



Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges Running Firmware Version 11.23T

July 31, 2002

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running firmware version 11.23T.

Contents

- [Introduction, page 2](#)
- [New Features, page 2](#)
- [Installation Notes, page 3](#)
- [Limitations and Restrictions, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 8](#)
- [Troubleshooting, page 10](#)
- [Obtaining Documentation, page 11](#)
- [Obtaining Technical Assistance, page 12](#)



Caution

If an access point or bridge configuration contains host names (*ftp.cisco.com*, for example) instead of IP addresses in one or more configuration fields, the access point or bridge might lose some or all of its configuration when you upgrade the firmware from 11.21 to 11.23T. Use IP addresses instead of host names in all configuration fields when upgrading from 11.21 to 11.23T.



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Introduction

Cisco Aironet Access Points are wireless LAN transceivers that can act as the connection point between wireless and wired networks or as the center point of a standalone wireless network. Cisco Aironet Bridges are wireless LAN transceivers that connect two or more remote networks into a single LAN.

The access point and bridge use a browser-based management system. The system settings are on web pages in the system firmware. You use your internet browser to view and adjust the system settings.

New Features

Firmware version 11.23T includes these new software features:

- Configurable radius message transmission interval
- Displayable active authentication servers
- Configurable time interval for automatic reattempt to return to the primary server

The radius retransmission interval and primary server reattempt interval features are configurable using the web, console, or SNMP interfaces.

Radius Message Transmission Interval

The Request Radius Retransmission interval is now configurable for both authentication and accounting servers. The default value is 5 seconds. The total number of maximum transmissions is also configurable and has a default value of 3. Using this value, if nothing is heard from the server within 5 seconds, a second retransmission request is transmitted. After three retransmission requests with no reply, the server is assumed to be down.

If the access point and the AAA server are connected through a low-speed network and the Radius Message Retransmission Interval is set too low, the network may become congested because the access point retransmits unacknowledged requests that have not yet reached the server.

Display of Active Authentication Servers

By viewing the authentication server screens, an administrator can determine the most recently used authentication server for the following authentication functions:

- EAP (802.1X) authentication such as LEAP, EAP-TLS, and EAP-MD5
- MAC address authentication

For each authentication function, the access point configuration specifies one or more authentication servers, with the first one designated the primary or default server. The remaining servers act as backup servers. By default, the primary server is the currently selected server for the respective categories.

An administrator can view any server currently selected for a particular function. The currently selected server for each of these functions is displayed in green text so that the administrator can easily determine the active server in each category. On the console or Telnet interface, the active server is identified numerically.

The following new SNMP MIB objects have been added to keep the index values of the currently selected authentication servers:

- **awcAaaServerDot1xCurrent**: index of current server for IEEE 802.1x authentication functions
- **awcAaaMacAddrAuthCurrent**: index of current server for MAC address authentication functions

Automatic Return to Primary Authentication Server

An administrator can configure a time period specifying how often the access point should check if the primary authentication server is reachable again.

A new SNMP MIB object, **awcAaaServerPrimaryReattemptPeriod**, has been added to hold this value. The default value is zero. When the value is set to zero, the access point never attempts to return to the primary server; therefore, the default behavior can be the same as prior releases of access point software.

Initially, when an access point needs to contact an authentication server for one of its authentication functions, it selects the primary server and uses it as long as it is reachable. When the access point detects that the primary server is not reachable, it notes the current system time as **primaryServerAttemptTime** and selects the next server in sequence. It shifts to that server and uses it as long as it is reachable.

When an access point needs to send an access request and the currently selected server is not the primary server for the function requested, it attempts to contact the primary server if the server has not been contacted for longer than the value of **awcAaaServerPrimaryReattemptPeriod**. If the access point receives a response within the server timeout period, it marks the primary authentication server as the currently selected server and uses it for future authentication purposes. Otherwise, the access point updates the **primaryServerAttemptTime** as the current time and continues to use the previously selected server for authentication functions.

Installation Notes

You can find the latest release of access point and bridge firmware at this URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

Portions of Configuration Might be Lost During Upgrade from 11.21 to 11.23T

If an access point or bridge configuration contains host names (*ftp.cisco.com*, for example) instead of IP addresses in one or more configuration fields, the access point or bridge might lose some or all of its configuration when you upgrade the firmware from 11.21 to 11.23T. Use IP addresses instead of host names in all configuration fields when upgrading from 11.21 to 11.23T.

Installation in Environmental Air Space

Cisco Aironet 350 Series Bridges and metal-case access points are suitable for use in environmental air space in accordance with Section 300-22(c) of the *National Electrical Code*.



Caution

The Cisco Aironet power injector has a smaller operating temperature range (32 to 104°F; 0 to 40°C) than the 350 series bridge and metal-case access point. The power injector is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

Antenna Installation

For instructions on the proper installation and grounding of external antennas, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.

**Warning**

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.

Power Considerations

**Caution**

The operational voltage range for 350 series access points and bridges is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

Cisco Aironet power injectors are designed for use with 350 series access points and 350 series bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

System Requirements

You must have a 340 or 350 series access point or a 350 series bridge to install firmware version 11.23T.

Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 11.23T.
Your bridge must be running version 11.07 or later to install firmware version 11.23T.

Upgrading to a New Firmware Release

Determining the Firmware Version

The firmware version number is in the upper-left corner of most management screens in the web-browser interface and at the top of the home (Summary Status) page in the command-line interface.

Upgrade Procedure

For instructions on installing access point and bridge firmware:

1. Follow this link to the Cisco Aironet documentation home page:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>

2. Follow this path to the product, document, and chapter:
Aironet 350 Series Wireless LAN Products > Cisco Aironet 350 Series Access Points > Cisco Aironet Access Point Software Configuration Guide > Managing Firmware Configurations > Updating Firmware
3. Follow this link to the Software Center on Cisco.com and download firmware version 11.23T:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Note**

To upgrade firmware from a file server, you must enter settings on the access point's or bridge's FTP Server Setup page. Refer to chapter 6 in the *Cisco Aironet Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

This section describes limitations and restrictions for 340 and 350 series access points and 350 series bridges.

Cisco Aironet 350 Series Bridges Incompatible with 340 Series Bridges

Cisco Aironet 340 and 350 Series Bridges can be connected to the same LAN segments, but they cannot communicate wirelessly. Although you can disable STP on non-root 350 series bridges, 350 and 340 series bridges are not designed to interoperate. If you use both 340 and 350 series bridges on your network, make sure the 340 series bridges have radio bridge links only to other 340 series bridges, and that 350 series bridges have radio bridge links only to other 350 series bridges.

Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on an access point or bridge, allow the unit to finish its start-up sequence before removing power. If you update the firmware and remove power before the unit finishes the start-up sequence, the radio firmware might be corrupted, making the unit inoperable. If the radio firmware is corrupted, the radio indicator (the bottom of the three indicators on top of the access point or bridge) lights steady red, and the following error message appears when the access point or bridge starts up:

```
Failed to start driver for port "awc0" (errno=0x006d0002)
```

If the radio firmware is corrupted, you should try to reset the unit to factory defaults using the **:resetall** command in the CLI; see chapter 9 of the *Cisco Aironet Access Point Software Configuration Guide* for instructions on resetting the access point. If the unit cannot be reset to defaults, you must return the unit to Cisco for service.

You can safely remove power after a firmware update when the configuration management pages reappear in the command-line or web-browser interfaces, or when the three status indicators on top of the unit complete the following pattern:

1. All three indicators are steady green, meaning that the access point is beginning to update the firmware.

- The middle indicator is steady green and the top and bottom indicators are off, indicating that the access point or bridge is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can remove power.

EAP Authentication Requires Matching 802.1x Protocol Drafts



Note

This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1x protocol draft. For example, if the radio firmware on the client devices that will associate with an access point is 4.16, the access point should be configured to use Draft 8 of the 802.1x protocol. [Table 1](#) lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 1 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10 ¹
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ²	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.21 through 11.23T	—	x	x

- The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
- The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.



Note

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page in firmware version 11.06 or later to select the draft of the 802.1x protocol the access point or bridge radio should use. Follow these steps to set the draft for your access point or bridge:

-
- Step 1** Browse to the Authenticator Configuration page in the access point management system:
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Security**.
 - c. On the Security Setup page, click **Authentication Server**.
- Step 2** Use the 802.1x Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1x protocol the access point or bridge radio should use. Menu options include:
- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
 - Draft 8—Select this option if LEAP-enabled client devices that associate with this access point or bridge use radio firmware versions 4.13, 4.16, or 4.23.
 - Draft 10—This is the default setting in firmware versions 11.06 and later. Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point or bridge use radio firmware version 4.25 or later. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point or bridge reboots.
-

Select WEP Key 1 as Transmit Key for EAP Authentication

If you use Network-EAP as the authentication type on your wireless network, you must select key 1 as the transmit key on the access point or bridge AP Radio Data Encryption page. The access point or bridge uses the WEP key you enter in key slot 1 to encrypt multicast and broadcast data signals that it sends to EAP-enabled client devices. Because the access point or bridge transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point or bridge uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients. When you set up a non-root bridge or repeater access point to authenticate as a LEAP client, the bridge or repeater derives a dynamic WEP key and uses it to communicate with the root bridge or access point. Bridges and repeaters not set up for LEAP authentication use static WEP keys when communicating with other bridges and access points.



Note

If you do not use EAP authentication on your wireless network, you can select any WEP key as the transmit key. If you use EAP authentication and you enable broadcast key rotation, you can enable WEP without entering WEP keys.

MIB File Compatible with Firmware Version 11.00 and Later

The access point MIB file (AWCVX-MIB) is supported only by access point firmware version 11.00 and later. Earlier versions of firmware do not support this MIB. You can download the access point MIB at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Important Notes

This section lists important information about access points and bridges running firmware version 11.23T.

Reboot of Workgroup Bridges Required When Allowing More Than 20

With firmware version 11.23T, you can select **no** for the *Classify Workgroup Bridges as Network Infrastructure* setting on the AP/Root Radio Advanced page to allow up to 50 workgroup bridges to associate to the access point or bridge. After selecting **no** for this setting, you must reboot workgroup bridges associated to the access point or bridge.

Cisco Discovery Protocol Re-Enabled for Individual Interfaces on Reboot

The Cisco Discovery Protocol (CDP) feature is enabled by default, and CDP is enabled for each of the access point's or bridge's individual interfaces by default. However, if you disable CDP for one of the individual interfaces, the access point or bridge re-enables CDP for that interface when it reboots. If you disable CDP completely, the access point or bridge does not re-enable CDP on reboot.

Caveats

This section lists open and resolved software issues in firmware version 11.23T.

Getting Bug Information on Cisco.com

If you are a registered Cisco user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at <http://www.cisco.com/support/bugtools/>.

Open Caveats

The following caveats have not been resolved for firmware version 11.23T:

- CSCdw89705—When a non-root bridge roams from one root bridge to another, messages might appear in the logs of the root bridges stating that Ethernet devices connected to the non-root bridge and wireless client devices associated to the non-root bridge have roamed. You can ignore these messages.
- CSCdy13290—Nested repeaters do not work with static WEP. The problem occurs when nested access points or bridge repeaters running 11.21 firmware, as in the following topology:

Root	Repeater	Repeater
(A)	(B)	(C)

Setting a 40- or 128-bit Static WEP key, will cause repeater (C) to associate to repeater (B), but no data

is passed. Error messages (about one per packet) print on repeater (B)'s console to the effect that a device that has associated with WEP tried to pass an unencrypted packet.

If WEP is disabled, this topology functions properly. If the firmware is set to 11.10T on all units, no WEP and Static WEP also function properly.

Workaround: No workaround currently exists for firmware versions greater than 11.10T. Customers with a nested repeater topology should stay with access point and bridge firmware 11.10T.

- CSCdx22660—Hot Standby does not work with LEAP enabled. Hot standby will work when an SSID or a WEP key is activated. However when LEAP is enabled, the hot standby process starts and then fails. When the failure occurs, the access point's radio is disabled, requiring a restart to bring it back up.

Workaround: Current LEAP support for the hot standby requires the following action:

1. Configure the standby unit's user name and password.
2. Do NOT enable Require EAP for Open and Shared Authentication type.

- CSCdy58522--Access point or bridge loses portions of configuration when upgrading firmware from 11.21 to 11.23T. If an access point or bridge configuration contains host names (*ftp.cisco.com*, for example) instead of IP addresses in one or more configuration fields, the access point or bridge might lose some or all of its configuration when you upgrade the firmware from 11.21 to 11.23T. Workaround: Use IP addresses instead of host names in all configuration fields when upgrading from 11.21 to 11.23T.

Resolved Caveats

The following caveats have been resolved in firmware version 11.23T:

- Resolved: CSCdx03420—The default for the *Require use of Radio Firmware X.XX* setting on the AP/Root Radio Advanced page is *yes* instead of *no*. This setting prevents the AP radio from going down when loading firmware.
- Resolved: CSCdx03869—Non-initial fragments (that only have the IP header info, but no UDP port info) are no longer blocked by IP port filters defined on the access point.
- Resolved: CSCdx07970—defaults can now be restored on the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters pages.
- Resolved: CSCdx11703—The frequency of hot standby packets has been decreased so that they do not flood the network.
- Resolved: CSCdu13008—DNS lookup timeout no longer permanently disables DNS.
- Resolved: CSCdw13878—The standby access point no longer fails when hot standby is configured with SNMP.
- Resolved: CSCdw16742—Broadcast key rotation now works with repeater access points and non-root bridges.
- Resolved: CSCdx19068—Roaming clients are no longer permanently locked out by limited concurrent session configuration on the ACS server.
- Resolved: CSCdx19118—The access point or bridge no longer reboots when more than 23 workgroup bridges are associated to it and certain settings are changed.
- Resolved: CSCdx19270—The access point no longer reboots when the *Classify Workgroup Bridges as Network Infrastructure* setting is set to yes on an access point or bridge with more than 23 workgroup bridges associated. The root cause of this defect is the same as CSCdx19118.

- Resolved: CSCdx28889—The access point console no longer locks up with error messages when LEAP is enabled and old firmware is in use on clients.
- Resolved: CSCdx51311—The **resetall** command can now be used to reset passwords regardless of settings.
- Resolved: CSCdx54863—Manually configured Ethernet/Duplex on access point now functions immediately.
- Resolved: CSCdx55145—An incomplete login no longer prevents future Telnet logins.
- Resolved: CSCdw64129—The access point now sends an accounting request on double LEAP login.
- Resolved: CSCdx67300—DNS lookup timeout no longer permanently disables DNS.
- Resolved: CSCdw75305—CDP now uses the access point host name as the device ID.
- Resolved: CSCdx80069—The access point now buffers traffic correctly while in power saving mode.
- Resolved: CSCdx83033—The FTP option to load a configuration file to the access point is now working.
- Resolved: CSCdw81244—The access point works correctly when set via DHCP while attempting to login to it using Telnet under certain circumstances.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Select **Wireless LAN** under Top Issues.

Related Documentation

Use the following documents with this document:

- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*
- *Quick Start Guide: Cisco Aironet 350 Series Bridges*
- *Cisco Aironet 350 Series Bridge Hardware Installation Guide*
- *Cisco Aironet 350 Series Bridge Software Configuration Guide*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2002-2003, Cisco Systems, Inc.
All rights reserved.