



Cisco Unified IP Phone 7970G and 7971G-GE Release Notes for Firmware Release 8.0(1) for Cisco Unified CallManager 5.0 (SIP)

March 6, 2006



Note

- The 8.0(1) firmware release will not be made available on Cisco.com. Cisco recommends that you use the available 8.0(2) SR1 release. See the [“Firmware Installation Notes” section on page 4](#) for more information.
 - This SIP firmware was designed and tested to interoperate with Cisco call control, most notably Cisco Unified CallManager 5.0. Although this SIP deployment is IETF RFC 3261 compliant, it is not supported by Cisco TAC or Cisco Engineering for use with non-Cisco call control systems.
-

Use these release notes with the Cisco Unified IP Phone 7970G and 7971G-GE running SIP firmware release 8.0(1) and Cisco Unified CallManager 5.0.

CISCO SYSTEMS



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

Contents

These release notes provide the following information. You might need to notify your users about some of the information provided in this document.

- [Related Documentation, page 2](#)
- [New and Changed Information, page 3](#)
- [Installation Notes, page 3](#)
- [Important Notes, page 5](#)
- [Caveats, page 7](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 13](#)
- [Cisco Product Security Overview, page 14](#)
- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 18](#)

Related Documentation

Cisco Unified IP Phone Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified CallManager version. Navigate from the following documentation URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Cisco Unified CallManager Documentation

Refer to the Cisco Unified CallManager Documentation Guide and other publications specific to your Cisco Unified CallManager version. Navigate from the following URL:

- http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

New and Changed Information

For a complete list of new and changed phone features introduced in Cisco Unified CallManager version 5.0, refer to the Release Notes for Cisco Unified CallManager 5.0. See [“Related Documentation” section on page 2](#) for help locating these documents.

DTMF Transport

Cisco Unified IP Phone firmware release 8.0(1) supports DTMF Transport. DTMF Transport transmits RTP packets in band for each a digit pressed during a call, according to RFC2833. This feature allows an SCCP endpoint to interwork with a SIP endpoint or gateway.

Installation Notes

This sections contains these topics:

- [Firmware Upgrade Issues, page 3](#)
- [Firmware Installation Notes, page 4](#)

Firmware Upgrade Issues

Note the following firmware upgrade issues:

- If you are currently running firmware earlier than 6.0(2) on a Cisco Unified IP Phone 7970G or 7971G-GE and want to upgrade to 8.0(x), you must first install an intervening 7.0(x) load to prevent upgrade failure. Cisco recommends using the most recent 7.0(3) load as the intervening load to avoid lengthy upgrade times (see item below).
- If you are currently running firmware 6.0(2) to 7.0(2) on a Cisco Unified IP Phone 7970G or 7971G-GE and want to upgrade to 8.0(x), you can do so directly. However, expect the upgrade to take twice as long as usual.

Firmware Installation Notes

Before using the Cisco Unified IP Phone models 7970G or 7971G-GE with Cisco Unified CallManager release 5.0, you must install the latest firmware on all Cisco Unified CallManager servers in the cluster.

The 8.0(1) firmware release has been made available on Cisco Unified CallManager installation CDs; however, it will not be made available on Cisco.com due to additional bugs filed during final testing. Cisco recommends that you instead use the updated 8.0(2) SR1 firmware load, which is now available on Cisco.com. This recommendation is limited to this specific firmware release and has no bearing on any other software or firmware available on Cisco Unified CallManager CDs.

The SIP 8.0(2) SR1 installation program for the 7970G and 7971G-GE for Cisco Unified CallManager 5.0 is named:

cmterm-7970_7971-sip.8-0-2SR1.cop

The readme file that contains installation instructions is named:

cmterm-7970_7971-sip.8-0-2SR1-readme.htm

Both of these 8.0(2) SR1 files can be downloaded from this location on Cisco.com:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser>



Note

- If you are upgrading from an earlier firmware version, see the “[Firmware Upgrade Issues](#)” section on page 3 before upgrading.
- Cisco recommends installing 8.0(2) SR1 instead of 8.0(1), as explained earlier in this section.

Important Notes

This section contains these topics:

- [Failover Time Using TCP is Faster than Failover Time with UDP, page 5](#)
- [Cisco Unified CallManager Load Server Setting for Firmware Upgrades, page 5](#)
- [Secure PC Logoff in an 802.1X Network, page 7](#)

Failover Time Using TCP is Faster than Failover Time with UDP

You can configure SIP profiles for the Cisco Unified IP Phone 7970G or 7971G-GE to operate with TCP or UDP by using the SIP Phone Security Profile Configuration window in Cisco Unified CallManager Administration. If TCP is selected as a transport protocol, the failover time between primary, secondary and tertiary Cisco Unified CallManagers is approximately 5 seconds or less. If you select UDP, the failover time is approximately 120 seconds. The failover time is the maximum time that the phone waits before it can detect Cisco Unified CallManager failure status. The difference in the failover times is due to the behavior of TCP and UDP and not a bug on the Cisco Unified IP Phones or Cisco Unified CallManager.

Cisco Unified CallManager Load Server Setting for Firmware Upgrades

Cisco Unified CallManager Administration contains a setting to optimize installation time for phone firmware upgrades.



Note

The setting is intended for future use, and is not yet a supported feature.

The Load Server setting is visible on the Phone Configuration page (Product Specific Configuration section) in the Cisco Unified CallManager Administration application. This setting lets you specify an external TFTP server IP address or

name (other than the TFTP Server 1 or TFTP Server 2) from which the phone firmware can be retrieved for upgrades on the phones. When the Load Server is set, the phone contacts the designated server for the firmware upgrade.



Note

- If the firmware load is not found on the Load Server, the phone does not upgrade and is not redirected to the TFTP Server 1 or TFTP Server 2.
 - On a factory reset or during a software recovery operation, the phone may fall back to using TFTP Server 1 or TFTP Server 2 to recover the phone load. In these scenarios, the phone will recover the phone load either via the term70.default.loads or term71.default.loads file, or it will attempt to recover the phone load based on its load.hist file.
 - If the phone is auto-registering with Cisco Unified CallManager for the first time, the phone will request the phone load via TFTP Server 1 or TFTP Server 2. This will only occur once when the phone is first installed into the system. This can be mitigated by preloading the phones with the correct firmware so that no firmware upgrade is required in combination with the auto-registration, or by auto-registering the phones at the main site prior to deployment at a remote site.
-

You can view the Load Server setting on the phone from **Settings > Device Configuration > Network Configuration > Load Server**. If the value in the Load Server setting is invalid, a “Load Server is invalid” message is displayed on the phone in **Settings > Status > Status Messages**.

Secure PC Logoff in an 802.1X Network

Firmware release 8.0(1) provides support for the Cisco Unified IP Phone 7970G and 7971G-GE to monitor IEEE 802.1X messages between an authenticating switch and a connected PC (supplicant).

When a PC is disconnected from the Cisco IP Phone, the phone issues an EAPOL-Logoff message on behalf of the PC to the authenticating switch. The proxy EAPOL-Logoff message causes the authenticating switch to set the port to an unauthenticated state.

If you have an 802.1X network and upgrade to Cisco Unified IP Phone firmware release 7.0(2) or greater, be aware that you must re-authenticate a PC that is connected to the Cisco Unified IP Phone 7970G and 7071G-GE.

For more information about 802.1X re-authentication, refer to the Cisco Catalyst switch configuration guides at:

http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html

Caveats

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

-
- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
 - Step 2** Log on with your Cisco.com user ID and password.
 - Step 3** Click the **Launch Bug Toolkit** hyperlink.
 - Step 4** To look for information about a specific problem, enter the bug ID number in the “Enter known bug ID” field and click **Search**.
-

Open Caveats

[Table 1](#) lists Severity 1, 2, and 3 defects that are open for the Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(1).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that [Table 1](#) 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 as described in the “[Caveats](#)” section on page 7.

Table 1 *Open Caveats for the Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(1)*

Identifier	Headline and Bug Toolkit Link
CSCsb11707	PLAR causes a short dialtone prior to an INVITE message being sent. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb11707
CSCsb17473	Call instance number is skipped when speed dial is used. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb17473

Table 1 *Open Caveats for the Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(1) (Continued)*

Identifier	Headline and Bug Toolkit Link
CSCsb77075	Corporate directory search fails when using Russian locale. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb77075
CSCsb78781	The phone issues a BYE message instead of a 488 message if it does not accept a reInvite with SDP body. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb78781
CSCsb99327	The Cisco Unified IP Phone 7970G does not obey the Retain Forward Information service parameter. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb99327
CSCsc06398	The phone uses HTTP cookies received from Cisco Unified CallManager while communicating with another server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc06398
CSCsc13134	Phone downloads image multiple times during a reboot. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc13134
CSCsc46668	SIP phones display “from anonymous” instead of “private” from restricted calls. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc46668
CSCsc47974	The phone might hang when pressing keys during an observed held call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc47974
CSCsc50496	SIP phones are slow to respond to invite messages. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc50496
CSCsc71763	The SSHD process hangs after connections are abnormally terminated. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc71763
CSCsc79774	The phone cannot recover after a DNS entry has been corrected. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc79774
CSCsc83609	The phone does not cut the dial tone when the first digit is entered. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc83609
CSCsc86483	Conference tones are only heard by the conference controller. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc86483

Table 1 Open Caveats for the Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(1) (Continued)

Identifier	Headline and Bug Toolkit Link
CSCsc96389	SIP phones do not check errors in the MWI Notify message. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc96389
CSCsc96462	Files created by SIP runtime are not cleared on factory reset. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc96462
CSCsc96491	The phone accepts an MWI Notify message even if the message is not destined to it. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc96491
CSCsc98937	SIP phones accept duplicate IP addresses. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc98937
CSCsc99065	SIP might incorrectly detect the SDP has changed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc99065
CSCsc99166	SIP phones experience initial voice clipping. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc99166
CSCsd01353	The phone displays “reorder” in english when the phone is set to Japanese locale. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd01353
CSCsd02600	You can change ring volume even when the setting access is set to disabled. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd02600
CSCsd02671	CTI MONITORDIGITS event not returned when ABCD DTMF digits are received. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd02671
CSCsd04208	When a shared line is used with a restricted number, the SIP phone will still display the party number. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd04208
CSCsd04464	Non-secure phones are allowed to barge into an encrypted call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd04464
CSCsd04595	Pressing the Resume key on a held shared line after cBarge does not resume the call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd04595

Table 1 Open Caveats for the Cisco Unified IP Phone 7970G and 7971G-GE for Firmware Release 8.0(1) (Continued)

Identifier	Headline and Bug Toolkit Link
CSCsd05406	Phone completes attended call transfer feature when the New Call softkey is selected. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd05406
CSCsd05954	Call preservation does not work during a Cisco Unified CallManager upgrade. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd05954
CSCsd06032	Interdigit timeout is not reset after each digit is selected. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd06032
CSCsd06345	SIP phones register to tertiary when primary Cisco Unified CallManager is restarted. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd06345
CSCsd07675	The Cisco IP Phones 7970G/7971G-GE cannot make outgoing calls after failover or failback testing. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd07675
CSCsd09000	Phone might be out of memory if “Key not active” is displayed after a digit key press. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09000
CSCsd09042	The phone cannot boot up when auto registration is turned off in Cisco Unified CallManager. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09042
CSCsd09430	The phone will continue to respin when the DHCP response has no TFTP entry. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd09430
CSCsd10484	The transferee phone continues to hear ringback tone after early attended transfer is abandoned. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd10484

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>

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)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.