



Release Notes for the Cisco Unified Presence Server (CUPS) Release 1.0(1)

July 17, 2006

These release notes describe caveats for CUPS 1.0(1). For more specific information, please see the and the [“Open Caveats” section on page 6](#).

Contents

These release notes include the following topics:

- [Introduction, page 1](#)
- [Important Notes, page 3](#)
- [Caveats, page 3](#)
- [Troubleshooting, page 9](#)
- [Obtaining Documentation, page 9](#)
- [Documentation Feedback, page 10](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 13](#)

Introduction

The Cisco Unified Presence Server a critical component for delivering the full value of a Cisco Unified Communications environment, collects information about users' availability, such as whether they are using communications devices (for example, a phone) at a particular time. It can also collect information about individual user communications capabilities, such as whether web collaboration or video conferencing is enabled. Using this information, applications such as Cisco Unified Personal



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

© 2006 Cisco Systems, Inc. All rights reserved.

Communicator and Cisco Unified CallManager can improve productivity by helping employees connect with colleagues more efficiently through determining the most effective way for collaborative communication.

For More Information

Cisco strongly recommends that you review the following documents before you perform the installation.

- *Cisco Unified Presence Server Administration Guide*
- *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco IP Telephony Disaster Recovery System Administration Guide*
- *Cisco IP Telephony Platform Administration Guide*
- *Cisco Unified CallManager Security Guide*

Table 1 lists URLs for software and additional documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
<i>Cisco Unified CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
Cisco Unified CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
<i>Cisco Unified CallManager Security Guide</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm
Cisco Unified CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco Unified CallManager servicereleases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Important Notes

Restarting CUPS delays IPPM services

After a system restart, the IPPM service may not be available for up to 10 minutes while various components in the system are initializing.

Fresh installation on a subscriber can result in the inability to activate services on the subscriber node from the publisher node

Depending on the state of the hardware clock on the system and the time zone, it is possible the Tomcat certificate can be generated with a timestamp that is invalid (the validity of the certificate is some number of hours in the future; until this number of hours has elapsed since the subscriber installation, it is not possible to start services for this subscriber).

To activate the services,

1. Regenerate the Tomcat certificate (the only relevant ones) prior to service activation and after installation completes on the subscriber.
2. Log in to the subscriber platform GUI and select: **Security > Certificate Mgmt > Delete Regenerate Certificate**.
3. Activate services for the subscriber.

Running a large BAT job on Cisco Unified CallManager, can result in change notification not working properly.

If you run a large BAT job, stop the synchronization so that change notification works properly.
CDET:

Running a large synchronization from Cisco Unified CallManager to CUPS over AXL, may cause intermittent timeouts in the NCSCClient connection.

If you run a large synchronization over AXL, stop any provisioning on Cisco Unified CallManager.

Caveats

The following sections contain information on how to obtain the latest resolved caveat information and descriptions of open caveats of severity level 1, 2 and 3.

Caveats describe unexpected behavior on a Cisco Unified Presence server. Severity 1 caveats represent the most serious caveats, severity 2 caveats represent less serious caveats, and severity 3 caveats represent moderate caveats.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Unified Presence Server 1.0(1) by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.



Tip

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section includes the following topics:

- [Using Bug Toolkit, page 4](#)
- [Saving Bug Toolkit Queries, page 5](#)

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

-
- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
Log on with your Cisco.com user ID and password.
- Step 2** Click the **Launch Bug Toolkit** hyperlink.
- Step 3** If you are looking for information about a specific caveat, enter the ID number in the “Enter known bug ID:” field.

To view all caveats for Cisco Unified CallManager, go to the “Search for bugs in other Cisco software and hardware products” section, and enter Cisco Unified CallManager in the Product Name field. Alternatively, you can scroll through the product name list and click Cisco Unified CallManager.
- Step 4** Click **Next**. The Cisco Unified CallManager search window displays.
- Step 5** Choose the filters to query for caveats. You can choose any or all of the available options:
- a. Choose the Cisco Unified CallManager version:
 - Choose the major version for the major releases (such as, 5.0, 4.1, 4.0).
A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.
 - Choose the revision for more specific information; for example, choosing major version 5.0 and revision version 3 queries for release 5.0(2) caveats.
A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

- b. Choose the Features or Components to query; make your selection from the “Available” list and click Add to place your selection in the “Limit search to” list.
 - To query for all Cisco Unified CallManager caveats for a specified release, choose “All Features” in the left window pane.

**Note**

The default value specifies “All Features” and includes all of the items in the left window pane.

- To query only for Cisco Unified CallManager-related caveats, choose “ciscocm” and then click **Add**.
 - To query only for phone caveats, choose “ciscocm-phone” and then click **Add**.
 - To query only for gateway caveats, choose “voice-gateway” and then click **Add**.
- c. Enter keywords to search for a caveat title and description, if desired.

**Note**

To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- d. Choose the Set Advanced Options, including the following items:
 - Bug Severity level—The default specifies 1-3.
 - Bug Status Group—Check the **Fixed** check box for resolved caveats.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.
- e. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.
 - You can save your query for future use. See the [“Saving Bug Toolkit Queries” section on page 5](#).
-

**Note**

For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Perform your search for caveats, as described in the “Using Bug Toolkit” section on page 4 . |
| Step 2 | In the search result window, click the This Search Criteria button that displays at the bottom of the window. |
- A new window displays.

- Step 3** In the Name of saved search field, enter a name for the saved search.
- Step 4** Under My Bug Groups, use one of the following options to save your defects in a bug group:
- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
 - Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.

**Note**

This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

- Step 5** Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:
- Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
 - Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
 - Updates as they occur**—Bug Toolkit provides updates that are based on status change.
 - Weekly summaries**—Bug Toolkit provides weekly summary updates.
 - Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.
- Step 6** To save your changes, click **Save**.
- Step 7** A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

For complete Cisco Unified IP Phone firmware release note information, refer to the applicable firmware release notes for your specific model IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/.

Open Caveats

[Table 2](#) describes possible unexpected behaviors, which are sorted by component, in Cisco Unified Presense Server 1.0(1) and are sorted by component.

**Note**

For more information about an individual defect, click the associated Identifier in [Table 1](#) to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the “First Fixed-in Version” or “Integrated-in” fields. The information that displays in these fields identifies the list of Cisco Unified Presence interim versions in which the defect was fixed. These interim versions then get integrated into Cisco Unified Presence Server releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1.

Because defect status continually changes, be aware that [Table 2](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the [“Using Bug Toolkit” section on page 4](#).

Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 2 *Open Caveats*

Identifier	Headline
Component: AXL	
CSCse41364	Running a large synchronization from Cisco Unified CallManager to CUPS over AXL, may cause intermittent timeouts in the NCSCClient connection.
Component: BAT	
CSCse41850	Running a large BAT job on Cisco Unified CallManager, can result in change notification not working properly.
Component: Database	
CSCsd96341	CUPS does not support contacts that are not in CUPS/Cisco Unified CallManager database.
CSCse41364	Running a large synchronization from Cisco Unified CallManager to CUPS over AXL, may cause intermittent timeouts in the NCSCClient connection.
CSCse44825	After initial installation or L2 upgrade, the Cisco Unified Presence Engine can experience a core.
CSCse55238	Users who specify a non-automatic state may see "Busy" when the phone is off-hook despite their override.
CSCse62494	If a customer is not using DNS, CUPS currently auto creates CTI profiles using hostnames from the Cisco Unified CallManager cluster, which will not resolve
Component: ESP	
CSCsd78497	Large TCP message is not printed fully using StateMachine.
CSCsd78525	TCP debug does not print.
CSCsd94525	TCP debug messages do not follow servicablity formatting.
CSCse58084	System does not allow CUPS users to be spread across more multiple clusters.
Component: GUI	

Table 2 **Open Caveats**

Identifier	Headline
CSCsd94843	Provide administration interface to allow administrator to see which version of CUPC is registered.
CSCse31604	Logout broadcast only gets sent to the first node.
CSCse60410	Unable to see all available CTI gateway profiles for a user.
CSCse61524	Unable to set SMTP hostname after fresh install through the OS Administration GUI.
CSCse66336	A 404 Page Not Found is returned when attempting to access the Online Help for the System Status Administrative window.
CSCse66340	System Status window displays an MOC column.
CSCse70207	Bulk Administration: The CUPS export page is not accessible from Cisco Unified CallManager Administration GUI.
Component: Install	
CSCse77413	CUPS upgrade does not complete. The last line in the install log shows IDSWillStart...ok.
Component: IPPM	
CSCse38228	System does not allow instant messages to be sent or received when the publisher database goes down.
CSCse61278	IPPM users can login to their phones, though not provisioned in the LDAP server, and being listed as Inactive on the Cisco Unified CallManager End User page.
Component: OAM	
CSCse28257	Outbound-proxy server group does not get populated in pe_cfg.xml
Component: Security	
CSCse57662	SIP TLS does not get supported between CUPS and CUPC.
Component: Serviceability	
CSCse36656	The Disaster Recovery System fails to generate an alarm when the network disconnects during a backup.
CSCse57458	Remove extraneous SYSAPPL-MIB services from CUPS SNMP.
CSCse10902	Second node feature activation window is not available from the first node.
Component: SOAP Interface	
CSCse16839	CUPS keeps the unencrypted LDAP server login password in its database.
CSCse38370	UC cannot log in while publisher server is down.
Component: Synch-agent	
CSCse41850	Running a large BAT job on Cisco Unified CallManager, can result in change notification not working properly.
Component: VOS	
CSCsd52374	SNMP agent fails to recognize drive failure on new 7825 server with serial ATA drives.

Table 2 Open Caveats

Identifier	Headline
CSCse16130	During an L2 upgrade of the CUPS image, some syslog warning messages print to the console window.
CSCse70123	Unable to start CTI gateway after L2 upgrade from 1.0(1) to 1.0(2).

Troubleshooting

For troubleshooting information, refer to the *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)*. This document provides troubleshooting procedures for Cisco Unified CallManager systems. The *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)* provides guidance for network administrators who are responsible for managing the Cisco Unified CallManager system, for enterprise managers, and for employees. This document does not cover every possible trouble event that might occur on a Cisco Unified CallManager system but instead focuses on those events that are frequently seen by the Cisco Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

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/techsupport>

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

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

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



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- 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 “[Obtaining Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc. All rights reserved.