj51546]
- The value of the STP RootPort number shown from SNMP (Bridge MIB object dot1dStpRootPort) is incorrect.
Use the CLI **show spantree** command to find the STP RootPort number. [CSCdj51560]
- Telnet out from the system does not work.
Telnet from the system to other stations is not supported. [CSCdj51155]
- Power-On Self-Test failure message for Ethernet port is suppressed.
If it is suspected that this is happening because one of the ports is not working, observe the front-panel LEDs during system startup. If one or more port LED is amber for a period of time after system startup is complete, you can assume that the corresponding port is defective. [CSCdj51535]
- STP Designated Port number and STP Designated Cost shown from SNMP (dot1dStpPortDesignatedCost and dot1dStpPortDesignatedPort) are always 0.
To obtain the correct value of STP Designated Port Number and STP Designated Cost, use the **show spantree** command. [CSCdj51594]
- The violation action for the Port Security page should read Shutdown, not Disable. This will provide consistency between online help and the web page. [CSCdj52608]
- After issuing a write **erase command**, the **show running** command returns an error.
Do not execute the **write erase** command if you intend to use the **show running** command. If a **write erase** needs to be done, reload the switch after entering the command. [CSCdj51956]
- Help description for the tar command is incorrect. The text should read: "List or extract a file from a tar image." [CSCdj52165]
- No link is detected after a Compaq computer with a NETELLIGENT 10/100 PCI adapter connected to one of the ports on the switch is power-cycled.
The workaround is to disable both speed and duplex auto negotiation on the port and to manually set the speed and duplex mode on the port to match those of the link partner. [CSCdj53272]

- Broadcast frames that are filtered due to broadcast storm control are not counted in the **show-interface** statistics.

If an accurate number of broadcast frames received on an interface is required, do not enable broadcast storm control on the interface. [CSCdj53486]

- No link is detected on a port connected to device via a cable of a certain length. If a port is connected to a 100-Mbps-capable link partner via a cable of 35 to 41 meters and the partner does not autonegotiate, the port might not get the link. To ensure connectivity, turn off both speed and duplex-mode auto-negotiation on the port, and set the speed and duplex mode on the port to match those of the link partner. [CSCdj53500]

- SNMP ifInUcastPkts, ifOutUcastPkts, ifInNUcastPkts, and ifOutNUcastPkts counters are incorrect.

The ifInUcastPkts or ifOutUcastPkts counters include unicast and multicast packets received or sent by the switch. The ifInNUcastPkts or ifOutNUcastPkts counters only include broadcast packets received or sent by the switch. [CSCdj54209]

- On the HTML page that displays the switch, a port in STP blocking state is displayed in green. To find out if a port is in STP blocking state, go to the Spanning-Tree Management page, or check the LED above the port on the front panel of the switch itself. [CSCdj54388]

- The operator is sometimes not prompted to save configuration changes when issuing the **reload** command. Save the configuration from the command-line interface before issuing the **reload** command. [CSCdj54346]

- STP and CDP packets on port 1 are not forwarded to the monitor port.

Switch the connections between port 1 and the monitor port. Disable port monitoring on the monitor port, and enable port monitoring on port 1. [CSCdj54447]

- The output of the **show port storm-control** will be incomplete for ports that do not have both filter and trap enabled on them.

Ports that do not have filtering or traps enabled display <inactive>. When the **show port storm-control** command is entered through the HTML command-line interface (The Monitor the Switch link on the Access Page), the browser removes the *inactive* value and the angle brackets.

Display the port storm-control status using the console or Telnet interface. [CSCdj54589]

- The following message might be printed on the console at boot time:

```
%SYS-3-CPUHOG: Task ran for 2232 msec (275/259), Process = Init, PC = 1116B0
-Traceback= A9798 128B94 129298
```

This message is most likely to occur on a switch with two modules installed. This message can be ignored. [CSCdj56860]

- 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.

Configure the switch port to operate at a fixed speed and specify the duplex mode; for example, choose 100 Mbps and half duplex. This will disable autonegotiation on the switch port and allow the link between the client and the switch to set up faster. This allows the initial broadcast frames from the client searching for the Novell server to be forwarded through the switch more quickly. [CSCdj57531]

- Address security violations are not reported when the switch address table is full.
Avoid filling up the address table of the switch if security violations should cause actions. Ensure that the network is partitioned so that there are fewer than 2500 stations connected to the switch. [CSCdj57731]
- The switch might reset if the user tries to set one of the switch port's own MAC address. The workaround is to avoid changing the switch port's own MAC address. [CSCdj58119]
- Some configuration changes do not take effect when the configuration is changed through the web-based Switch Manager.
When using the web-based management, do not make more than 15 configuration changes before clicking **Apply**. [CSCdj58539]
- STP cannot be enabled under certain circumstances.
Depending on whether the static address table or system-address table is full, the workaround is either to reduce system static address number by 2 or to reduce the number of existing system addresses by 2 to allow STP to be enabled. [CSCdj59203]
- LED can stay green for a while after the link on the port is down.
After the link on a port is down, allow some delay before using the LED as indicator of the port status. [CSCdj60674]
- Sometimes MAC addresses for module ports cannot be added to the address table.
The workaround is to reboot the system after new modules are inserted. [CSCdj61019]
- Set commands issued for individual objects in the SNMP private MIB are treated as set-all commands for all objects in that group. For example, if the c2900PortLinkbeatStatus of c2900PortTable needs to be set, then all the other objects in the c2900PortTable also get set.
Do not set an object separately in a group. Instead, set all the objects in the group. [CSCdj61728]
- Sometimes the interface drops incoming packets destined for the system itself.
Certain valid TCN packets could cause buffer leak. When input buffer threshold for the interface is reached as a result of the buffer leak, all incoming packets received from the interface are dropped. No workaround is available. [CSCdj61832]
- Console output can hang. When a lot of console output is generated faster than it can be displayed, a race condition can cause the console output to hang. When this happens, output can be restarted by causing a syslog message to be generated. This can be done by unplugging and replacing one of the Ethernet cables on the front panel. For this to work, syslog output to the console must be enabled, which is the default behavior. [CSCdj63078]
- When using Microsoft Internet Explorer, the screen is sometimes not updated correctly after clicking **Apply**.
Microsoft Internet Explorer does not always update the screen when it should.
The workaround is to change the Microsoft Internet Explorer settings as follows:
 - 1) Select menu **View->Internet Options...**
 - 2) Click **General** tab, and choose **Temporary Internet Files** settings.
 - 3) Click **Every visit to the page**, and click **OK**. [CSCdj63729]
- The CISCO-C2900-MIB object c2900BandwidthUsagePeakEntry should be treated as a read-only object. An error is returned if you attempt to set this object. [CSCdj63917]

- The SNMP MIB object C2900BandwidthUsagePeakEntry Peak values are too large. There is no workaround for this problem. Do not rely on the value of this field to provide accurate information. [CSCdj64613]

- The timestamp values stored in the SNMP MIB object C2900BandwidthUsagePeakEntry can indicate too much time between intervals.

There is no workaround for this problem. The time elapsed during one interval might be too long if the CPU was under heavy load during the interval. This could cause the intervals to not land on exact interval boundaries (for example, 24-hour periods from midnight to midnight). [CSCdj65046]

- The CISCO-C2900-MIB returns incorrect values for c2900PortFloodUnknownMulticasts and c2900PortFloodUnknownUnicasts objects. The workaround is that the value returned by c2900PortFloodUnknownUnicasts is the value that should be returned by c2900PortFloodUnknownMulticasts. [CSCdj65178]
- A 3Com 3c509 NIC connected to a switch port will establish link at 100 Mbps and full duplex after the PC is rebooted, even though the NIC is set to 100 Mbps and half duplex.
This is caused when the NIC is powered on and comes up in full autonegotiating mode, which will establish link with the autonegotiating port on the switch in 100 Mbps and full-duplex mode. When the operating system on the PC is then initialized, it resets the NIC to be in 100 Mbps and half-duplex mode, without forcing the link to drop between the switch and the NIC. The solution is to also put the switch port into 100 Mbps and half-duplex mode or to leave the NIC settings on the PC in autonegotiating mode. [CSCdj65919]
- The CISCO-C2900-MIB does not allow the c2900BandwidthUsagePeakInterval to be set. The default interval of 1 hour is the only interval available in this release. [CSCdj67159]
- If the c2900BandwidthUsagePeakRestart is set to TRUE, the c2900BandwidthUsagePeakTable is cleared, and the peak bandwidth recording is restarted. If the c2900BandwidthUsagePeakRestart is set to FALSE, no action should be taken. But even if the c2900BandwidthUsagePeakRestart is set to FALSE, the peak table is getting cleared, and the peak bandwidth recording is restarted.

Do not set the c2900BandwidthUsagePeakRestart to FALSE. [CSCdj67194]

- System does not automatically find the Cisco IOS image in Flash memory during system startup.
To work around this, change the name of the file used to boot the system, and enter the **boot system flash:boot_filename** command to identify the name of the new Cisco IOS image. [CSCdj68326]

- The RPS indicator on the physical view of the switch is not shown.

This error does not have a workaround. [CSCdj70757]

- Layer 2 output queues can become blocked when an interface is reset with a low probability.

When a Layer 2 interface has become blocked, this condition can be detected by entering **show interface interface** and observing the status of the output queue.

```
pheller-malibu#show int f0/14 FastEthernet0/14 is up, line protocol is up Hardware
is Fast Ethernet, address is 00e0.1ee2.de0e (bia 00e0.1ee2.de0e) MTU 1500 bytes,
BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255 Encapsulation ARPA,
loopback not set, keepalive not set Half-duplex, 100Mb/s, 100BaseTX/FX ARP type:
ARPA, ARP Timeout 04:00:00 Last input 19:08:48, output 00:00:01, output hang never
^^^^^^^^ (1) Last clearing of "show interface" counters never Queueing strategy:
fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops ^ (2)
```

(1) When an interface running STP is blocked, the time of last output should not be more than 2 seconds.

(2) The number of output frames queued should be either 0, or in rare cases, 1.

If this condition is detected, resetting the interface clears the output queue and restarts transmission. You can either enter **shutdown** and then **no shutdown** to reset the interface or disconnect and reconnect the Ethernet cable at both ends of the connection. [CSCdj70808]

- Sometimes the LED on a shut-down secure port does not turn amber.

For a port enabled for port security, use the **show interface** command to determine whether the port has been shut down because of security violations. [CSCdj70986]

- A new file is extracted from a tar file, over-writing a previous file with the same name, and the new file size is larger than it should be.

To work around this problem, before extracting tar files, remove any files that will be over-written. [CSCdj71812]

- On the CDP web page, the help explanation for the Browse button should read as follows:

“Start a new browser session and display the HTML interface of the selected neighboring device.” [CSCdj71921]

- Alternating amber/green port status LED due to collision fragments.

If collision fragments are being generated at a fast enough rate on a switch port, the port status LED displays an alternating green/amber port fault condition.

Collision fragments are not an error condition in a half-duplex Ethernet network. If the port fault indication is activated on a port, use **show controllers ethernet-controller interface** to display a table of port statistics. Several other statistics are also used to activate the port fault display, such as Transmit Late Collisions, Transmit Excessive Collisions, Transmit Too Late Discards, Receive Alignment Errors, Receive FCS Errors, Receive Oversize Frames, and Receive Undersize Frames.

If none of these statistics are incrementing or are not incrementing very quickly, the port fault indicator was activated due to collision fragments and should not be considered a fault condition. [CSCdj72160]

- Every time a port MAC address is changed, the address table size available to the user is reduced by one because the old MAC address is not removed from the address table until the system is reset.

The workaround is to reset the system after a port MAC address is changed and the change has been saved. [CSCdj73177]

- The command **snmp host <hostname>** returns the following error:

```
% Illegal subtree oid: c2900MibNotificationsPrefix.1 % Illegal subtree oid:
c2900MibNotificationsPrefix.2
```

Even though this command returns an error, the traps still work. As a side effect, the proprietary traps for the switch are received by all the trap hosts, even though the hosts are configured to receive only certain kind of traps.

Ignore the error message returned by the **snmp host** command. Do not depend on the trap filtering defined by **snmp host hostname** command. [CSCdj73497]

- When the user enters the **enable** command, the following message is printed on the console:

```
% No authentication server running
```

This happens if the user has previously entered the following configuration mode command: **enable use-tacacs**.

TACACS is not supported on the switch, and the above command is not supported and should not be entered. If the user has already entered the above command and now cannot enter enable mode, the user must follow password recovery procedures. [CSCdj75618]

- Static MAC addresses can be seen in BRIDGE-MIB dot1dStaticEntries, but cannot be removed. To remove a CGMP-learned group address from the bridge forwarding table, use the Exec-mode command: **clear ip igmp address** *address*. [CSCdj83295]
- When entering the **reload** command, the operator is not prompted to save configuration changes. If you want to save the running configuration to the startup configuration file, save the configuration from the CLI before entering the **reload** command. [CSCdj54346]
- The output of the **show port storm-control** command is incomplete for ports that do not have either filter or trap enabled on them. Display the port storm-control status by using the console or the Telnet interface. [CSCdj54589]
- A port remains in a Spanning-Tree Protocol (STP) listening state. Do not use SNMP to disable spanning tree on a port if you intend to reenabling spanning tree. [CSCdj73797]
- The RMON numbers shown on the console using **show rmon statistics** become negative after they are wrapped. The workaround is to use SNMP application to view RMON statistics. [CSCdj80162]
- The value for dot1dStpTimeSinceTopologyChange is in seconds, not in hundredths of seconds as defined in MIB definition for dot1dStpTimeSinceTopologyChange. Multiply the value by 100 to get the dot1dStpTimeSinceTopologyChange value in hundredths of a second. [CSCdj80322]
- An empty description for an interface is displayed in the output of the **show running-config** command after using SNMP to set the LinkUpDownTrapEnable field of the IF-MIB ifXEntry. The empty description does not interfere with the switch operation. To remove the empty description, issue the command **no description** in the configuration menu for the interface. [CSCdj84929]
- The saved RMON alarm table cannot be reloaded. No workaround is available. [CSCdj85687]
- The **copy running-config startup-config** command does not exist in the c2900XL-h-mz images. The workaround is to use the **write mem** command instead. [CSCdj86914]
- When a switch is attached to a network with heavy broadcast or multicast traffic, newly connected interfaces can remain in an STP listening state without moving to learning and forwarding. A network producing this much broadcast or multicast traffic is not operating correctly. However, if the traffic that is saturating the network is broadcast traffic, broadcast storm control can be used to reduce it. Similarly, if the traffic is multicast and the address can be obtained, a static address can be added that keeps these frames from being forwarded to the CPU. [CSCdj87200]
- A Catalyst 2916XL with an IP address configured in the VLAN1 interface and an interface in the “down” state, “administratively down” state, or in “blocked” state due to STP can send broadcast traffic from the CPU out to the network. [CSCdj87852]

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.

Note 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, 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, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratm, 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, FastPacket, ForeSight, FragmentFree, 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.

Copyright © 1998, Cisco Systems, Inc.
All rights reserved. Printed in USA.
9805R