



# Release Notes for the Cisco PIX Firewall Version 6.1(5)

---

July 2003

## Contents

This document includes the following sections:

- [Introduction](#)
- [System Requirements](#)
- [New and Changed Information](#)
- [Important Notes](#)
- [Caveats](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

## Introduction

These release notes describe the features, restrictions, and caveats for Cisco PIX Firewall software version 6.1(5).



---

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

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

# System Requirements

The sections that follow list the system requirements for Cisco PIX Firewall software version 6.1(5).

## Memory Requirements



### Note

The PIX 501 has 16 MB of RAM and will operate correctly with version 6.1(1) and higher, while all other PIX Firewall platforms continue to have at least 32 MB of RAM (and therefore are also compatible with version 6.1(1) and higher). In addition, all units except the PIX 501 and PIX 506/506E require 16 MB of Flash memory to boot. (The PIX 501 and PIX 506/506E have 8 MB of Flash memory, which works correctly with version 6.1(1) and higher.)

Table 1 lists Flash memory requirements for this release:

**Table 1** Flash Memory Requirements

PIX Firewall Model	Flash Memory Required in 6.1
PIX 501	8 MB
PIX 506/506E	8 MB
PIX 515/515E	16 MB
PIX 520	16 MB (Some PIX 520 units may need a memory upgrade because older units had 2 MB, though newer units have 16 MB.)
PIX 525	16 MB
PIX 535	16 MB

Use the PIX-1GE-66 card in systems with a 64-bit/66 MHz PCI bus; for example, in a PIX 535. (If you use the PIX-1GE-66 cards in a PIX Firewall, the system RAM should be at least 128 MB.) For a PIX Firewall with only a 32-bit/33 MHz bus, such as the PIX 520 and PIX 525, use the PIX-1GE card.

## Software Requirements

The following are requirements for Cisco PIX Firewall software version 6.1(5):

1. The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, you need to download the Boothelper file from Cisco.com to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from version 4 or earlier and want to use the IPSec, SSH, PDM, or VPN features or commands, you must have a new 56-bit DES activation key. Before getting a new activation key, write down your old key in case you want to retrograde to version 4. You can have a new 56-bit DES activation key sent to you by completing the form at the following website:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>

3. If you are using PIX Firewall Syslog Server (PFSS), we recommend you install Windows NT Service Pack 6 to fix year 2000 conflicts in Windows NT.
4. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to [“Upgrading to a New Software Release”](#) for new installation requirements.

## Cisco IOS Software Interoperability

Cisco VPN Series	Interoperability
Cisco IOS Routers	If using IKE mode configuration on the PIX Firewall, the router must be running Cisco IOS Release 12.0(6)T or higher.
Cisco VPN 3000 Concentrators	PIX Firewall version 6.1 requires Cisco VPN 3000 Concentrator version 2.5.2 or higher for correct VPN interoperability.

## Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco Secure VPN Client v1.1	PIX Firewall version 6.1 requires Cisco Secure VPN Client version 1.1. Cisco Secure VPN Client version 1.0 and 1.0a are no longer supported.
Cisco VPN 3000 Client v2.5	PIX Firewall version 6.1 requires Cisco VPN 3000 Client version 2.5 or higher. This VPN client can be used with Windows 95, Windows 98, and Windows NT version 4.0. It is not supported on Windows 2000.
Cisco VPN Client v3.x (Unified VPN Client Framework)	PIX Firewall version 6.1 supports the Cisco VPN Client version 3.x. The Cisco VPN Client runs on Linux and all current Microsoft Windows platforms. At this time, the Cisco VPN Client is not supported on other UNIX or Mac platforms.

## Determining the Software Version

Use the **show version** command to determine the software version of your PIX Firewall unit.

## Upgrading to a New Software Release

If you are a registered cisco.com user, you can obtain software from the following site:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>

To register for a cisco.com login, go to the following site:

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

# New and Changed Information

## New Features in Release 6.1(5)

This is a maintenance release for bug fixes only. No new features were introduced.

## New Features in Release 6.1

### PIX 501

The PIX 501 joins the PIX Firewall product line. The PIX 501 offers consumers affordable, enterprise-strength firewall and VPN capabilities. The PIX 501 works with cable and xDSL modems and, additionally, ships with a default configuration for easier “plug-n-play” installation.

### PIX 535 Interfaces

These practices must be followed to achieve the best possible system performance on the PIX 535:

- PIX-1GE-66 interface cards should be installed first in the 64-bit/66 MHz buses before they are installed in the 32-bit/33 MHz bus. If more than four PIX-1GE-66 cards are needed, they may be installed in the 32-bit/33 MHz bus but with limited potential throughput.
- PIX-1GE and PIX-1FE cards should be installed first in the 32-bit/33 MHz bus before they are installed in the 64-bit/66 MHz buses. If more than five PIX-1GE and/or PIX-1FE cards are needed, they may be installed in a 64-bit/66 MHz bus but doing so will lower that bus speed and limit the potential throughput of any PIX-1GE-66 card installed in that bus.

The PIX-1GE Gigabit Ethernet adaptor is supported in the PIX 535; however, its use is strongly discouraged because maximum system performance with the PIX-1GE card is much lower than that with the PIX-1GE-66 card. The software displays a warning at boot time if a PIX-1GE is detected.

Table 2 summarizes the performance considerations of the different interface card combinations.

**Table 2 Gigabit Ethernet Interface Card Combinations**

Interface Card Combination	Installed in Interface Slot Numbers	Potential Throughput
Two to four PIX-1GE-66	0 through 3	Best
PIX-1GE-66 combined with PIX-1GE or just PIX-1GE cards	0 through 3	Degraded
Any PIX-1GE-66 or PIX-1GE	4 through 8	Severely degraded



**Caution**

The PIX-4FE and PIX-VPN-ACCEL cards can only be installed in the 32-bit/33 MHz bus and must never be installed in a 64-bit/66 MHz bus. Installation of these cards in a 64-bit/66 MHz bus may cause the system to hang at boot time.

**Caution**

If Stateful Failover is enabled, the interface card and bus used for the Stateful Failover LAN port must be equal to or faster than the fastest card used for the network interface ports. For example, if your inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then your Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. A PIX-1GE or PIX-1FE card cannot be used in this case, nor can a PIX-1GE-66 card installed in bus 2 or sharing bus 1 with a slower card.

**Note**

Starting with PIX Firewall software version 6.0(1), and in all subsequent higher versions, the PIX Firewall Classic, PIX10000, and PIX 510 platforms are not supported.

## Default Configurations

The PIX 501 ships with a default configuration as of PIX Firewall software version 6.1(1). For more information on the PIX 501 default configuration, please refer to the *Cisco PIX 501 Firewall Quick Start Guide*.

## DHCP Server Pool

The DHCP server pool of the PIX 506 has been expanded to 256 addresses.

For information on new features in previous PIX Firewall software versions, refer to the following website:

[http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/prod_technical_documentation.html)

## Maximum Configuration File Size

For the PIX 525 and PIX 535, the maximum configuration file size limit is increased to 2 MB for PIX Firewall software versions 5.3(2) and higher. For other PIX Firewall platforms and earlier software versions, the maximum configuration file size limit is 1 MB except for the PIX 501, which is limited to a 256 KB configuration file size. However, if you are using PIX Device Manager (PDM), we recommend no more than a 100 KB configuration file because larger configuration files can interfere with the performance of PDM on your workstation.

While configuration files up to 2 MB are now supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as **write term** and **show conf**
- Failover (the configuration synchronization time)
- During a system reload

Cisco Secure Policy Manager may also experience limitations if a PIX Firewall configuration file near 2 MB is used. Please take these considerations into account when planning and implementing your configuration.

# Important Notes

## AAA Authentication

Configure the access list specified in Attribute 11 (specifies per-user access-list name) on the PIX Firewall. Otherwise, remove Attribute 11 from the AAA RADIUS server configuration if no access list is intended for user authentication. If the access list is not configured on the PIX Firewall when the user attempts to log in, the login will fail. AAA, RADIUS, and Attribute 11 information can be found at the following websites:

[http://www.cisco.com/en/US/products/sw/secursw/ps2086/products\\_user\\_guide\\_chapter09186a008007deec.html](http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007deec.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/products\\_configuration\\_guide\\_book09186a0080102925.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080102925.html)

Fast Ethernet cards in 64-bit slots for the PIX 535 are not visible in monitor mode. This problem means that the TFTP server cannot reside on one of these interfaces. The user should use the **copy tftp flash** command to download the PIX Firewall image file via TFTP.

## DHCP Server Functionality

The functionality of the DHCP server on the PIX Firewall has been changed to allow users to define a pool of up to 256 DHCP addresses on the PIX 506/506E and larger platforms.

## Restrictions

Starting with PIX Firewall software version 6.0(1), FDDI, PL2, and Token Ring interfaces are not supported.

Starting with PIX Firewall software version 6.0(1), PFM is no longer supported; PFM has been replaced by the Cisco PIX Device Manager (PDM).

## Caveats

The following sections describe the open caveats for the 6.1(2) release.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

To become a registered cisco.com user, go to the following website:

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

## Open Caveats - Release 6.1(5)

There are no open caveats in this release.

## Resolved Caveats - Release 6.1(5)

The caveats in [Table 3](#) are resolved in this release.

**Table 3** *Resolved Caveats*

DDTS Number	Description
CSCdv33495	static PAT and fixup ftp breaks ACTIVE ftp
CSCdw00291	402103 message for ICMP, although the identities
CSCdw25718	uauth_thread uap->proxy 0 scrolling on console &
CSCdw37960	VSA in accounting records not defined correctly
CSCdw82839	H323:wrong TCP length in proxy ACK with TCP options
CSCdx64091	Cannot connect to HTTP server,SSL:crypto_pki_get_certificates failed
CSCdx65119	PIX waiting for enable password restarts when closing
CSCdx69408	dhcp client failed to get addr from QWEST VDSL router
CSCdx70054	SIP:Compact form of Content-Length not parsed
CSCdx71320	replication does not start by power OFF/ON the Standby
CSCdx72571	active-x filtering is not done when there are no quotes
CSCdx77189	Generating RSA key on active causes stand-by PIX to crash
CSCdx81167	FTP long banner problem when using PIX AAA - v6.2.1
CSCdx84107	SIP:2nd 200 OK from Cancel on same interface dropped
CSCdx85024	H323:Error decoding tunneled H245 message
CSCdx87758	PIX should send source IP of the traffic being
CSCdx89579	PIX 525 Crashes intermittently
CSCdx90840	Failure Detected - No Block Memory (size 272) in failover
CSCdx95442	FTP does not honor norandomseq with PAT
CSCdy01111	Cant TFTP across the VPN between router and PIX(w/VPN accl
CSCdy02422	PIX sending cookies in wrong order in initial contact

**Table 3 Resolved Caveats (continued)**

<b>DDTS Number</b>	<b>Description</b>
CSCdy09114	WinCE and Pocket PC2002 clients cannot get IP address from
CSCdy13293	PIX H225 fixup protocol breaks zero byte TCP keepalives
CSCdy14129	WDT possibility in fixup_h245
CSCdy16100	Block 256 running LOW with syslog severity level =
CSCdy27157	Telnet to PIX does not prompt for username or password
CSCdy27158	PIX gig interface does not support non-auto negotiation
CSCdy28750	SIP:Call forwarding with Pingtel phones do not work
CSCdy29514	TCP window size > 64k breaks NT drive maps through PIX
CSCdy30421	PIX:Unnecessary failover happens when issuing write
CSCdy34949	Command aaa authentication includeexclude ip rejected on
CSCdy40004	PIX may reload at rn_match with high number of routes
CSCdy43488	Standby PIX misrepresenting the status of an interface/s
CSCdy44911	SIP:Session not found when port added to To and/or From
CSCdy47457	standby cfg replicate fails after removing and connecting
CSCdy51810	PIX outside subnet IP is vulnerable to TCP/22 attacks
CSCdy51810	PIX responds to TCP requests destined to the network
CSCdy53135	FTP port command can cause the PIX to stop responding
CSCdy56000	SIP:Fails to find session when Call-ID differs in # of LWS
CSCdy58717	xlate table does not timeout entries.Need clear xlate to
CSCdy65109	first HTTP GET after uauth lacks CR in the end of request
CSCdy68931	Call transfer/no answer fails. Pix doesnt send back 200-OK
CSCdy78026	Inbound TCP connection denied (2nd SYN having same dest
CSCdy78256	PIX should send gratuitous ARP if new Primary inserted in
CSCdy85743	inbound AAA authentication on pix breaks for DNS requests
CSCdz00255	Traceback in isakmp_receiver thread
CSCdz06901	Sip fails with Error-no matching session found for
CSCdz07228	VoIP embryonic conn lookup should match on exact match
CSCdz07673	PIX - SSH via CW2000 will crash PIX during Inventory
CSCdz08403	VoIP:Some embryonic TCP conns not marked as Embryonic
CSCdz09957	PIX - DHCP Client - remove minimum lease time restriction
CSCdz14833	SIP:No matching session found when lws after ; before tag
CSCdz17893	Active MAC of Giga Ethernet remains on Standby after
CSCdz22128	H245:data structures deleted early & causes out of state,
CSCdz29265	SIP:error in sip_skip_lws()
CSCdz31844	PIX does not pass SIP 200 OK messages
CSCdz32478	H.323:one-way audio for scenario with POTS and Skinny

**Table 3 Resolved Caveats (continued)**

DDTS Number	Description
CSCdz54598	SIP:content length wrong if URI contains l:
CSCdz57754	uauth:absolute timeout gets reset upon the tacacs authorization
CSCdz58273	PIX crashes while running out of memory when building new
CSCdz58644	SIP:UDP conns not opened from 100 Trying response
CSCdz82967	SIP:Drop 200 OK due to w/ or w/o display-name of From
CSCea15381	PPPoE and EZVPN mem leak with pix622124diag.bin
CSCea39838	PIX uauth becomes unresponsive after auth in progress
CSCeb01565	PIX crash upon receipt of malformed IPSec/ESP packet -
CSCeb23737	tcp intercept delay when embryonic threshold at max
CSCeb28943	PIX fails to delete SA when receiving invalid-spi notify

## Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN 3000 Client documentation at the following websites:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_technical_documentation.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod_technical_documentation.html)

Cisco provides PIX Firewall technical tips to registered cisco.com users at the following website:

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

To become a registered cisco.com user, go to this website:

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

## Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you are a registered cisco.com user, you can visit the following websites for assistance:

TAC Customer top issues for PIX Firewall:

[http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/products\\_installation\\_guide\\_chapter09186a008017a424.html](http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a008017a424.html)

TAC Sample Configs for PIX Firewall:

[http://www.cisco.com/cgi-bin/Support/PSP/psp\\_view.pl?p=Hardware:PIX&s=Software\\_Configuration](http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX&s=Software_Configuration)

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

[http://www.cisco.com/cgi-bin/Support/PSP/psp\\_view.pl?p=Hardware:PIX](http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX)

To become a registered cisco.com user, go to this website:

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

# 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](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](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>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the 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 comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto: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, 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.

### 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

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or 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 these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (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 Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the the documents listed in “[Related Documentation](#)” section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

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

