Cisco IP Phone 7970G and 7971G-GE Release Notes for Firmware Release 7.0(2) for Cisco CallManager Versions 3.3, 4.0 and 4.1

October 6, 2005

These release notes are for use with the Cisco IP Phone 7970G and Cisco IP Phone 7971G-GE for firmware version 7.0(2) running on Cisco CallManager 3.3.3 SR2 or later.

These release notes provide the following information:

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

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

Documentation Roadmap

For detailed information about administering or using the Cisco IP Phone 7970G and the Cisco IP Phone 7971G-GE, refer to the following documentation references.

Cisco IP Phone 7970G/7971G-GE

- *Cisco IP Phone 7970 Series Administration Guide for Cisco CallManager, Models 7970G and 7971G-GE*
- *Cisco IP Phone 7970 Guide 7970G/7971G-GE*
- *Regulatory Compliance and Safety Information for the Cisco IP Phone 7900 Series*
- *Cisco IP Phone 7970G and 7971G-GE Release Notes for Firmware Release 7.0(1) for Cisco CallManager Versions 3.3, 4.0 and 4.1*

These documents are available from the following location on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7970/index.htm

Cisco CallManager Administration

- *Cisco CallManager Administration Guide*
- *Cisco CallManager System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Bulk Administration Tool User Guide for Cisco CallManager*
- *Cisco CallManager Features and Services Guide*

These documents are available from the following location on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/index.htm

Upgrade Issue for 6.0(x) to 7.0(x)

When upgrading from a 6.0(x) load to a 7.0 load, the following settings are lost:

- Brightness
- Viewing angle
- Volume (all volume settings)
- Call history
- Background image

Installation Notes

This section contains firmware information and installation instructions.

Firmware Information

The Cisco IP Phone 7970G and 7971G-GE firmware installation program is named cmterm-7970_7971-sccp.7-0-2.exe. The readme file that contains installation instructions is named cmterm-7970_7971-sccp.7-0-2-readme.htm.

Both files can be downloaded from this location on Cisco.com:

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

Supported CallManager Versions

This firmware release, 7.0(2), is compatible with the following releases of Cisco CallManager—shown for each phone model:

- Cisco IP Phone 7970G
  - Cisco CallManager 3.3(4) or later release
  - Cisco CallManager 4.0(2a) or later release
  - Cisco CallManager 4.1(2) or later release
- Cisco IP Phone 7971G-GE
  - Cisco CallManager 3.3(5) or later release
  - Cisco CallManager 4.0(2a) SR2a or later release
  - Cisco CallManager 4.1(2) SR1 or later release

This firmware release provides support for new telephony features provided by Cisco CallManager 4.1. For a full description of the new phone features introduced in Cisco CallManager 4.1, refer to the *Release Notes for Cisco CallManager Release 4.1(x)*:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/rel_note/index.htm

Cisco CallManager Device Packs

You should install the following device packs for these Cisco CallManager versions. You can download the device packs from this location on Cisco.com:

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

The device pack readme files provide installation information.

Cisco CallManager Version	Device Pack
3.3(5), SR1	ciscocm.3-3-DevPack-63.2.exe, or later
4.0(2), SR2b	ciscocm.4-0-DevPack-42.2.exe, or later
4.1(3), SR1	ciscocm.4-1-DevPack-22.3.exe, or later

Cisco IP Phone Expansion Module 7914

The Cisco IP Phone Expansion Module 7914 is supported on the Cisco IP Phone 7970G and Cisco IP Phone 7971G-GE.

If you are using the Cisco IP Phone Expansion Module 7914, you must upgrade the Expansion Module to firmware release S00104000100. You can download the installation program, which is named cmterm-7914-sccp.4-0-1.exe, and the readme file from Cisco.com at this location:

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

Important Notes

Review these important notes for this firmware release.

Cisco CallManager Load Server Setting for Firmware Upgrades

A new setting that optimizes installation time for phone firmware upgrades is available in Cisco CallManager Administration.

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

To view the load server setting, you must install the latest Cisco CallManager Device Pack (see the "Cisco CallManager Device Packs" section on page 4).

The new Load Server setting is visible on the Phone Configuration page (Product Specific Configuration section) in the Cisco 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 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**.

Securing the Phone with a Cable Lock

You can secure the Cisco IP Phone 7961G and 7941G to a desktop using a laptop cable lock. The lock connects to the security slot on the back of the phone and the cable can be secured to a desktop.

The security slot can accommodate a lock up to 20 mm. Compatible laptop cable locks include the Kensington® laptop cable lock and laptop cable locks from other manufacturers that can fit into the security slot on the back of the phone.

Power Supply Information

Cisco IP Phone 7970G/7971G-GE documentation contains references to CP-PWR-CUBE-2.

The Cisco IP Phone 7970G now supports both CP-PWR-CUBE-3 and CP-PWR-CUBE-2. Therefore, all references to CP-PWR-CUBE-2 in the Cisco IP Phone 7970G documentation also apply to CP-PWR-CUBE-3.

Cisco IP Phone 7971G-GE supports only CP-PWR-CUBE-3, so all references to CP-PWR-CUBE-2 in the Cisco IP Phone 7971G-GE documentation apply only to CP-PWR-CUBE-3.

Multiple-Reset Warning

If you reset the Cisco IP Phone as many as three times in five minutes, all locally stored phone settings—including data about placed and received calls—will be lost. (See CSCsb26814 in the "Open Caveats" section on page 12.)

Secure PC Logoff in an 802.1X Network

Firmware release 7.0(2) provides support for the Cisco IP Phone 7970G/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 PC port on the phone to an unauthenticated state and immediately terminates the 802.1x secure session.

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

Resolved Problems

Table 1 lists the severity 1, 2, and 3 problems that have been resolved since the 7.0(1) release.

Table 1 Cisco IP Phone 7970G/7971G-GE Resolved Problems

Bug ID	Summary
CSCec41908	Access Network Config. menu during boot up
CSCed93627	Phone cannot be reset to its factory defaults.
CSCee18228	Full-duplex performance of the phone should be the same as that of the Cisco IP Phone 7960.
CSCeg05241	CNU memory leak occurs on starting/killing applications.
CSCeg48102	CAPF connection closes during Cisco CallManager failover.
CSCsa65885	The amount of time needed to upgrade phone firmware should be reduced.
CSCsa69207	Phone does not display a “DNS unknown host” status message.
CSCsa76694	The timestamp in console messages and on the phone display is not the same.
CSCsa96530	Phone does not hard reset after image upgrade, it just registers.
CSCsb03511	Incoming call cancels an in-progress predial.
CSCsb05127	The latest display appears again, momentarily, when the user presses a different menu button.
CSCsb05445	Phone resets when a high volume of calls are placed on an attached Cisco IP Phone Expansion Module 7914.
CSCsb08266	Phone stuck at Cisco logo; constantly rebooting.
CSCsb08632	Phone accepts invalid TFTP and DNS addresses.
CSCsb09530	Focus immediately shifts to a second call arriving on the same line.
CSCsb10140	Phone continuously resets.
CSCsb10261	Inconsistency occurs in the start time and report time in the Streaming Statistics page.
CSCsb10819	Phone caches invalid port number and uses it when pushing RTPRx.
CSCsb11543	Empty XML push hangs HTTP Server on phone.
CSCsb12499	Some parameters on the Streaming Statistics page do not get updated.
CSCsb13518	Phone gets stuck when a power cycle is performed.

Table 1 Cisco IP Phone 7970G/7971G-GE Resolved Problems (Continued)

Bug ID	Summary
CSCsb14899	Phone displays Missed Call message while new call is coming in.
CSCsb15000	placedCall log does not include DisplayID with translation pattern.
CSCsb15908	Possibility of vieo CastMiscellaneousCommandMessage getting corrupted.
CSCsb15939	Possible data corruption occurs in vieo StationUpdateCapabilitiesMessage.
CSCsb15947	Possible data corruption occurs in vieo miscVideoCommand message.
CSCsb15963	Possible data corruption occurs in vieo CallInfoMessage.
CSCsb15996	Forwarded call does not show original calling name.
CSCsb16611	Intermittent: phone line lights not lighting up.
CSCsb17232	Phone gets stuck when reset from Cisco CallManager.
CSCsb17239	Phone has registered lockout with incoming packets dropped.
CSCsb17277	Call-related user interface is very sluggish with CVTA.
CSCsb17280	Phone with two sidecars crashes when multiple sidecar buttons are pressed.
CSCsb17491	Autodial entries are getting duplicated for the same dial number.
CSCsb18955	Continuously accessing the Help Page makes the UI disappear, and only the phone softkeys display.
CSCsb18969	Phone does not dial a call from the Placed Call list when the phone already has a call.
CSCsb19187	Some phone models allow Key:X URIs for keys not on the phone.
CSCsb19310	Calls between phone and CTI port dropped after 15 seconds.
CSCsb19755	Recovery.tab is missing from 7.0 loads.
CSCsb19755	Recovery.tab missing from 7.0 loads.
CSCsb19871	Phone should not try to register when IP address is released.
CSCsb20310	tcpIF.c: sendTcpMiscCommand() garbling Misc cmd.
CSCsb20391	Phone unable to Rx or Tx Multicast Services when the Publisher fails.
CSCsb20545	Pressing **NewCall** and dialing ****#** unlocks the settings.
CSCsb22202	Message Factory does not handle FlowControlNotifyMessage.
CSCsb22206	Expansion Module Stats are available on phone models that do not support expansion modules.

Table 1 Cisco IP Phone 7970G/7971G-GE Resolved Problems (Continued)

Bug ID	Summary
CSCsb22507	TX Unicast is missing from the Ethernet Information web page.
CSCsb23040	A restart causes a “Error Verifying Config Info” message to appear in the Status Message Log.
CSCsb25148	79X1/7970 Admin VLAN ID inconsistent.
CSCsb25895	Phone boots up with wrong viewing angle setting.
CSCsb26733	The Cancel softkey, displayed after an XML error message timeout, does not work.
CSCsb27750	RTPTx URI allows specification of port 0.
CSCsb27759	Phone lights fail on incoming call.
CSCsb29691	Incorrect Services URL error display not correct.
CSCsb30546	DHCP Disable is not accepting valid addresses.
CSCsb30698	Cisco Extension Mobility is not working.
CSCsb32501	Phone disconnects call to CUE after 35 seconds.
CSCsb32965	UI locked after user pressed Directory button.
CSCsb33818	Phone never comes up if the DHCP lease duration is unlimited.
CSCsb34559	RTP packets not received at destination for RTP URIs
CSCsb36265	ICMP Unreachable—Ignoring errors from a router.
CSCsb39247	Phone unregisters and stays unregistered—BlockingQueue DevRecoveryTask.
CSCsb43537	The Cisco IP Phone 7961 downloaded the configuration file twice when restarted from Cisco CallManager.
CSCsb44304	Race condition occurs on closure of multi-threaded sockets.
CSCsb44674	Memory leak occurs in PropertiesJNI.c.
CSCsb45619	Phone does not register to Cisco CallManager after a reset.
CSCsb46516	Reset-Restart to the phone every five seconds causes kernel crash.
CSCsb46548	Property Listener leak occurs in SccpConfig.
CSCsb47854	7970: Power neg advertises 10250 10250 after negotiation is complete
CSCsb50077	Phone does not perform TFTP and gets stuck after erase or reset.
CSCsb52192	Noise toggling/pumping noticeable at high volumes.

Table 1 Cisco IP Phone 7970G/7971G-GE Resolved Problems (Continued)

Bug ID	Summary
CSCsb54991	Cisco IP Phone 7970 touch screen: IP Phone URL shows Delay.
CSCsb55440	Phone not able to re-register after losing Cisco CallManager connection.
CSCsb59731	The Cisco IP Phone 7941/61 gets stuck in Registration loop.
CSCsb61721	Phone cannot register with Cisco CallManager after a reset.
CSCsb62087	The Cisco IP Phone 7970/7971 gets stuck in a reboot loop.
CSCsb66487	CTL file being requested from an unauthorized TFTP server.
CSCsb67660	File system formats on reset from Cisco CallManager.
CSCsb70867	VM gets stuck at "Verifying Load" while waiting for initial load response.
CSCsb71049	7971: Phone stuck in "Updating Locale" state
CSCsb71049	Phone stuck in Updating Locale state.
CSCsb71190	Using alt TFTP to connect to new secure or unsecure Cisco CallManager causes the phone to connect briefly, then un-register from Cisco CallManager.
CSCsb71317	disp will cause disp.xx.core to be generated.
CSCsb71409	Phone locks up with only off hook working.
CSCsb72254	Corporate directory search fails if username contains special characters
CSCsb72254	Corporate Directory search fails when using German (DAN) Locale.
CSCsb73851	Files getting corrupted and causing kernel to BugTrap.
CSCsb74797	The Cisco IP Phone 7970 will not respin the IP Stack when it detects voice VLAN changes by switch.
CSCsb77075	Corporate Directory Search Fails When using Russian Locale
CSCsb77225	CNU: Fix race condition in getportcfg()/getdhcpinfo().
CSCsb82560	Filesystem thrashing malloc.
CSCsb86341	BUGTRAP: Multi-threaded access of syslog files corrupts CNU kernel heap
CSCsb86382	bugtrap on cdp process, flashReleaseBlock() called by fileTrunc().
CSCsb87704	syslogd not writing log files in order
CSCsb88108	Java phone app gets wrong value from CDP and phone fails to come up
CSCsb88186	7970 won't failback to a TFTP server once registered to an SRST router

Table 1 Cisco IP Phone 7970G/7971G-GE Resolved Problems (Continued)

Bug ID	Summary
CSCsb89297	Kernel freezes on flashSync() when init exits
CSCsb92344	IP Phone doesn't mark SCCP packets with correct DSCP marking
CSCsb95435	File truncate problems

Open Caveats

Open caveats (bugs) are graded according to severity level. These release notes contain descriptions of bugs with severity level 1, 2, or 3. In some cases, bugs with lesser severity levels are also included, depending on the issue.

Tip If you have an account with Cisco.com (Cisco Connection Online), you can use the Bug Toolkit to find caveats of any severity for any release. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.

Table 2 describes the caveats that are known to exist in this release.

Table 2 Open Caveats

Identifier	Summary
CSCeg40271	Received and missed calls show wrong calling party number. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg40271
CSCsb14397	Phone indicates "CM Fallback Service Operating" when it is registered to a Cisco Call Manager. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb14397
CSCsb16212	The Cisco IP Phone 7971G-GE can only get full brightness intermittently. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb16212
CSCsb26814	Phone Extra reboot wipes call history http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb26814

Table 2 Open Caveats (Continued)

Identifier	Summary
CSCsb27783	"Your current options" is lost from the phone display when a Cisco CallManager failover occurs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb27783
CSCsb32965	UI locked after pressing Directory button http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb32965
CSCsb45684	Phone stops playing multicast after an unanswered call http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb45684
CSCsb56569	Cisco IP Phone Doctor enables logging automatically. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb56569
CSCsb58897	Phone display goes blank for consult transfer to busy monitor line http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb58897
CSCsb59801	Need to press mute twice for an incoming intercom call http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb59801
CSCsb62226	SoftKeys intermittently do not gray out. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb62226
CSCsb66203	Phone detects file system problem and loses configuration settings after file formatting. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb66203
CSCsb74796	Phone freeze after reset stress http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb74796
CSCsb83788	Exit soft key is not working in Callback Screen http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb83788
CSCsb85391	HTTP CGI ModeInfo query does not return if Services URL does not resolve. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb85391
CSCsb89882	Phone drops IPX rip response during IPX logon http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb89882

Table 2 Open Caveats (Continued)

Identifier	Summary
CSCsb91567	UI : Phone Unable to Update the Service Pane with XML Service http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb91567
CSCsb95198	Phone does not preserve the state of mute/spkr button in handset mode http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb95198
CSCsc03492	CDP crashs from broadcasted CDP pkt, results in restart of all apps http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc03492
CSCsc04301	Add fault-tolerance to filesystem http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc04301
CSCsc05743	Phone responds to CDP triggers from upstream port http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc05743

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

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco 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

  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.

- 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 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 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.

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)—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, 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 "Documentation Roadmap" 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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, TeleRouter, 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. (0502R)

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