



Release Notes for the Catalyst 2900 Series XL

December 30, 1997

These release notes describe the caveats for the Catalyst 2900 series XL switches.

Catalyst 2900 series XL switches are supported by Cisco IOS 11.2(8) SA. Cisco IOS 11.2(8) SA is not released on the same six-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 modules and the Catalyst 2900 series XL switches 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

Configuring the Switch for Telnet

You can use Telnet to access the Cisco IOS command-line interface (CLI), but you might want to configure your switch so that Telnet access is password-protected. This procedure describes one way to configure a password for Telnet.

Task	Command
Step 1 Attach a PC or workstation with emulation software to the switch console port. The data characteristics of the console port are 9600, 8, 1, no parity. When the command line appears, enter the following commands.	
Step 2 Enter privileged EXEC mode.	enable
Step 3 Enter configuration mode.	configuration terminal
Step 4 Enter the interface configuration mode for the Telnet interface. The 0 and 4 indicate that you are configuring all 5 possible Telnet sessions.	line vty 0 4

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

Copyright © 1997
Cisco Systems, Inc.
All rights reserved.

Task	Command
Step 5 Enter a password.	password <i>password</i>
Step 6 Return to EXEC mode so you can confirm the entry.	end
Step 7 Display the running configuration. The password is listed under the command <code>line vty 0 4</code> .	show running-config
Step 8 As an option, save the running configuration to the startup configuration.	write mem

Cisco IOS 11.2(8) SA Caveats

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(8) SA. Unless otherwise noted, these caveats apply to all Cisco IOS 11.2 releases up to and including 11.2(8) SA.

- CSCdj31392**

Cannot use the CDP name to connect to the CDP neighbor from the CDP HTML page.

If the CDP name of a CDP neighbor is not registered to a domain name server, the user cannot connect to the CDP neighbor by choosing the CDP name and clicking on the **Telnet** box 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 CDP HTML page.
- CSCdj36629**

Monitor port transmits its own BPDUs.

When a port is set to be a monitor port, the port still transmits its own BPDUs. It should only transmit frames transmitted by ports it monitors.

Ignore the monitor port BPDUs during traffic analysis.
- CSCdj43070**

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, does nothing.

Do not enter router-based IOS commands such as **ip routing**.
- CSCdj47044**

If the user uses `?` when entering an interface name of a CLI command to find out the available module numbers, the module number (interface number) that the help prompt displays is incorrect.

Depending on whether the system has no module, only one module, or two modules, the available module numbers are 0, 0-1, or 0-2.
- CSCdj47912**

IGMP group addresses cannot be registered on secure ports.

Configure a secure port, and then attach an IGMP host to that port. The IGMP host will not be added to IGMP multicast groups.

IGMP and secure ports are not compatible. In order to use IGMP, turn off port security on all ports to which IGMP hosts and routers are attached.

- CSCdj47945

IGMP hosts whose station addresses are in the static address table will not join IGMP multicast groups.

Configure a static address for the MAC address of an IGMP host. When the IGMP host attempts to join a multicast group, it will not be added to the group.

Static addresses and IGMP are not compatible. Delete the station address from the static address table, and allow it to be dynamically learned. The station can then join the CGMP multicast groups.

- CSCdj48602

Turning on Port Fast on ports in a Fast EtherChannel port group might cause connectivity loss between switches.

When two switches are connected by a port group, and the user turns on Port Fast on ports in the port group, the connectivity between the two switches might be lost when one of the ports in the port group loses link.

The workaround is not to turn on Port Fast on ports in a Fast EtherChannel port group.

- CSCdj48915

Cannot tar directly from Xmodem.

If the user uses the **tar** command to tar directly from Xmodem, the command will fail, and an error message will be printed on the console.

The workaround is to copy the file to the Flash file system using Xmodem, and then use the **tar** command to tar the local tar file. Alternatively, the user can tar directly from TFTP.

- CSCdj49285

On the Port Security HTML page, security action cannot be configured by choosing the security action and clicking **Apply**.

If security on a port is already enabled, modifying security action on the port and then clicking **Apply** does not configure port security.

The workaround is to disable port security, click **Apply**, and then reenables port security and set the security action before clicking **Apply**.

- CSCdj50013

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.

- CSCdj50275

The MAC Address aging time can be set to less than 10 seconds.

The valid range for the **mac aging-time** command is 0–1000000 seconds. The 802.1d specification states that the aging time for MAC addresses should be in the range 10–1000000. Therefore, the user can configure the switch to age addresses faster than is allowed by the 802.1d specification.

The user should not configure the **mac aging-time** with a value between 0–9.
- CSCdj50400

When the user uses the **reload** command to reboot the system, no prompt for saving configuration changes into NVRAM appears.

If the **clear** command is used to modify system configuration and the user uses the **reload** command to reboot the system, no prompt is given to remind the user to save the configuration change.

Either use a **write mem** command before using **reload** to reboot the system, or avoid using the **clear** command to modify system configuration.
- CSCdj50857

The user cannot add a static address through the HTML Web page if no output port is specified. Add the static address by using the CLI command: **mac-address-table static hwaddr input-port**.
- CSCdj51155

Telnet out from the system does not work.

Telnet from the system to other stations is not supported.
- CSCdj52165

Help description for the **tar** command is incorrect.

When the user uses the ? command to show the help description for CLI commands, the help description for the **tar** command is incorrect. It should be "List or extract a file from a tar image."
- CSCdj52719

Switch resets when extracting a module.

Modules cannot be dynamically installed and removed while the switch is running. First, turn off the switch, and then remove the module.
- CSCdj54388

On the HTML page that displays the switch, a port in STP blocking state is displayed in green.

If a port has a link and is not administratively down, the port is displayed in green on the HTML page, even though it is in STP blocking state. On the front panel of the switch, the LED above the port is amber if the port is in STP blocking state.

Go to the Spanning-Tree Management page to check the STP state of the port, or check the LED right above the port on the front panel of the switch to find out whether a port is in STP blocking state.

- CSCdj54447

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

When a monitor port is configured to monitor port 1, the STP and CDP packets transmitted by port 1 are not forwarded to the monitor port.

Switch the connections between port 1 and the monitor port, meaning to switch the connections to Port 1. Disable port monitoring on the monitor port and enable port monitoring on port 1.

- CSCdj57531

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 will not log into it.

Configure the switch port to operate at a fixed speed and specify the duplex mode, for example, 100 Mbps and half duplex. This will disable autonegotiation on the switch port and allow the link between the client and the switch to be 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.

- CSCdj57731

Address security violations are not reported when the switch address table is full.

Configure a port as a secure port and set a limit for the number of addresses that can be learned on that port. Then let the port learn the configured number of addresses on that port, and learn enough addresses on the other switch ports to fill up the switch address table. When packets with new source addresses (unsecured) are seen on the secure port, they are filtered, but they do not generate error messages or cause any security-violation actions.

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.

- CSCdj58119

The switch might reset if the user tries to set one of the switch ports own MAC address.

If the user tries to set a MAC address on a switch ports own MAC address as a secure address already on a secure port with the number of secure addresses equal to the maximum allowed for the port using the **mac-address** command, the switch resets.

The workaround is to avoid changing the switch ports own MAC address.

- CSCdj58539

Some configuration changes do not take affect when changing the configuration by using the web-based Switch Manager.

When making configuration changes using the web-based management, change more than 15 items before selecting **Apply**. For example, on the SPAN configuration page, change the settings on more than 15 of the check boxes. Then click **Apply**. Only 15 of the changes will actually take affect. The other configuration changes will be ignored.

When using the web-based management, do not make more than 15 configuration changes before clicking **Apply**.

- CSCdj35909

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

When configuring a port for port security and using SNMP to generate traps, address security violation traps are not sent when address security violations occur.

The security violations will appear on the console. Refer to the switch console for security violation messages, or configure the switch to send syslog messages to a server and examine them on that server.

- CSCdj36918

The MIB-II IpRoute table is always empty even though a default gateway has been defined.

Configure a default gateway by using the **ip default-gateway** command. Then get the MIB-II IpRoute table via an SNMP management station. The IpRoute table will be empty.

The MIB-II IpRoute table only contains entries if Cisco IOS is running on a router. As this is a switch, not a router, the IpRoute table will always be empty.

- CSCdj44968

A message appears on the console shortly after booting which says:

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

Enable SNMP with the **snmp-server** command on a Catalyst 2900 series XL. When the system boots, the above message will appear.

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

- CSCdj47348

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.

- CSCdj47637

A switch port loses link.

If the speed of a switch port is set to autonegotiate, and the user tries to force full duplex on the port, the port will lose the link.

The workaround is to set the port speed to 10 Mbps or 100 Mbps before forcing full duplex on the port.

- CSCdj47867

Traps are not sent for RMON events.

If an RMON event table entry with the eventType set to snmp-trap or log-and-trap, when the event occurs, a trap is not sent.

The events can be captured by selecting to log the events. The event log can be examined through the Cisco IOS command line.
- CSCdj48441

Bandwidth Group object in Cisco C2900 MIB are not updated.

Access the c2900Bandwidth* objects in the Cisco C2900 MIB via an SNMP manager. The objects will always return their default values.

These MIB objects are not implemented and therefore will always return the default values. Use statistics in the interface group of the MIB-II to derive bandwidth values.
- CSCdj48447

The value of private MIB object c2900PortRxSuppressBcastFrames is always zero.

The MIB object c2900PortRxSuppressBcastFrame, used to count the broadcast frames received that were discarded because of the threshold-based broadcast suppression, is not supported.
- CSCdj49182

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 CLI commands to set these variables.
- CSCdj49186

In the C2900PortEntry table, four objects are not maintained:

c2900PortNumberOfDroppedAddresses c2900PortFloodUnknownMulticasts
c2900PortAddrSecureAddrViolations c2900PortNumberOfLearnedAddresses

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

These objects are not currently supported. The values returned by these four objects should be ignored.
- CSCdj49195

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

Retrieve the c2900PortVisualIndicator object in the Cisco C2900 MIB. If the c2900InfoVisualIndicatorMode object is not portStatus, then the value returned will not reflect the true color of the LED. Instead, it will return the color of the LED as if the c2900InfoVisualIndicatorMode were set to portStatus.

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.

- CSCdj49197

The c2900ConfigAddressViolationAction and c2900PortFrameAge objects in the CISCO-C2900 MIB always return their default values.

Retrieve the c2900ConfigAddressViolationAction or c2900PortFrameAge objects from the CISCO-C2900 MIB by using any SNMP manager. These objects will return the default values regardless of their current settings.

If the default values for these MIB objects are altered, do not rely on their current values to be returned by the MIB.

- CSCdj49295

The EntryStatus of an RMON table entry cannot be changed from Valid to underCreation.

Create a table entry in one of the RMON tables, such as the HistoryControl table. After the table entry is created, the EntryStatus for that row should be Valid. Change the EntryStatus for that row to underCreation. This status transition will not be allowed.

To re-create an RMON table entry, first change the status of the row from Valid to Invalid. Then the row can be re-created by adding the row with a status of CreateRequest.

- CSCdj49296

The historyControlIndex in the RMON MIB can be greater than 65535.

Create an entry in the HistoryControl Table with an index that is greater than 65535. The switch will allow this to occur, even though the range of values for the historyControlIndex is supposed to be 1–65535.

No workaround is necessary, as the switch functions properly regardless of the historyControlIndex value. For compliance with the RMON MIB, however, do not specify a historyControlIndex value greater than 65535.

- CSCdj49324

The RMON monitoring of ifIndex.1 doesn't work properly.

Create a History Control entry which specifies ifIndex.1 as the interface to monitor. The values in the Ether History Group will not be updated.

The ifIndex.1 interface refers to the internal, or CPU, interface to the network. As this is an internal interface, RMON monitoring of this interface is not supported. This interface, therefore, should not be specified in the historyControlDataSource.

- CSCdj50083

All OwnerString and DisplayString RMON MIB variables can be set to strings longer than 127 octets.

Create an RMON table entry with an OwnerString that is greater than 127 octets. The SNMP "set" of this table entry will not be rejected, even though the maximum length of an OwnerString should be 127 octets.

As this is an expansion of the capabilities of the RMON MIB, no workaround is necessary. To remain strictly compliant with the RMON MIB, do not define any OwnerString or DisplayString objects longer than 127 octets.

- CSCdj50306

RMON reports all traffic on an interface, not just receive traffic.

Use RMON to retrieve the traffic statistics on a port, such as the Ethernet Statistics Group. The statistics retrieved contain all of the traffic on that port (both the traffic transmitted and received) not just the traffic received.

There is no workaround necessary. This operates differently from other Cisco RMON implementations, so it is documented here.

- CSCdj50342

The number of entries in the RMON EtherHistory Table is one less than the number of buckets granted in the historyControl Table.

Create an entry in the RMON HistoryControl table with ten buckets. The entry is created and the number of buckets granted will display ten buckets. The number of entries in the EtherHistory table will be one less than the number of buckets granted, or nine in this case.

If a specific number of entries in the EtherHistory table is desired, request one extra bucket in the historyControlBucketsRequested object in the HistoryControl table. This will cause the correct number of entries to be created in the EtherHistory table.

- CSCdj50759

Entries in RMON tables can be set to underCreation with incomplete data source object identifiers.

Create an entry in the etherStats, etherHistoryControl, or alarm table with a data source field set to ifIndex (instead of ifIndex.1, for example). Setting the status of this row to underCreation will be accepted by the switch.

Specify the complete interface object identifier when creating a row in a table. If a partial identifier is specified, the row cannot be set to valid, but must be set to invalid.

- CSCdj50799

Creating an RMON event table entry via the CLI with a duplicate eventIndex writes over the previous entry.

Create an entry in the RMON event table with the **rmon event** command. Create a second entry in the table with the same event number (eventIndex). The second entry will supersede the first entry, which will no longer exist.

When creating entries in the RMON event table via the CLI, be sure to choose unique event numbers for each entry.

- CSCdj51546

Creating RMON event table entries with large eventIndex fields will cause CPUHOG messages on the console.

Create an entry in the RMON event table with an eventIndex greater than 1000. Then get this entry from an SNMP management station with a get-next operation. The CPUHOG message will appear 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.

- CSCdj51560

The value of the STP RootPort number shown from SNMP (Bridge MIB object dot1dStpRootPort) is incorrect.

Use the CLI **show spantree** command to find out the STP RootPort number.

- CSCdj51594

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 CLI **show spantree** command.

- CSCdj51607

STP Topology Change Number does not increase.

When the switch STP topology changes from root to non-root, its Topology Change Number does not increase. The Topology Change Number increases when the switch STP topology changes from non-root to root.

Do not rely on Topology Change Number to count the times STP topology has changed.

- CSCdj51956

After entering a **write erase** command, the **show running** command returns an error.

When executing the following commands

```
Switch# write erase
[OK]
Switch# show run
Non-Volatile memory is in use
```

The error message after **show run** is incorrect.

Do not use 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.

- CSCdj53272

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.

If a port on the switch is connected to a device that uses the National DP83840 PHY part and autonegotiation is turned on for the port, neither the port nor the device gets link after the device is power-cycled.

Disable both speed and duplex autonegotiation on the port, and set the speed and duplex mode on the port to match those of the link partner.
- CSCdj53486

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

Configure an interface for broadcast storm control, and generate broadcast frames to that interface at a rate greater than the rising threshold. The **show interface** command for that interface will not count the frames that were filtered due to broadcast storm control.

If an accurate number of broadcast frames received on an interface is required, do not enable broadcast storm control on the interface.
- CSCdj53500

No link is detected on a port connected to a device via cable of a certain length.

If a port is connected to a 100-Mbps capable link partner via a cable of a certain length (35–41 meters), and the partner does not autonegotiate, the port might not get the link.

Turn off both speed and duplex mode autonegotiation on the port, and set the speed and duplex mode on the port to match those of the link partner.
- CSCdj53587

The etherHistoryUtilization in the RMON Ethernet History Group is incorrect.

Generate traffic on a 100-Mbps link, and retrieve the etherHistoryUtilization for that link. The value will be incorrect.

The utilization calculation assumes that the network speed is 10 Mbps. Therefore, utilizations that are greater than 100 percent might be reported on 100-Mbps interfaces. The etherHistoryUtilization can be converted for 100-Mbps interfaces by dividing the reported value by 10.
- CSCdj54209

SNMP ifInUcastPkts/ifOutUcastPkts and ifInNUcastPkts/ifOutNUcastPkts counters are incorrect.

When multicast packets are received or sent by the switch, SNMP ifInUcastPkts/ifOutUcastPkts counters are incremented, and ifInNUcastPkts/ifOutNUcastPkts counters remain unchanged. According to RFC 1573, multicast packets shall be included in ifInNUcastPkts and ifOutNUcastPkts counters.

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

- CSCdj54230

The value reported in the RMON MIB Ethernet Statistics Group etherStatsCollisions object does not match the value reported by the **show interface** command.

Retrieve the etherStatsCollisions RMON MIB object by using any SNMP management station, and then enter the **show interface** command. The collisions value printed might not match the value retrieved from the RMON MIB.

No workaround is necessary. The value reported in the MIB is a total of the number of collisions that transmit and receive packets experience. The value that the **show interface** command displays is the number of frames that were transmitted with collisions. Therefore, frames that experience multiple collisions will be counted multiple times in the MIB while being counted only once in the **show interface** output.

- CSCdj54636

The status of an RMON table entry can be changed from invalid or non-existent to valid.

Create an entry in an RMON table with an EntryStatus of valid. The SNMP "set" will be accepted, even though the RMON specification does not allow such state transitions.

This is an expansion of the capabilities of the RMON specification. If it is desired to strictly follow the RMON specification, do not set the EntryStatus to valid from the invalid or non-existent states.

- CSCdj55491

Cannot access the web-based CLI after periods of extremely high network activity.

Generate wire-speed traffic on all ports with random source addresses. Then access the switch through the web, and select Monitor the Switch link on the home page. The web-based CLI might not be available.

Access the switch directly through the serial port or through Telnet. Interface with the CLI through these methods instead of the web-based CLI.

- CSCdj55499

Some commands executed through the web-based CLI use excessive amounts of memory and thus will not work.

Enter the **show startup-config** command through the web-based CLI. This command will produce an error message on the console, indicating that the switch is out of memory.

For commands that do not complete properly on the web-based CLI, enter the commands through the serial port console or a Telnet session.

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
- 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, Cache Director System, the CCIE logo, CD-PAC, Centri, Centri Bronze, Centri Gold, Centri Security Manager, Centri Silver, the Cisco Capital logo, Cisco IOS, the Cisco IOS logo, *CiscoLink*, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, Fast Step, FragmentFree, IGX, JumpStart, Kernel Proxy, LAN²LAN Enterprise, LAN²LAN Remote Office, MICA, Natural Network Viewer, NetBeyond, Netsys Technologies, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, StrataSphere, StrataSphere BILLder, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratum, StreamView, SwitchProbe, *The Cell*, TokenSwitch, TrafficDirector, VirtualStream, VlanDirector, Workgroup Director, Workgroup Stack, and XCI are trademarks; The Network Works. No Excuses. is a service mark; and BPX, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, EtherChannel, FastHub, FastPacket, ForeSight, IPX, LightStream, OptiClass, Phase/IP, StrataCom, and StrataView Plus 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 © 1997, Cisco Systems, Inc.
All rights reserved. Printed in USA.
9711R

