



Release Notes for Cisco VG224 Voice Gateway

Contents

These release notes describe new features of Cisco VG224 voice gateway and include the following sections:

- [New and Changed Information, page 1](#)
- [Caveats, page 1](#)
- [Port Numbering, page 8](#)
- [ROM Monitor Commands, page 9](#)
- [Known Problems, page 10](#)
- [Documentation Feedback, page 11](#)

New and Changed Information

New Hardware Features

No new hardware features.

New Software Features

No new software features.

Caveats

For general information on caveats and the bug toolkit, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

This section contains the following caveat information:



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Open Caveats - Release 12.4\(11\)XW7, page 2](#)
- [Resolved Caveats - Release 12.4\(11\)XW7, page 2](#)

Open Caveats - Release 12.4(11)XW7

No open caveats.

Resolved Caveats - Release 12.4(11)XW7

CSCsi17020- Router may reload after NATing fragmented skinny packets

Symptom A router that is running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:---- Partial decode of process block ----Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540

Conditions This symptom is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets are not larger than 800 bytes.

CSCsi55685- kron removes recurring tclsh cli after first run

Symptom The following recurring kron schedule fails and gets removed after the first run. kron occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh disk0:hello.tcl!

Conditions enter the following configuration commands: kron occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh unix:hello.tcl ! create a file on disk0: called hello.tcl with the following contents: puts "hello"

Workaround None

CSCsk25697- unprotected buginf may cause cpuhog under repeated udp traffic to 53

Symptom A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53. Sample for 3800 router: [%SYS-3-CPUHOG](#): Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input. -Traceback=0x60D68CDC

0x6033D984 0x6180E58C FFFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFFF8 FFFFFFFA5
 FFFFFFFA3 FFFFFFF92 FFFFFFFA7 FFFFFFF8B 7A 3A FFFFFFF5 17 FFFFFFF9B FFFFFFFC9 FFFFFFF9B
 FFFFFFFA2

Conditions Router needs to have dns server configured and listen to udp port 53 conf t ip dns server end

Workaround Apply rate limit to port 53 to interfaces facing untrusted networks: access-list 100 permit udp any any eq domain access-list 100 deny ip any any interface GigabitEthernet0/0 ip address 10.2.2.2 255.255.255.0 rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action drop.

CSCs148237- incorrect bounding length in strncpy() calls in l2tp files

Symptom If a large name string is used when configuring the command "security crypto-profile" under the l2tp-class submode, we could have a buffer overflow which may crash the router.

Conditions This problem only occurs if a large name string is used in the "security crypto-profile" command.

Workaround There is no workaround.

CSCs159294- %DATACORRUPTION-1-DATAINCONSISTENCY at caplog_logger_proc

Symptom A Cisco router may see the following error once shortly after bootup: *Nov 21 15:16:28 CDT: [%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error, -PC= 0x416DE178 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178 0x416DE650 0x423E303C 0x423E3020 *Nov 21 15:16:28 CDT: [%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error, -PC= 0x416DE188 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650 0x423E303C 0x423E3020 No functional impact is seen.

Conditions Occurs on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround Disable the following configuration on the router: **voice hpi capture buffersize voice hpi capture destination filename**

CSCek41543- Cisco2811 Processor Pool Memory Leak in ISDN and Crash

Symptom A Cisco 2811 router running Cisco IOS Release 12.4(7a) may have a memory leak in the ISDN process as has been seen in the **show process memory**. The leak rate appears to be about 1.20MB/Hour.

Conditions This symptom has been observed with BRI-U interface that is UP/UP (spoofing).

Workaround Administratively shut down the BRI interface.

CSCsi17020- Router may reload after NATing fragmented skinny packets

Symptom A router that is running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:---- Partial decode of process block ---Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540

Conditions This symptom is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets are not larger than 800 bytes.

CSCsi21389- One-way multicast traffic over wireless.

Symptom Routers that have the ability to use the optional 802.11b/g card, such as the Cisco ISR series do not pass multicast traffic across the wireless interface.

Conditions Cisco routers that have the 802.11 b/g HWIC card do not pass multicast traffic across the wireless interface, though multicast routing is enabled and otherwise is configured normally. Wireless hosts cannot pass multicast traffic between each other, and multicast traffic from the wired network will not be transmitted out the wireless interface.

Workaround None

CSCsi44510- CME multicast audio to the 7921 cuts out on HWIC-AP

Symptom Multicast audio to the 7921 cuts out after a few seconds and will not resume.

Conditions A 7921 registered to CME doing multicast paging or multicast MOH

Workaround none

CSCsj14277- Wrong Calling ID by transfer, only with 7931 - 12.4(4)XC6

Symptom The caller id on the transfer-to is not updated with the transferee after the transferor commits the transfer.

Conditions When the transfer-to answers the call from the transferor, the caller id on the transfer-to shows that the call is from transferor. After the transferor commits the the transfer, the caller id should be updated with the transferee. This caller id display issue can be observed if the transferor DN is shared by the transfer-to.

Workaround There is no workaround without removing the XOR DN from the XTO.

CSCsj34770- Having problem in establishing QSIG Prime call

Symptom QSIG PRIME call is not going between slave and master routers

Conditions This issue is seen in 12.4(16.5)T

Workaround No workaround

CSCsj50982- Wrong isdn cause code while making call to wrong destination

Symptom Wrong isdn cause code comming while making call to wrong destination

Conditions While call made to wrong destination number

Workaround none

CSCsk25697- unprotected buginf may cause cpuhog under repeated udp traffic to 53

Symptom A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53. Sample for 3800 router: [%SYS-3-CPUHOG](#): Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input. -Traceback= 0x60D68CDC 0x6033D984 0x6180E58C FFFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFFF8 FFFFFFFA5 FFFFFFFA3 FFFFFFF92 FFFFFFFA7 FFFFFFF8B 7A 3A FFFFFFFF5 17 FFFFFFF9B FFFFFFFC9 FFFFFFF9B FFFFFFFA2.

Conditions Router needs to have dns server configured and listen to udp port 53 conf t ip dns server end.

Workaround Apply rate limit to port 53 to interfaces facing untrusted networks: access-list 100 permit udp any any eq domain access-list 100 deny ip any any interface GigabitEthernet0/0 ip address 10.2.2.2 255.255.255.0 rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action drop.

CSCsk71610- CCSIP_UDP_SOCKET causes high CPU Usage

Symptom Incoming and outgoing calls fail due to high CPU Usage.

Conditions CPU Usage is at 99-100% and CCSIP_UDP_SOCKET is using 88+%.

Workaround There is no workaround.

CSCsl18024- HWIC Country Code Issue

Symptom Error message [%DOT11-3-POWERS_INVALID](#): Interface Dot11Radio0/3/0, no valid power levels available is displayed during boot up.

Conditions Occurs for certain HWIC-AP cards with wrong country code values

Workaround Work around is to use HWIC AP cards of correct country code values.

CSCsl59294- %DATACORRUPTION-1-DATAINCONSISTENCY at caplog_logger_proc

Symptom A Cisco router may see the following error once shortly after bootup: *Nov 21 15:16:28 CDT: [%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error, -PC= 0x416DE178 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178 0x416DE650 0x423E303C 0x423E3020 *Nov 21 15:16:28 CDT: [%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error, -PC= 0x416DE188 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650 0x423E303C 0x423E3020 No functional impact is seen.

Conditions Occurs on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround Disable the following configuration on the router: voice hpi capture buffersize voice hpi capture destination *filename*.

CSCsm04209- PVDm2-DM fails to initiate calls over EuroISDN BRI while TEI is inactive.

Symptom Modem calls fail to establish when 'isdn tei-negotiation firstcall' configured on ISDN interfaces.

Conditions The ISDN BRI interfaces are added to CSM signaling interface queue only when they are active (layer 2, MULTI-FRAME-ESTABLISHED). Since, the ISDN L2 is not activated until the first call is initiated which in turn means there is no signaling interface available, which results in call failure.

Workaround Add the ISDN BRI interfaces to CSM signaling interface if they are not administratively down (shutdown).

CSCsm45689- UC520 crashed when system test was executed with debug logs enabled.

Symptom UC520 crashed when system test was executed with debug logs enabled.

Conditions UC520 crashed when system test was executed with the below debug logs enabled. debug callmon core debug callmon info debug callmon detail debug ccsip message.

Workaround None.

CSCsm46227- Router crash with CPUHOG for trunk port monitoring.

Symptom Cisco 3845 may crash when there is an incoming trunk call.

Conditions Occurs if the shared trunk DN is monitored by a FXO port and it is call-forwarded to another trunk DN with "call-forward all".

Workaround None.

CSCsm49011- VG224 SCCP port plays reorder before CM routes call-IOS interdigit timer.

Symptom On an FXS port configured for SCCP usage (such as on a VG224), reorder is heard 10 seconds after the last digit dialed when a number is dialed that requires waiting for interdigit timeout on CallManager.

Conditions Using SCCP controlled FXS port on an IOS box. Dialing a number which requires waiting for interdigit timeout to route (such as a variable length international number).

Workaround Increase the interdigit timeout setting on each SCCP FXS port to 16 secs (to be greater than CallManager's 15 secs). This is done by configuring "timeouts interdigit 16" under each voice port. OR decrease the CallManager interdigit timeout to 9 seconds (to be less than the VG224 port's 10 secs). This is done by changing the CallManager service parameter T302 Timer value to 9000 msec (9 seconds). If this workaround is chosen the new interdigit timeout setting will apply to all devices attached to the CallManager, not just the IOS SCCP FXS ports.

CSCsm55045- Crash illegal deallocation of unassigned/in-use memory.

Symptom A Cisco router configured with Call Manager Express (CME) may reload due to point to illegal deallocation of unassigned/in-use memory.

Conditions Occurs when CME is enabled.

Workaround There is no workaround.

CSCsm50874- CME: calling name in facility IE doesn't display on IP phone.

Symptom CME 4.2 does not display calling name when sent in an ISDN facility IE message. The facility is received and interpreted correctly however it doesn't show up on the IP phone display.

Workaround IOS 12.4(11)XW3 and 12.4(15)XY correct display the calling name.

CSCsm65685- Need to enable vendorConfig parameters on 7912.

Symptom After the configuraiton of telephony-service service phone settingsAccess 2 <settingsAccess>2</settingsAccess>" is missing in system:/its/XMLDefault7921.cnf.xml.

Workaround None.

CSCsm92260- CSKU wrong country code issue.

Symptom Error message Feb 28 08:50:28.459: [%DOT11-3-POWERS_INVALID](#): Interface Dot11Radio0/0/0, no valid power levels available seen on router console during router boot up.

Conditions Occurs for cerain CSKU cards with wrong country code values.

Workaround Work around is to use CSKU cards of correct country code values.

CSCso33776- spurious access error in AFW_M_Destination_Initiate.

Symptom Spurious memory access messages may be generated by a router. Mar 28 02:45:02.016: [%ALIGN-3-SPURIOUS](#): Spurious memory access made at 0x41DCE7E0 reading 0x60 Mar 28 02:45:02.016: [%ALIGN-3-TRACE](#): -Traceback= 0x41DCE7E0 0x41DCF674 0x41DD351C 0x41DD6BBC 0x41DA96CC 0x41E0E428 0x41E0F2C4 0x41DF36D4. This issue may be cosmetic in nature.

Conditions These spurious memory accesses may be triggered by a T1/E1 PRI call or other event.

Workaround There is no known workaround. This issue may be cosmetic in nature.

Port Numbering

Port numbering conventions for Cisco VG224 voice gateway includes:

- An external Compact Flash card is numbered CF 0.
- 10/100BASE-T Fast Ethernet ports are numbered Fast Ethernet 0/0 and Fast Ethernet 0/1 from right to left.
- FXS voice port numbering begins at 2/0 and extends to 2/7, 2/15, or 2/23, depending on the number of voice ports.

ROM Monitor Commands

The Cisco VG224 voice gateway adds new ROM monitor commands for downloading a software image by TFTP for disaster recovery and for FPGA selection.

The `tftpdnld` Command

The `tftpdnld` command downloads a Cisco IOS software image from a LAN server to Compact Flash using TFTP.

`tftpdnld [-r]`—Begins the TFTP copy procedure.

- `r`—Loads the Cisco IOS software image only to DRAM and launches the image without writing the image to Compact Flash.

The `tftpdnld` command requires you to specify certain variables in the following syntax:

VARIABLE_NAME=value

The following variables are required:

- IP_ADDRESS—IP address for the router you are using.
- IP_SUBNET_MASK—Subnet mask for the router you are using.
- DEFAULT_GATEWAY—Default gateway for the router you are using.
- TFTP_SERVER—IP address of the server from which you want to download the image file.
- TFTP_FILE—Name of the file that you want to download.

The following `tftpdnld` variables are optional:

- TFTP_VERBOSE—Print setting. The default is 1.
 - 0=quiet—After you enter the `tftpdnld` command, the prompt `Do you wish to continue? y/n:` is the only information that appears until the command completes successfully or fails.
 - 1=progress—Displays the state of the required `tftpdnld` command variables. Also displays progress characters to indicate successful and lost packet transmissions.
 - 2=verbose—Displays all progress print setting messages, along with error information. The information provided by this print setting may be useful when debugging interface link and configuration problems that may prevent connecting to the TFTP server.
- TFTP_RETRY_COUNT—Number of times from 1 to 65535 that the ROM monitor retries ARP and ACK. The default is 7 retries.
- TFTP_TIMEOUT—Overall timeout of the download operation in seconds. The range is from 1 to 65535 seconds. The default is 7200 seconds.
- TFTP_CHECKSUM—Performs a checksum test on the image: 0=checksum off, 1=checksum on. The default is 1.
- FE_SPEED_MODE—Sets the Fast Ethernet speed and duplex mode. 0=10 Mbps half-duplex mode, 1=10 Mbps full-duplex mode, 2=100 Mbps half-duplex mode, 3=100 Mbps full-duplex mode, 4=auto-negotiation. The default is 4.

After you specify the variables, you must reenter the **tftpdnld** command. For example:

```
rommon 1 > IP_ADDRESS=172.15.19.11
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=172.16.19.1
rommon 4 > TFTP_SERVER=172.15.20.10
rommon 5 > TFTP_FILE=/tftpboot/cVG224-i-mz
rommon 6 > tftpdnld
```

```
IP_ADDRESS=172.15.19.11
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=172.16.19.1
TFTP_SERVER=172.15.20.10
TFTP_FILE=/tftpboot/VG224-i-mz
```

Invoke this command for disaster recovery only.
 WARNING: all existing data in all partitions on flash will be lost!
 Do you wish to continue? y/n: [n]:

Enter **y** to begin downloading the Cisco IOS software image. When the process is complete, the ROM monitor mode prompt appears on your screen.

Known Problems

There are currently no known problems with the Cisco VG224 voice gateway. To view software related problems, access the following URL:

[Products and Services > Voice Gateways > Cisco VG224 Voice Gateway> Technical Documentation > Cisco VG224 Voice Gateway> Software Center](#)

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Information


Information about Cisco products, services, technologies, and networking solutions is available from various online sources.

- Sign up for Cisco e-mail newsletters and other communications at the Cisco Subscription Center at:
<http://www.cisco.com/offer/subscribe>
- Learn about modifications to or updates about Cisco products. Go to the Product Alert Tool to create a profile, and then choose those products for which you want to receive information. Go to:
<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>
- Order the Cisco Product Quick Reference Guide, a reference tool that includes product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through partners. Go to:
<http://www.cisco.com/go/guide>
- Visit the Cisco Services website to learn the latest technical, advanced, and remote services available to increase the operational reliability of your network. Go to:
<http://www.cisco.com/go/services>
- Visit Cisco Marketplace, the company store, for a variety of books, reference guides, documentation, and logo merchandise at:
<http://www.cisco.com/go/marketplace/>
- Purchase a copy of Cisco technical documentation on a DVD, (Cisco Product Documentation DVD) from the product documentation store at:
<http://www.cisco.com/go/marketplace/docstore>
- Obtain general networking, training, and certification titles from Cisco Press publishers at:
<http://www.ciscopress.com>
- Read the Internet Protocol Journal, a quarterly journal published by Cisco for engineering professionals who design, develop, and operate internets and intranets. Go to:
<http://www.cisco.com/ipj>
- *What's New in Cisco Product Documentation* is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category:
<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>
- Access international Cisco websites at:
http://www.cisco.com/public/countries_languages.shtml

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

 Printed in the USA on recycled paper containing 10% postconsumer waste.