



Cisco CallManager Multilevel Administration Troubleshooting Guide, Release 1.2(4a)

Contents

- [Introduction, page 1](#)
- [Troubleshooting Information, page 2](#)
 - [Installation and Configuration, page 2](#)
 - [Uninstalling MLA, page 5](#)
 - [Replication, page 6](#)
 - [Login, page 6](#)
 - [User Groups/Functional Groups, page 11](#)
 - [Access Privileges, page 12](#)
 - [Trace, page 12](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation, page 13](#)
- [Documentation Feedback, page 14](#)
- [Cisco Product Security Overview, page 14](#)
- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 16](#)

Introduction

This document provides troubleshooting information for Cisco CallManager Multilevel Administration Access (MLA) software.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Troubleshooting Information

The following sections provide troubleshooting information for multilevel administration access (MLA). For each error, the sections provide possible causes and corrective actions for errors, which are grouped by error type.

Installation and Configuration

Error Page cannot be displayed. Error displays upon accessing CCM Administration or Serviceability pages.

An authentication dialog asking for userid and password pops up as before installation of multilevel administration access.

Possible Cause

Internet Information Service (IIS) Admin and the World Wide Web (WWW) services stopped. The Cisco CallManager server that is accessed does not have multilevel administration access (MLA) installed.

Incorrect multilevel administration access CCMAdmin and CCMService virtual directories setup exists.

Corrective Action

Check the following conditions:

- Internet Information Service (IIS) Admin and the World Wide Web (WWW) services are running.
- Multilevel administration access is installed on the Cisco CallManager server to which you are trying to connect.

If the preceding checks are fine, verify the following conditions:

- Open Internet Information Service form by choosing **Start > Programs > Administrative Tools > Internet Services Manager**. Choose CCMAdmin and CCM Service under Default Web Services. Right-click to open the Properties window.

For CCMAdmin virtual directory, check the following conditions:

1. The Local Path should point to C:\CiscoWebs\MLA\Admin.
2. The Application Protection should be set to High[Isolated].
3. Choose the Directory Security tab. Click Edit on Anonymous access and authentication control. Click Edit on Anonymous access. Open the Anonymous User Account window.
4. Check whether the Username is set to Administrator.
5. Check whether the Allow IIS to control password check box is checked.

For CCMService virtual directory, check the following conditions:

1. The Local Path should point to C:\CiscoWebs\MLA\Service.
2. The Application Protection should be set to High[Isolated].
3. Choose the Directory Security tab. Click Edit on Anonymous access and authentication control. Click Edit on Anonymous access. Open the Anonymous User Account window.

4. Check whether the Username is set to Administrator. Make sure that the password is given correctly.
5. Check whether the Allow IIS to control password check box is unchecked.

Error Page cannot be displayed. Error displays upon accessing CCM Administration or Serviceability pages after uninstalling multilevel administration access.

Possible Cause

Internet Information Service (IIS) Admin and the World Wide Web (WWW) services stopped. CCMAAdmin and CCMService virtual directories are not set up correctly.

Corrective Action

Check the following condition:

- Internet Information Service (IIS) Admin and the World Wide Web (WWW) services are running.

If the preceding check is fine, verify the following conditions:

- Open Internet Information Service form by choosing **Start > Programs > Administrative Tools > Internet Services Manager**. Choose CCMAAdmin and CCM Service under Default Web Services. Right-click to open the Properties window.

For CCMAAdmin virtual directory, check the following conditions:

1. The Local Path should point to C:\CiscoWebs\Admin.
2. The Application Protection should be set to High[Isolated].
3. Choose the Directory Security tab. Click Edit on Anonymous access and authentication control. Click Edit on Anonymous access. Check whether the Basic Authentication check box is checked.

For CCMService virtual directory, check the following conditions:

1. The Local Path should be pointing to C:\CiscoWebs\Service.
2. The Application Protection should be set to High[Isolated].
3. Choose the Directory Security tab. Click Edit on Anonymous access and authentication control. Click Edit on Anonymous access. Check whether the Basic Authentication check box is checked.

Error Web pages are freezing periodically.

DLLHOST.exe memory consumption is growing.

Possible Cause

Internet Information Service (IIS) server may not be releasing memory.

Corrective Action

Check the following conditions:

1. Open Internet Information Service form by choosing **Start > Programs > Administrative Tools > Internet Services Manager**.

2. Under Default Web Services, choose CCMAAdmin.
3. Right-click to open the Properties window.
4. Set the Application Protection to High[Isolated].
5. Under Default Web Services, choose the CCMService.
6. Right-click to open the Properties window.
7. Set the Application Protection to High[Isolated].
8. Restart IIS.

If the preceding settings are fine, make sure MLA 1.2 Support Patch spA is installed in your system.

Error Black bar displays in the CCMAAdmin page after you log in.

Possible Cause

You installed MLA 1.2(4a) or upgraded to this version, and you logged into MLA.

Corrective Action

Perform the following steps:

1. Log out from MLA.
2. Clear the Internet Explorer (IE) cache.
3. Log in to MLA again.

Error After an upgrade to MLA 1.2(4a), the previous MLA version continues to display in the Add/Remove Programs menu.

Possible Cause

You upgraded to MLA 1.2(4a).

Corrective Action

Take no action. Display of previous MLA versions in the Add/Remove Programs menu does not affect MLA performance.

Error You cannot install MLA 1.2(4a) because an error message states that MLA is already installed, but MLA is not found in the Add/Remove Programs list.

Possible Cause

Removal of the MLA registry key did not complete.

Corrective Action

Perform the following steps to work around this problem:

1. Check whether the following registry key is present:

HKLC\Software\Cisco Systems, Inc.\Multilevel Admin

2. If the registry key is present, delete the registry key manually before you install MLA 1.2(4a).

Uninstalling MLA

Error Uninstalling MLA 1.2(4a) produces an error when a Service Release (SR) of Cisco CallManager 3.3(5) is installed.

Possible Cause

Removal of the MLA registry key did not complete.

Corrective Action

Perform the following steps to work around this problem:

1. When the message displays during the uninstall process, disregard the message and click **OK**.

The MLA 1.2(4a) uninstall process continues. When the uninstall DOS window stops displaying, the uninstall process has finished.

2. Check whether the following registry key is present:

HKLC\Software\Cisco Systems, Inc.\Multilevel Admin

3. If the registry key is present, delete the registry key manually to complete the MLA uninstall process.

Replication

Error Replication of multilevel administration access data does not happen between the publisher and a subscriber.

Possible Cause

No DBConnection entry for the subscriber in the Cisco CallManager system registry exists.

Corrective Action

Make sure that the MS SQL Server is running fine on the Cisco CallManager servers:

1. Run Regedit on the Cisco CallManager servers.
2. Go to HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\DBL.
3. Make sure a database connection entry exists for each Cisco CallManager server.

If any change exists in the entries, rerun the multilevel administration access installation.

Possible Cause

The subscriber does not have multilevel administration access installed.

Corrective Action

Unless multilevel administration access is installed on a subscriber, database replication will not be set up for that subscriber. Install multilevel administration access on the subscriber for database replication and failover.

Login

Error After installing multilevel administration access, cannot login in to the CCM Administration and CCM Serviceability pages as any user. “You do not have access to Cisco CallManager Administration” message displays.

Possible Cause

Configuring of multilevel administration access did not yet occur.

Corrective Action

Perform the following steps:

1. Log in as *CCMAdministrator* with the password that was given during the install the first time after installing multilevel administration access.
2. Configure user groups and functional groups.
3. Add users to user groups and set up access privileges to functional groups for user groups.

Refer to the “Multilevel Administration Access Configuration” chapter in the *Cisco CallManager Administration Access Guide* for details.

Possible Cause

The user does not belong to any user group.

Corrective Action

Ensure CCMAdministrator or a user who has privileges to configure user groups and assign access privileges does the following tasks:

1. Add this user to a user group.
2. Assign access privileges to functional groups for this user's user group.

Refer to the "Multilevel Administration Access Configuration" chapter in the *Cisco CallManager Administration Access Guide* for details.

Error "Administrator has not defined access privileges for you. Contact your administrator" message displays upon trying to log in.

Possible Cause

User group to which this user belongs did not get assigned any access privileges to any functional groups.

Corrective Action

Ensure CCMAdministrator or a user who has privileges to assign access privileges assigns access privileges to functional groups for this user's user group.

Refer to the "Assigning Privileges to a User Group" section of the "Multilevel Administration Access Configuration" chapter in the *Cisco CallManager Administration Access Guide* for details.

Error Cannot access Cisco CallManager Serviceability pages.

Possible Cause

The system did not get rebooted after multilevel administration access install, and the local System Administrator password has been changed.

Corrective Action

Reboot the Cisco CallManager server after multilevel administration access install for the password synchronization on change of local System Administrator password. Reboot the system.

Error Cannot log in as CCMAadministrator after changing the CCMAadministrator password on one of the Cisco CallManager servers.

Possible Cause

CCMAadministrator password changed, but was not changed in all Cisco CallManager servers where multilevel administration access is installed.

Corrective Action

The local registry stores CCMAadministrator password. So, you can connect with the new password only to the Cisco CallManager server in which you changed the password. Other Cisco CallManager servers will still have the CCMAadministrator's old password. You have to log in with the old password when you access a Cisco CallManager server in which password has not been changed.

You must make this password change in all the Cisco CallManager servers.

Error A login dialog pops up upon accessing the Real-Time Monitoring Tool.

Possible Cause

This works as designed.

Corrective Action

Enter the local System Administrator userid and password.

Error When you are trying to log in, the following message displays: "Another user is already logged in from this machine. Only one user is allowed to log in from a machine."

Possible Cause

User logged in to Cisco CallManager Administration and Cisco CallManager Serviceability from the same browser window and logged out.

Corrective Action

Because Cisco CallManager Administration and Cisco CallManager Serviceability correspond to two different sessions, logging out from one does not log the user out from another.

To work around, close the browser window. Open a new browser window to log in to Cisco CallManager Administration and Cisco CallManager Serviceability.

Error When you are trying to log in, the following message displays: “Directory Server is not accessible. At this time, only CCMAAdministrator has access.”

Possible Cause

This condition indicates that the directory server is down.

Corrective Action

Because the directory users cannot be authenticated when the Directory server is down, multilevel administration access allows only CCMAAdministrator to log in at this time because the password for this user is stored in the local registry for validation.

Make sure the Directory server is up and running.

Error Cannot log in to the CCM Administration and CCM Serviceability pages as any user after installing multilevel administration access.

Possible Cause

After you click the Logon button, nothing happens, the logon pages stays on, and a warning icon with the text “Done” displays at the bottom, left corner of the window.

Clicking this icon shows the following error:

Line: 63

Char: 13

Error: Object expected

Code: 0

URL: `http://server-name/ccmadmin/logon.asp`

Corrective Action

This problem occurs because of the caching of internet files in the system. As a workaround, delete the temporary internet files from Internet Explorer on the system where this problem occurs.

Perform the following steps:

1. Open Internet Explorer.
2. Go to **Tools > Internet Options**.
3. Inside the Temporary Internet Files option under the General tab, click the **Delete Files** button.
4. On the Delete Files dialog box that pops up, click **Ok**.
5. On the main dialog, click **Ok** to exit.
6. Refresh the login page or close and open another browser window to log in.

Error Cannot log in as CCMAAdministrator after changing the CCMAAdministrator password using Cisco CallManager’s admin utility tool.

or

Two CCMAAdministrators show up in the Cisco CallManager admin utility tool.

Possible Cause

The multilevel administration access CCMAAdministrator user differs from the user who is shown in the change password tool user interface (CCMPDWChanger.exe), and the password can only be changed by using the multilevel administration access user interface.

Corrective Action

The “Changing CCMAAdministrator Password” section in the *Cisco CallManager Multilevel Administration Access Guide* documents how the password can be changed for the CCMAAdministrator account that multilevel administration access uses, from the multilevel administration access user interface.

Error Unable to authenticate via multilevel administration access (CSCee08639).

Possible Cause

The following popups were experienced:

- Microsoft Internet Explorer “You could not be authenticated successfully. System encountered internal error.”
- Remote Scripting Error - Microsoft Internet Explorer Error Information

Corrective Action

A possible trigger (untested) could be the installation of a NetIQ client on the publisher server. Change the reference in the DBConnection0 registry key to the IP Address of the server instead of the hostname:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\DBL

DBConnection0

DSN=CiscoCallManager;SERVER=<hostname>;DATABASE=CCM030x

Change to:

DBConnection0

DSN=CiscoCallManager;SERVER=<IP Address>;DATABASE=CCM030x

User Groups/Functional Groups

Error User groups page displays the following message: “Check Directory Base in MLA Enterprise Parameter Configuration page.”

Possible Cause

Multilevel administration access uses an incorrect LDAP directory search base.

Corrective Action

Ensure CCMAdministrator or a user who has privileges to Access Rights interface does the following tasks:

1. Log on to Cisco CallManager Administration.
2. Go to **User >Access Rights > MLA Configuration Parameters**.
3. Correct the Directory Base Value and click **Update**.

Error SuperUserGroup user group cannot be deleted even by a user who has Full Access privilege.

Functional groups created by install cannot be deleted.

Possible Cause

This works as designed.

Corrective Action

SuperUserGroup user group represents standard user group (created at install time) that is Read Only and cannot be deleted. You can add or delete users from this group. Also, if you are using Active Directory, you cannot delete any user group.

The standard functional groups (created at install time) specify Read Only and cannot be deleted or updated.

Error Cannot configure user groups or functional groups. The following message displays: “Primary Database is down. No updates can be done.”

Possible Cause

This works as designed.

Corrective Action

When the publisher server is down, multilevel administration access does not allow configuration changes to the multilevel administration access database because the changes will not be effective after the publisher server comes up.

The workaround requires you to have the publisher up and running and then configure user groups or functional groups.

Access Privileges

- Error** User's access privilege is not as expected.
- Case 1: User is in two or more user groups with different permissions to a functional group. user gets the Maximum of permissions.
- Case 2: User is accessing a web page that belongs to two or more functional groups to which user's user group has different permissions. User gets the Maximum of permissions.

Possible Cause

For Case 1: Setting for effective access privileges for overlapping user groups specifies Maximum (default).

For Case 2: Setting effective access privileges for overlapping functional groups specifies Maximum (default).

Corrective Action

Check the permissions for the user by performing the following steps:

1. Go to User Groups.
2. Choose the user group to which the user belongs.
3. Click the key icon in the permission field for the user.

If you want to set the effective privileges as minimum, do the following tasks:

1. Log in as CCMAAdministrator or a user who has privileges to Access Rights.
2. Go to **User > Access Rights > MLA Configuration Parameters**.
3. Set the Effective access privileges for overlapping users groups to Minimum to grant the minimum of permissions.
4. Set the Effective access privileges for overlapping functional groups to Minimum to grant the minimum of permissions.

Trace

- Error** Multilevel administration access does not generate debug logs for troubleshooting problems.

Possible Cause

Setting for multilevel administration access debug level specifies *None*.

Corrective Action

Perform the following tasks:

1. Log in as CCMAAdministrator or a user who has privileges to Access Rights.
2. Go to **User > Access Rights > MLA Configuration Parameters**.
3. Set the Debug Level to *Debug*.

The multilevel administration access logs display in the directories C:\CiscoWebs\MLA\Debug (Trace/Debug logs) and C:\CiscoWebs\MLA\Logs (Login and Access logs and messages).

Related Documentation

The following documentation provides related information about Cisco CallManager Multilevel Administration Access:

- *Cisco CallManager Multilevel Administration Access Guide, Release 1.2(4a)*
- *Release Notes for Cisco CallManager Multilevel Administration Access, Release 1.2(4a)*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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 © 2005 Cisco Systems, Inc. All rights reserved.

