



Release Notes for the Catalyst 1900 and Catalyst 2820 Series Switches, Version 9.00

October 2, 2000

These release notes provide information on the Catalyst 1900 and Catalyst 2820 series Ethernet switches (hereafter referred to as the Catalyst 1900 switches and the Catalyst 2820 switches) using Standard and Enterprise Edition firmware version 9.00.04.



This document describes the problems that are resolved in versions 9.00.00 through 9.00.04.

Contents

- “Using Previous Releases of the Switch Firmware” section on page 2
- “Supported Browsers” section on page 2
- “New Features” section on page 3
- “Problems Resolved Since Version 9.00.00” section on page 4
- “Problems Resolved in Version 9.00.00” section on page 4
- “Limitations” section on page 5
- “Usage Guidelines” section on page 8
- “Related Documentation” section on page 11
- “Cisco Connection Online” section on page 11
- “Documentation CD-ROM” section on page 12

The tracking numbers for some items in this document are added for your convenience.



Using Previous Releases of the Switch Firmware

The Catalyst 1900 and Catalyst 2820 switches are now shipped with firmware version 9.00.02. Depending on the board version of your switch, the minimum firmware releases listed in Table 1 are required.

The “System Revision” field on the System Configuration menu displays the board revision of your switch. When you use the **show version** command from the command-line interface (CLI), the “Hardware Board Revision Is” field displays the board revision.

The Firmware Configuration Menu and the Console and Upgrade Configuration page display the firmware version in use.

Table 1 Supported Firmware on the Catalyst 1900 and Catalyst 2820 Switches

Board Revision	Switch	Supported Firmware Version
1	Catalyst 1900-A Catalyst 1900-EN	6.x or higher
1	Catalyst 2820-A Catalyst 2820-EN	6.x or higher
4	Catalyst 1900-A Catalyst 1900-EN	8.00.04 or higher
5	Catalyst 1900-A Catalyst 1900-EN	8.01.00 or higher
5	Catalyst 2820-A Catalyst 2820-EN	8.01.01 or higher

Supported Browsers

To use the Catalyst 1900 or Catalyst 2820 Switch Manager, you must have one of these web browsers installed on your management station:

Table 2 Browser Support for Web-based Management

Browser	Minimum Version	Supported Version
Netscape Communicator	4.5	4.5, 4.51, 4.61
Microsoft Internet Explorer	4.01a	4.01a, 5.0



Note

Netscape Communicator 4.60 is not a supported browser. Microsoft Internet Explorer is not a supported browser on Solaris 2.5.1 or higher operating systems.

For information about configuring your browsers, see the *Catalyst 1900 Series Installation and Configuration Guide* and *Catalyst 2820 Series Installation and Configuration Guide*.

New Features

The following features were added in version 9.00.00:

- Cluster membership capability—The Catalyst 1900 and Catalyst 2820 switches can be added to switch clusters and managed by a Catalyst 2900 XL or Catalyst 3500 XL command switch. The following requirements must be met:
 - The Catalyst 2900 XL or Catalyst 3500 XL command switch must be running IOS Software Release 12.0(5)XP or higher and must have an IP address assigned.
 - The Catalyst 1900 or Catalyst 2820 switch must be running firmware version 9.x or higher.
 - The Catalyst 1900 or Catalyst 2820 switch must be CDP version 2-enabled.
 - The Catalyst 1900 or Catalyst 2820 switch must be connected to a cluster member or to a command switch port that belongs to the management VLAN on the command switch.
- Encrypted (secret) passwords—You can assign encrypted privileged- and user-level passwords to the switch. An encrypted password can have 1 to 25 characters, including spaces and punctuation. Encrypted passwords are case-sensitive.
- Secured access to management interfaces—At initial setup, you can assign a switch IP address and an unencrypted privileged-level password to the switch. A privileged password, encrypted or unencrypted, must be assigned to the switch to access the Catalyst 1900 or Catalyst 2820 Switch Manager and to Telnet to the switch.
- Security enhancement to password recovery—On previous releases of the firmware, you could view the password from the diagnostic console, which posed a security threat to networks that used the same password for other devices in the network. When using the diagnostic console, you can now only clear the switch password if you have lost or forgotten it.
- Additional SNMP community strings—You can assign up to four Read and four Write community strings from the Catalyst 1900 or Catalyst 2820 Switch Manager.
- Clear addresses on link down—You can enable a secured switch port to remove its address associations when the port loses its link.
- TFTP Put option disabled by default—To prevent unauthorized upgrades, the Accept Upgrade Transfer from Other Hosts option default setting is Disabled.
- Increased RMON history tables—The switch supports a maximum of 540 RMON history tables. However, previous releases of the firmware only supported up to 20 RMON history tables for each switch port. You can now allocate the 540 history tables among all switch ports, in any combination. For example, you can allocate 540 history tables to one switch port, or you can allocate 20 history tables among 27 ports.
- CGMP Fast Leave—This option enables the switch port to leave an IP multicast group immediately when all the members have left the multicast group.
- Message-of-the-day banner—From the CLI, you can create a 400-character (or 20-line) message, which is displayed before the management console logon screen is displayed.

Problems Resolved Since Version 9.00.00

Version 9.00.04 corrects a condition on the Catalyst 1900 and 2820 switches running Enterprise Edition firmware that caused VLAN Trunk Protocol (VTP) configuration information to be lost. The VTP mode changes from transparent or server mode to client mode after VTP parameters are configured. In version 9.00.03, these parameters were lost after the switch was reset, and the switch would revert back to server mode. [CSCds28410]



Note

Upgrading to version 9.00.04 can cause the loss of restricted static addresses. If you have restricted static addresses configured, save your configuration file to a TFTP server before upgrading. Upgrade to version 9.00.04, and then reload your configuration file.

Version 9.00.03 corrected an anomolous user-invoked system reset condition. If you reset the system through the console interface (as opposed to recycling power), it was statistically possible for a single random port on the unit to fail to acquire link and operate properly. You would then observe a nonfunctional or dead port. Power cycling the switch corrected the problem. The software modification reset all ports in the switch so that a port cannot lock up immediately after a user-invoked reset.

The following problem was resolved in version 9.00.02:

- Catalyst 1900 and 2820 switches can no longer cause spanning-tree loops when UplinkFast is enabled. [CSCdp70664]

The following problems were resolved in version 9.00.01:

- If you issue a Get_Next_Request in an SNMP MIB list on an interface, there is no longer an extra entry at the end that does not belong. [CSCdp09675]
- In a Telnet session, the paste function in the CLI configuration mode now works correctly. [CSCdm14589]

Problems Resolved in Version 9.00.00

The following problems were resolved in version 9.00.00:

- The CDP checksum algorithm was changed to be compatible with the Cisco IOS software. Previously, when a CDP packet has an odd number of bytes and the value of the last byte is greater than 0x80, the device sending the packet is not recognized as a neighbor.
- You can use a DEC Alpha 1000a BOOTP server to automatically assign an IP address to the switch. [CSCdm80245]
- The switch can now autoconfigure from a DHCP server that is *not* Windows NT. [CSCdm85421]
- You can use the ipNetToMediaEntry MIB object from a Catalyst 1900 WS-C1912 model. [CSCdm87247]
- Whether in VTP transparent or server mode, the switch drops VTP packets from blocked ports and no longer receives and forwards these packets to unblocked ports. [CSCdm58378]
- The switch can use a CiscoSecure NT TACACS server to authenticate access based on the switch IP address. [CSCdm83795]

Limitations

The following sections provide usage limitations for the switches:

- “Limitation Specific to the Catalyst 2820 Switches” section on page 5
- “Limitations for the Catalyst 1900 and Catalyst 2820 Switches” section on page 6

Limitation Specific to the Catalyst 2820 Switches

After removing or inserting a module, click **Reload** to display a fresh switch image on the Home page.

Limitations for the Catalyst 1900 and Catalyst 2820 Switches

- When using Netscape Communicator 4.xx on Sun workstations, minimized and maximized pages of the Catalyst 1900 and Catalyst 2820 Switch Manager might not refresh properly. Click **Reload** to refresh the page.

When using Netscape Communicator 4.xx on PCs and Sun workstations, resized pages of the switch manager might not refresh properly. Click **Reload** to refresh the page. [CSCdj85607]

- Clicking **Reload** from any switch manager page displays a fresh copy of the Home page, not the currently displayed page.
- When using Netscape Communicator 4.xx on Windows 95, clicking **Apply** after making changes to the Port Security Table page sometimes displays a blank page. Click **Stop** to redisplay the Port Security Table page with your saved changes. [CSCdj95153]
- The switch manager does not check parameter values that are outside the value range. If you enter an invalid parameter value, the switch manager redisplay the switch manager page with the original value. Parameter value ranges are provided in the management console, the switch manager online help, and the *Catalyst 1900 Series Installation and Configuration Guide* and *Catalyst 2820 Series Installation and Configuration Guide*.
- The Catalyst 1900 and Catalyst 2820 switches do not support the hidden-enable password. If the switch inherits the command-switch hidden-enable password, the switch stores the password as an unencrypted password. When your cluster contains Catalyst 1900 and Catalyst 2820 member switches, we recommend that you assign a secret enable password to the command switch. [CSCdp16523]
- Do not use the following settings for the console port when upgrading the switch through the XMODEM protocol: 9600 baud, 7 data bits, 2 stop bits, and even parity. Use other settings or the console port default settings (9600 baud, 8 data bits, 1 stop bit, and no parity). [CSCdj87375]
- If you use bridge groups and Spanning-Tree Protocol (STP) is disabled on a bridge group, the switch does not forward the bridge protocol data units (BPDUs) received on any ports in the bridge group to other members of the bridge group. If you are running STP on the rest of your network, network loops might result if the switch connects to other switches. [CSCdk01665]

If the problem occurs and you want to use bridge groups with STP disabled, you must disable STP on *all* bridge groups so that the switch forwards received BPDUs. Assign at least one port to all bridge groups, and then disable STP for each bridge group, using the Bridge Group Spanning Tree Configuration menu (or CLI or SNMP). You can then reassign the ports to whichever group you wish.

- RMON statistics gathering has the following maximum limits:
 - 27 rows in these tables: etherStatsTable, historyControlTable, alarmTable, and eventTable.
 - If you are logging events, you can have 10 entries per event, and the list is circular.

- Networks that use IBM Type 1 cabling can have the following problems if the cable becomes disconnected:
 - Ports configured as monitor ports in an environment using IBM Type 1 cabling should be configured for half-duplex operation because the switch does not detect a loopback if the hermaphroditic connector on the cable is disconnected. [CSCdk66781]
 - In a full-duplex configuration with Spanning-Tree Protocol (STP) disabled, the switch does not detect a loop if an IBM Type 1 cable is disconnected. Therefore, configure ports for half-duplex operation if you must have STP disabled. [CSCdk57978]
 - If a 100-Mbps switch port has a disconnected IBM Type 1 cable, a change to the Port Fast mode does not take effect until you reset the switch. [CSCdk67260]
 - If a full-duplex port is assigned to more than one bridge group and an IBM Type 1 cable is disconnected, the switch might not detect a loopback. [CSCdk67219]
 - If a nonroot switch is bridged to a root switch through full-duplex ports using IBM Type 1 cabling, the root port on the nonroot switch might take longer to reach the STP blocking state if the cabling is disconnected and creates a loopback. [CSCdk67682]
 - If a dynamic port that is assigned to a VLAN is disconnected and reconnected to a different station, the VLAN of the port is not rediscovered. Change the port to half duplex so that the switch assigns the port to a new VLAN. [CSCdk67157]

- If there are two or more Catalyst 1900 or Catalyst 2820 switches connected to a Catalyst 5000 switch using Fast EtherChannel—and if there are two stations communicating through the Catalyst 5000 switch—the switches learn the addresses of both stations from the broadcast packets sent from those stations. Flooding of unknown unicast packets can occur if one of the stations becomes disconnected from the Catalyst 5000 switch and the other station continues to send packets to that station. The flooding stops when the switches reach the specified aging time for retaining the address of the disconnected station.

Use the **port-channel preserve-order** command to preserve the frame transmission order on the switch port. [CSCdk69024]

- When using the Fast EtherChannel feature with VLAN trunking between two Catalyst 1900 or Catalyst 2820 switches, changing the active link might cause flooding. You can change an active link either by changing the Port Aggregation Protocol (PAgP) port priority or by disconnecting one of the high-speed links and reconnecting it. We recommend that you disconnect both ports to change the active link. [CSCdj89498]
- If you use VTP pruning with Fast EtherChannel, losing one connection on one high-speed link prevents pruning from working properly. This does not cause connectivity problems, but flood traffic is sent to the neighboring switch (which should drop such traffic, resulting in minimal degradation to network performance). Pruning still works in the neighboring switches. Disconnect the remaining link, and then reconnect both links to restore proper operation of VTP pruning. [CSCdk01961]
- When a Catalyst 1900 or Catalyst 2820 switch is operating at the edge of a VTP domain and is subsequently configured for VTP transparent mode, trunk ports will not be in the correct pruning state. You need to reestablish the trunk after changing the VTP mode to transparent. Reestablish the trunk in one of the following ways:
 - Remove, and then reconnect the trunk cable to the switch.
 - Disable, and then re-enable the trunk either by using the **trunk off** and **trunk on** commands or by using the Port Configuration Menu [S] Status of Trunk option.
 - Reset the switch.

[CSCdp08683]

Usage Guidelines

The following sections provide usage limitations for the switches:

- “Usage Guidelines Specific to the Catalyst 1900 Switches” section on page 8
- “Usage Guidelines Specific to the Catalyst 2820 Switches” section on page 8
- “Usage Guidelines for the Catalyst 1900 and Catalyst 2820 Switches” section on page 9

Usage Guidelines Specific to the Catalyst 1900 Switches

- Some switches are shipped with screws installed in the top rack-mounting holes closest to the front panel. If you want to rack-mount the switch with the front panel forward, remove these screws before attaching the mounting brackets. Do not use these screws to attach the mounting brackets to the switch. Use the screws supplied with the brackets. For information on attaching the mounting brackets to the switch, see the *Catalyst 1900 Series Installation and Configuration Guide*.
- If you connect to the switch AUI port, you might notice that the fan in the switch slows down. This does not affect the operation of the switch.
- If there is no link after you connect an MT-RJ fiber-optic port on a WS-C1924F-A or a WS-C1924F-EN switch to an SC port on a 100BaseFX-compatible device, the polarity of the SC connectors on the MT-RJ patch cable and the SC port on the device might not match. Remove the SC connectors from the snap-on holder on the cable, and transpose the connectors for A and B.
- If you connect an autonegotiating 100BaseTX port of a Catalyst 1900 switch to a device that does not autonegotiate, there could be problems establishing a link. To work around this problem, configure the switch port to either half or full duplex to match the configuration of the other device.
- After you select Auto-negotiate as the 100BaseTX port duplex mode from the Port Management page and click **Apply**, “Auto-negotiate” displays in the Actual field while the switch and the other device negotiate the duplex mode. Click the **Port** option on the Catalyst 1900 Switch Manager menu bar to display the final duplex state of the port. [CSCdk03911]

Usage Guidelines Specific to the Catalyst 2820 Switches

- If you try to upgrade the module firmware from the Catalyst 2820 Switch Manager and the **Module (Slot A or B) TFTP Upgrade** button is not on the Console and Upgrade Configuration page, the module firmware is corrupted. Do not continue the upgrade attempt from the switch manager. Use the management console to upgrade the module firmware. [CSCdj92758]
- After you select Auto-negotiate as the 100BaseTX switch module port duplex mode from the Module Management page and click **Apply**, “Auto-negotiate” displays in the Actual field while the switch and the other device negotiate the duplex mode. Click the **Module** option on the switch manager menu bar to display the final duplex state of the port. [CSCdk03911]
- If your attempt to upgrade the ATM module firmware fails while the module is operating normally, the expansion slot LED on the switch turns amber. The module continues operation, but the module image in Flash memory is corrupted. When you reset the ATM module, it will not find a valid Cisco IOS image, and the ATM module will not pass the power-on self-test (POST). To correct this problem, repeat the firmware upgrade procedure to download a new firmware image on the ATM module.

- If you connect an autonegotiating 100BaseTX switch module port of a Catalyst 2820 switch to a device that does not autonegotiate, there could be problems establishing a link. To work around this problem, configure the module port for either half or full duplex to match the configuration of the other device.

Usage Guidelines for the Catalyst 1900 and Catalyst 2820 Switches

- The RJ-45-to-DB-9 female DTE (labeled PC) adapter is now the only adapter that ships with the Catalyst 1900 and Catalyst 2820 switches. You can order a kit (part number ACS-DSBUASYN=) containing the RJ-45-to-DB-25 female DTE adapter and RJ-45-to-DB-25 male DCE adapters from Cisco.
- The DOS diskette containing the switch firmware and device-specific MIBs is no longer shipped with the switch. You can download the latest switch firmware and MIBs from the Service and Support site on Cisco Connection Online (CCO). For information about CCO, see the “Cisco Connection Online” section on page 11.
- Be sure that JavaScript is enabled. From Netscape Communicator 4.xx, select **Edit>Preferences>Advanced>Enable JavaScript**. JavaScript is enabled by default on Microsoft Internet Explorer.
- Be sure the switch manager page is updated whenever you visit the page. Set the caching of pages to **Every time** on Netscape Communicator or **Once per session** on Microsoft Internet Explorer.
- You can bookmark the switch IP address to easily retrieve the switch manager for later use.
 - If you are using Netscape Communicator, choose the **Communicator** menu option, and select **Bookmarks>Add Bookmark**.
 - If you are using Microsoft Internet Explorer, choose the **Favorites** menu option, and select **Add to Favorites**.

Do not use the right mouse-button to bookmark the switch IP address; doing so only saves the specific frame (image) of the switch manager page.

- If the switch is directly connected to a terminal or terminal emulator rather than to a modem connection, you must configure the switch to the same baud rate and character format as the terminal or emulator.

If the switch is dialing out, the configured baud rate of the switch does not change. The Match Remote Baud rate option (auto baud) applies only when the switch is answering an incoming call and matches a rate less than or equal to the configured rate. When the call is over, the switch reverts to the last configured baud rate.

- Be sure that the port monitoring feature (used for diagnostics) is disabled during normal operation. Enabling the port monitoring feature can degrade the performance of the switch.
- When the switch does not have its own IP address and is a cluster member, the Telnet link on the Catalyst 1900 or Catalyst 2820 Switch Manager Home page is disabled. To Telnet to the switch, you must use the **command member-number** command from the command-switch CLI. [CSCdm69165]

- When a switch port is assigned to be the network port, unknown unicast address packets are only sent to that port. If an attached device, such as a server, is idle for longer than the specified address aging time value, the switch removes the device address from its address table. Therefore, if a network port is assigned, the switch does not forward any unknown unicast address packets destined to that device.
 - Configure a static address for the server.
 - Increase the address aging time to a value higher than the maximum idle time for the server.
 - Enable port security on the switch port connected to the server, set the upper limit of the number of addresses the secure port can have, and set the Action Upon Address Violation option to Ignore.
 - Do not use the network port.

[CSCdj55509]

- Bridge group configuration is supported on the management console and the CLI, but not on the switch manager.
- When you have bridge groups enabled, the switch manager displays information only for bridge group 1.
- Do not connect a port that belongs to more than one bridge group to another port in any of those bridge groups; this causes a network loop.
- VLAN configuration is supported on the management console and the CLI, but not on the switch manager.
- Fast EtherChannel configuration is supported on the switch manager and the CLI, but not on the management console.
- When you have VLANs enabled, the switch manager displays information only for VLAN 1.
- The switch resets when you change from using VLANs to bridge groups and vice versa, and any configured options revert to the default settings. You will need to reconfigure the options that you need for VLANs or bridge groups.

Use the System Configuration menu, CLI, or SNMP to change from VLANs to bridge groups and vice versa.

- When the switch initializes after a reset or when a port is assigned a different VLAN membership, the port experiences the complete Spanning-Tree Protocol (STP) transition, as specified by IEEE 802.1D, even if Port Fast mode is enabled. When the transition is complete, the Port Fast mode setting is enforced. This process ensures that no temporary loop is formed after a reset and allows STP to safely discover the topology of the network.
- If trunking mode is enabled after the switch initializes, the switch can take up to 5 minutes to automatically learn VLAN Trunk Protocol (VTP) information from the network.
- To prevent the formation of undetected loops, nontrunk ports assigned to different VLANs must not be connected to each other. Use routers to connect devices residing on different VLANs.
- When the trunking capability is enabled on a high-speed port, the port configuration on the following features is ignored, and the default configuration is used:
 - VLAN membership configuration for that port.
 - STP Port Fast mode (default: disabled on high-speed ports).
 - Flooding of unknown unicast and unregistered multicast packets (default: enabled).
 - Network port configuration (default: no network port is configured). When trunking is disabled, the port configurations function as configured.

- Be sure the management VLAN is not pruned if VTP pruning is enabled. You cannot use IP to manage the switch if the management VLAN is pruned. [CSCdj34652]
- When the Fast EtherChannel feature is enabled, remember the following:
 - Spanning-tree state for the port channel is shown as N/A on the Port Configuration menu for port A or port B. To find out the actual state of the port channel, use the Fast EtherChannel Management page, the CLI, or the SNMP Bridge MIB.
 - VTP pruning statistics on the VTP Statistics Report apply to the port channel as a whole, not specifically to port A or port B. [CSCdj92968]
- Switch configuration changes take effect immediately. However, the switch requires 30 seconds to write changed parameters to permanent storage. If you turn off the switch too soon, the changes to the switch configuration are lost the next time the system is restarted.
- While performing a firmware upgrade, the switch might not respond to commands for as long as 1 minute. This is normal and correct. If you interrupt the transfer by turning the switch off and on, the firmware could be corrupted. If this happens, follow the procedure described in “Using the Diagnostic Console” in the “Troubleshooting” chapter of the *Catalyst 1900 Series Installation and Configuration Guide* or *Catalyst 2820 Series Installation and Configuration Guide*.

Related Documentation

Use the following Catalyst 1900 and Catalyst 2820 publications for firmware version 9.x with this document:

- *Catalyst 1900 Series Installation and Configuration Guide*
- *Catalyst 2820 Series Installation and Configuration Guide*
- *Installing the Cisco Catalyst 1900/2820 Enterprise Edition Software*
- *Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide*
- *Catalyst 1900 Series and Catalyst 2820 Series Command Reference* (online only)
- *Catalyst 2820 Modules User Guide*
- *Catalyst 2820 ATM Modules Installation and Configuration Guide*

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>
- 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.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is orderable as a single package or as an annual subscription on the World Wide Web at <http://www.cisco.com/subscription>. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

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

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, CiscoLink, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQuick Study, iQ Readiness Scorecard, The iQ Logo, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document/website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0008R)

Copyright © 2000, Cisco Systems, Inc.
All rights reserved.