



Cisco PIX Firewall Release Notes Version 6.1(1)

December 2001

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

The Cisco PIX Firewall provides secure networking and NAT (Network Address Translation). Version 6.1(1) adds support, optional default configurations, and enhancements to features introduced in earlier releases for the PIX 501. The PIX 506 has an expanded DHCP server pool (up to 256 addresses).



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

Copyright © 2001 Cisco Systems, Inc. All rights reserved.

System Requirements

The sections that follow list the system requirements for operating a PIX Firewall with version 6.1(1) software.

Memory Requirements


Note

All PIX Firewall units require at least 32 MB of RAM memory or the PIX Firewall will not boot. In addition, all units except the PIX 501 and PIX 506 require 16 MB of Flash memory to boot. (The PIX 501 and PIX 506 have 8 MB of memory, which works correctly with version 6.1(1).)

The following table lists Flash memory requirements for this release:

Table 1 *Flash Memory Requirements*

PIX Firewall Model	Flash Memory Required in 6.1(1)	Flash Memory Sold with Unit
PIX 501	8 MB	8 MB
PIX 506	8 MB	8 MB (not upgradeable)
PIX 515	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 525	16 MB	16 MB
PIX 535	16 MB	16 MB

We highly recommend that you use Livengood Gigabit Ethernet cards in systems with a 64-bit/66 MHz PCI bus; for example, in a PIX 535. (If you use the Livengood Gigabit Ethernet 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, we recommend that you use Wiseman Gigabit Ethernet cards.

Software Requirements

The following is required for version 6.1(1):

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 Connection Online (CCO) 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 PFSS (PIX Firewall Syslog Server), 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 later.
Cisco VPN 3000 Concentrators	PIX Firewall version 6.1(1) requires Cisco VPN 3000 Concentrator version 2.5.2 or later for correct VPN interoperability.

Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco Secure VPN Client version 1.x	PIX Firewall version 6.1(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 version 2.5	PIX Firewall version 6.1(1) requires Cisco VPN 3000 Client version 2.5 or later. 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 version 3.0 and version 3.1 (Unified VPN Client Framework)	Supported by PIX Firewall version 6.1(1). The Cisco VPN Client version 3.0 and version 3.1 run on the following systems: <ul style="list-style-type: none"> • PC running Windows 95 OSR2+, Windows 98, Windows ME, Windows NT 4.0, and Windows 2000 • Intel system running Red Hat Linux 6.2 or compatible libraries with glibc version 2.1.1-6 or later, using kernel version 2.2.12 or later
Cisco VPN Client version 3.5 (Unified VPN Client Framework)	Supported by PIX Firewall version 6.1(1). The Cisco VPN Client version 3.5 runs on the following systems: <ul style="list-style-type: none"> • PC running Windows 95 OSR2+, Windows 98, Windows ME, Windows NT 4.0, and Windows 2000 • Intel system running Red Hat Linux 6.2 or compatible libraries with glibc version 2.1.1-6 or later, using kernel version 2.2.12 or later • UltraSPARC running 32-bit Solaris kernel, OS version 2.6 or later • Macintosh running OS X version 10.1.0 or later

Determining the Software Version

Use the **show version** command to verify 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 Hardware Features in Release 6.1(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.

The following table 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.

Changed Hardware Features in Release 6.1(1)



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.

New Software Features in Release 6.1(1)

Default Configurations

The PIX 501 is shipped with default configurations 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*.

The PIX 506 has 25 VPN peers in this release.

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/products/sw/secursw/ps2120/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 later. For other PIX Firewall platforms and earlier software versions, the maximum configuration file size limit remains the same. (In most cases, the optimal maximum configuration size is 1 MB.)

While configuration files up to 2 MB are supported, 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

The following section describes important notes for the 6.1(1) release.

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 login, the login will fail.

Documentation Correction

In the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* under “Failover Usage Notes,” located at the following website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/advanced.htm#82528

Step 2 should read as follows.

Perform the following on any switch that connects to the PIX Firewall:

- a. Enable portfast on all ports on the switch that connects directly to the PIX Firewall.
- b. Turn off trunking on all ports on the switch that connects directly to the PIX Firewall.

- c. Turn off channeling on all ports on the switch that connects directly to the PIX Firewall.
- d. Ensure the MSFC is not running a deferred Cisco IOS software version.

**Note**

Starting in CAT OS 5.4, a new command was added called **set port host**. Essentially, this is a CLI macro that executes the **set spantree portfast enable**, **set trunk off**, and **set port channel off** commands. This command provides a quick and convenient way to configure host or access ports to a mode that allows the port to forward traffic in less than one second from linkup.

Downloading the PIX Firewall Image

Fast Ethernet cards in 64-bit slots 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 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 PIX Device Manager (PDM).

The firewall might ignore requests from SSH clients for certain advanced features, including X11 forwarding, Authentication Agent forwarding, port forwarding, and compression.

Caveats

The following sections describe the open caveats for the 6.1(1) 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

Please use Bug Toolkit on [cisco.com](http://www.cisco.com) to view additional caveat information. Bug Toolkit may be accessed at the following website:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats - Release 6.1(1)

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

Table 3 Open Caveats

ID Number	Software Release	
	6.1(1)	
	Corrected	Caveat Title
CSCds54310	No	Traceback (ci/console) doing sh map , IPsec tunnel exists.
CSCds10112	No	Traceback (Crypto PKI RECV) after twice enrolling and getting denied
CSCds80108	No	Cisco Secure Intrusion Detection System (Cisco Secure IDS) signature number 1101 is not supported by PIX Firewall. When attempted to be accessed, PIX Firewall returns an incorrect error message: Invalid signature number.
CSCdt47829	No	PIX won't learn MAC addresses in range 0008.xxxx.xxxx
CSCdu31945	No	The command sysopt route dnat no longer works correctly.
CSCdu35560	No	netbios does not work with PIX IPsec
CSCdu59514	No	PIX syslogs sent with standby rather than active IP address.
CSCdu59841	No	Traceback in hosts conn cleaner thread.
CSCdu65432	No	Fingerprint of cert not displayed on telnet/ssh session to pix
CSCdu85817	No	hostobjdb being corrupted.
CSCdv14770	No	ACL: hitcnt wrong on outbound ACL with tcp permit eq <port#>
CSCdv21580	No	Cert enrollments fails with 2048bits sp keys with serial/ip options
CSCdv24360	No	PIX rebooted with traceback in qos_metric_daemon thread
CSCdv24986	No	Assertion if conf net and command write mem in config file.
CSCdv25850	No	PIX reboots with stack trace in isakmp_receiver thread (stress).
CSCdv26489	No	Error in cert validation occurs sometimes when peer changes certs
CSCdv26934	No	PIX reboots (isakmp_thread) when negotiating with PIX (revoked cert)
CSCdv30928	No	SIP: Register messages to remote Proxy dropped
CSCdv31029	No	SIP: maddr field not NATd

Resolved Caveats - Release 6.1(1)

The caveats in [Table 4](#) are resolved in this release.

Table 4 *Resolved Caveats*

ID Number	Software Release	
	6.1(1)	
	Corrected	Caveat Title
CSCds21095	Yes	pix pptp stop accepting new connections after sometimes of operation
CSCds71849	Yes	dbgtrace_is_debug_trace_on() function need to be optimized
CSCds89340	Yes	WDT in dbgtrace thread
CSCdt61216	Yes	Naptha (ESTABLISHED) Flooding causes PDM DoS
CSCdt77025	Yes	Assertion (IPsec response handler) while running pixIpsecIsakmp.
CSCdt82325	Yes	Reload due to exhausted memory while URL filtering heavy traffic.
CSCdt86736	Yes	Noticable pause with more than 50000 UDP connections
CSCdt94747	Yes	H323: PIX should proxy ACK TPKT if we recvd TPKT only
CSCdu01836	Yes	PDM sessions are not released even after closing all the browsers
CSCdu05134	Yes	H.323 call does not go thru if calling GW uses slow start
CSCdu10483	Yes	PIX doesn't delete its isa sas if the peer doesn't negotiate sa
CSCdu12321	Yes	pix fail to do write mem , if a big cmd line exists
CSCdu13760	Yes	Perfmon values increase when you do a show perfmon
CSCdu15498	Yes	501: have better err msg for write and conf floppy
CSCdu15512	Yes	501:VPN LED stays up when there is no VPN traffic/tunnel
CSCdu15537	Yes	501: PIX 501 takes 6-ifx license, and show ver lists max 6 supported
CSCdu20056	Yes	Blocks information is empty when PIX crashed.
CSCdu20593	Yes	Xauth: With IRE on rekey puts internal addr. entry for uauth.
CSCdu22069	Yes	SIP: With Out Proxy & global/nat, xlate created for outside addr
CSCdu22771	Yes	PIX is sending Initial Contact during rekey, between PIX-PIX
CSCdu24181	Yes	Traceback (IPsec response handler) after L2TP tunnel created.
CSCdu25110	Yes	501:mac-addr program in biosburn does not recognize interfaces
CSCdu25260	Yes	mkpdm with arg 1.0.1 shows up as 1.0(1)0 in PDM About window
CSCdu25837	Yes	Software needs to limit PIX 501 interface speed to 10baseT
CSCdu27169	Yes	VoIP: certain embedded IP addr not NATd
CSCdu28566	Yes	501: show version display processor speed 100 not 133MHz
CSCdu29410	Yes	PIX501: Unit takes failover license which it shouldn't
CSCdu32616	Yes	501: The RAM requirement for 501 should be 16M instead of 32M
CSCdu33209	Yes	IPSec Antireplay Checking Ineffective 32-64 sequence numbers back

Table 4 Resolved Caveats (continued)

ID Number	Software Release	
	6.1(1)	
	Corrected	Caveat Title
CSCdu33543	Yes	pix ptp rejects dial-in req after abnormal termination
CSCdu35041	Yes	Assertion crash with lport fport after startup
CSCdu36628	Yes	PIX neither uses nor discards CRL if time < last CRL update of CA.
CSCdu38093	Yes	PIX crashed in tcp_slow thread when enrolling for certs with sp keys
CSCdu38206	Yes	Config lines greater than 255 displayed incorrectly by sh conf
CSCdu38927	Yes	PIX failover should try to allocate additional blk if possible
CSCdu39748	Yes	H323: generating 50+ calls causes unexpected reload
CSCdu39748	Yes	H323: generating 50+ calls causes unexpected reload
CSCdu40845	Yes	PIX - Failover does not work with ip verify reverse-path RPF
CSCdu41413	Yes	xauth skipped with client 3.0 if inside and outside swapped
CSCdu41525	Yes	Netscape error when connecting to PIX with rsa special key
CSCdu41996	Yes	Watchdog after interface PAT pool exhausted
CSCdu42112	Yes	AAA:when down does not return rejection while using radius
CSCdu42645	Yes	Kodiak: some status bits are ignored
CSCdu42656	Yes	Kodiak: AH decapsulation requests not setup correctly
CSCdu43284	Yes	H323: make use of NELTS & sizeof, remove extern functions
CSCdu47003	Yes	Able to pass disallowed SMTP command thru PIX, by sending after mail
CSCdu48184	Yes	Nested traceback handling is confusing
CSCdu53473	Yes	H225 H245 messages greater than 1024 bytes not inspected
CSCdu53971	Yes	misconfigured failover ifc a.b.c.d lines cause flip-flops
CSCdu54443	Yes	501:slow performance with mismatched duplex on switch and eth ports
CSCdu54455	Yes	501:show version hangs when printing the pix version
CSCdu54495	Yes	Unexpected reload when using Websense with TCP4 and url-cache.
CSCdu55206	Yes	Traceback while trying to establish a PPTP tunnel (scripted).
CSCdu55859	Yes	URL with arguments are not handled properly
CSCdu57729	Yes	max arp number for small memory model should be 256 instead of 16
CSCdu59514	Yes	PIX syslog are sent with standby ip address
CSCdu60447	Yes	PIX should not initialize COM3 & COM4 serial ports
CSCdu61691	Yes	stateful failover doesn't replicate conn for passive ftp using PAT
CSCdu62372	Yes	Eliminator Disk does not transfer IP packets properly
CSCdu62647	Yes	Kodiak:IPSec encrypt packet introp with IOS is not working in ftp
CSCdu63067	Yes	Perfmon command causes interface no buffer
CSCdu63388	Yes	SYN-ACK retransmit zeroizes the idle timeout on conn

Table 4 Resolved Caveats (continued)

ID Number	Software Release	
	6.1(1)	
	Corrected	Caveat Title
CSCdu66557	Yes	H323 Skinny does not properly open 3rd party IP using nat 0 acl
CSCdu67493	Yes	clear int followed by interface number clears all the interfaces
CSCdu67799	Yes	IPSEC:pix takes long time to create a 2nd Isec tunnel (1 IKE)
CSCdu68118	Yes	Write net fails when the first two ethernet int are not in use
CSCdu68124	Yes	Intercepted connections timeout prematurely if they are idle
CSCdu70055	Yes	PRNG weakness in SSL
CSCdu70175	Yes	failing to contact secondary radius server
CSCdu72961	Yes	PIX fails to change identity field for RFC 2865
CSCdu73070	Yes	Xauth:2 extra prompts for any auth, when a auth request fails radius
CSCdu74672	Yes	SMTP Fixup: end-of-data checking incorrect
CSCdu76004	Yes	501:continuous reboot if pdm install is not successful
CSCdu78806	Yes	SIP: Pingtel phones SIP messages dropped by fixup module
CSCdu80080	Yes	SYSLOG: abbreviated logging cmd not replicated on standby PIX
CSCdu80222	Yes	Show version: change PIX and PDM product names.
CSCdu80852	Yes	Panic: pix/intf0 - init_sip: create_chunk failed
CSCdu83457	Yes	extra process_suspend() may cause missing stateful updates
CSCdu88336	Yes	IKE delete notify does not delete IPsec SA 60 seconds after setup
CSCdu89190	Yes	PIX crashes with multiple ssh aaa authen failures or success
CSCdu89348	Yes	PIX reboots with traceback in isakmp_receiver thread when no memory
CSCdu89431	Yes	Watchdog timeout failure in ci/console while clearing ipsec sas
CSCdv00692	Yes	PIX reboots dumping stack trace in isakmp_time_keeper thread
CSCdv01450	Yes	H225: wrong TCP seq if H225v1 re-encoded to H225v2
CSCdv01748	Yes	dhcpcd will not work with ip verify reverse path interface inside
CSCdv03096	Yes	PIX vulnerable to invalid SIP packets
CSCdv04717	Yes	i82550EY devices identified as i82557s
CSCdv06822	Yes	501:Watchdog timeout followed by traceback (isakmp_time_keeper)
CSCdv06996	Yes	501:PIX is unable to rekey phase1 when the limit reaches to 5 tunnel
CSCdv09731	Yes	PIX - AAA failing due to limited number of uauth sessions/source ip
CSCdv10117	Yes	Watchdog timeout failure, and hang after reload pri or sec PIX535.
CSCdv11921	Yes	501:VPN LED on with no ISA/IPSec SA when SA not deleted thru peer
CSCdv12077	Yes	PIX-506: ifx becomes 100full after reload, when configured to auto
CSCdv18119	Yes	Skinny: StationRegister message not NATd correctly

Table 4 Resolved Caveats (continued)

ID Number	Software Release	
	6.1(1)	
	Corrected	Caveat Title
CSCdv23491	Yes	Cannot load an image on PIX through copy tftp flash command
CSCdv25865	Yes	Watchdog timeout in isakmp_receiver thread

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/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

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

TAC Sample Configs for PIX Firewall:

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

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

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>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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.

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
- 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
- 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 documents listed in the “[Related Documentation](#)” section.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That’s Possible 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, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0110R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

