CISCO SYSTEMS

VPN 3002 Hardware Client
Getting Started, Release 4.0

April 2003

CONTENTS

CHAPTER 3   **Using the VPN 3002 Hardware Client Manager for Quick Configuration   3-1**

I N D E X INDEX

VPN 3002 Hardware Client Getting Started, Release 4.0

Preface

VPN 3002 Hardware Client Getting Started provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). You can do Quick Configuration from a console with the menu-based Command-Line Interface, or you can use the HTML-based VPN 3002 Hardware Client Manager with a browser. This manual describes both methods, and we recommend the latter for ease of use.

Audience

We assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices might be new to you. You should be familiar with Windows system configuration and management, and you should be familiar with Microsoft Internet Explorer or Netscape Navigator or Communicator browsers.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the VPN 3002 Hardware Client	Summarizes the hardware and software features and operation.
Chapter 2	Installing and Powering Up the VPN 3002	Explains how to prepare for, unpack, install, and power up the VPN 3002 Hardware Client, and how to begin quick configuration. Once you have completed the steps in this chapter, you can use *either* Chapter 3 *or* Chapter 4 to complete quick configuration.
Chapter 3	Using the VPN 3002 Hardware Client Manager for Quick Configuration	Explains how to start and complete quick configuration of the system using the VPN 3002 Hardware Client Manager with a browser. We recommend this method.

Chapter	Title	Description
Chapter 4	Using the Command-Line Interface for Quick Configuration	Explains how to complete quick configuration of the system using the command-line interface from the console or a Telnet or SSH session.
Appendix A	Troubleshooting and System Errors	Describes common errors that might occur while configuring or using the system, and how to correct them. It also describes all LED indicators on the VPN 3002.

Related Documentation

Refer to the following documents for further information about Cisco VPN 3000 Series applications and products.

VPN 3002 Hardware Client Documentation

The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.

The *VPN 3002 Hardware Client Quick Start* card summarizes the information for quick configuration. This quick reference card is provided with the VPN 3002 and is also available online.

The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for quick configuration. It is provided with the VPN 3002 and you can also print it from the online version; you can affix the label to the VPN 3002.

The HTML interface, called the VPN 3002 Hardware Client Manager, includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It defines and explains all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The HTML interface, called the VPN Concentrator Manager, includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

VPN Client Documentation

The *Cisco VPN Client User Guide for Windows,* the *Cisco VPN Client User Guide for Linux and Solaris,* and the *Cisco VPN Client User Guide for Mac OS X* explain how to install, configure, and use the VPN Client. The VPN Client lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN Concentrator.

The *VPN Client Administrator Guide* tells how to configure a VPN 3000 Concentrator for remote user connections using the VPN Client, how to automate remote user profiles, how to customize VPN Client software, how to use the VPN Client command-line interface, and how to get troubleshooting information.

Documentation on VPN Software Distribution CDs

The VPN 3000 Series Concentrator and VPN 3002 Hardware Client documentation are provided on the VPN 3000 Concentrator software distribution CD-ROM in PDF format. The VPN Client documentation is included on the VPN Client software distribution CD-ROM, also in PDF format. To view the latest versions on the Cisco web site, click the Support icon on the toolbar at the top of the VPN Concentrator Manager, Hardware Client Manager, or Client window. To open the documentation, you need Acrobat Reader 3.0 or later; version 4.5 is included on the Cisco VPN 3000 Concentrator software distribution CD-ROM and on the VPN Client software distribution CD-ROM.

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.

- *Virtual Private Networking: An Overview.* Microsoft Corporation: 1999. (Available from Microsoft website.)

- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`^`	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, 00.10.5A.1F.4F.07).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, VPN01). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Filenames	Filenames on the VPN 3002 follow the DOS 8.3 naming convention: a maximum of eight characters for the name, plus a maximum of three characters for an extension. For example, LOG00007.TXT is a legitimate filename. The VPN 3002 always stores filenames in uppercase.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at 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 is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

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/cgi-bin/order/order_root.pl

• Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

• Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) 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. In the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. Some services on the Cisco TAC Web Site require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Understanding the VPN 3002 Hardware Client

The Cisco VPN 3002 Hardware Client communicates with a VPN 3000 Series Concentrator to create a virtual private network across a TCP/IP network (such as the Internet). The VPN 3002 requires minimal configuration, and you can monitor, configure, and upgrade multiple hardware clients at multiple sites from a central location.

The secure connection between the VPN 3002 and the VPN Concentrator is called a tunnel; it uses the IP Security (IPSec) protocol to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. It can support a single IP network.

VPN 3002 Hardware Client or VPN Client Software?

The VPN 3002 Hardware Client provides an alternative to deploying the VPN client software to PCs at remote locations. Like the software client, the VPN 3002 is located at a remote site, and provides a secure connection to a VPN Concentrator at a central site. It is important to understand that it is a hardware *client*, and that you configure it as a client of the central-site VPN Concentrator, not as a site-to-site connection.

Reasons to use the VPN 3002 rather than the software client include:

- You do not own, control, or want to support the PCs at the remote site. Using the VPN 3002 eliminates the need to install and maintain software on those computers.

- You have a large number of remote sites to which you connect using VPNs, and you want to manage those VPNs from a central location.

- You have multiple computers at a remote site, and you want them to be able to access resources across the tunnel.

Hardware Features

There are two versions of this VPN 3002 Hardware Client:

- The VPN 3002 has one public and one private 10/100BASE-T Ethernet interface.

- The VPN 3002-8E has one public interface and a built-in 8-port 10/100BASE-T Ethernet switch as its private interface.

All systems feature:

- Motorola PowerPC CPU
- SDRAM memory for normal operation
- Nonvolatile memory for critical system parameters
- Flash memory for file management
- Software-based encryption
- Single power supply

Client Mode and Network Extension Mode

The VPN 3002 works in either of two modes: Client mode or Network Extension mode. Client mode is the default.

Online Technical Snapshot Explains PAT and Network Extension Modes

A new interactive multimedia piece explains the differences between Client (PAT) mode and Network Extension mode. To view it, go to this url:

http://www.cisco.com/mm/techsnap/VPN3002_techsnap.html

Your web browser must be equipped with a current version of the Macromedia Flash Player to view the content. If you are unsure whether your browser has the most recent version, you may want to download and install a free copy from:

http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash

Client Mode (PAT)

Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the VPN 3002 private network from those on the corporate network. In PAT mode:

- IPSec encapsulates all traffic going from the private network of the VPN 3002 to the network(s) behind the Internet Key Exchange (IKE) peer, that is, the central-site VPN Concentrator.
- PAT mode employs NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the IP address of the VPN 3002 public interface. The central-site VPN Concentrator assigns this address. NAT also keeps track of these mappings so that it can forward replies to the correct device.

All traffic from the private network appears on the network behind the central-site VPN Concentrator (the IKE peer) with a single source IP address. This IP address is the one the central-site VPN Concentrator assigns to the VPN 3002. The IP addresses of the computers on the VPN 3002 private network are hidden. You cannot ping or access a device on the VPN 3002 private network from outside of that private network, or directly from a device on the private network at the central site.

Client Mode with Split Tunneling

You always assign the VPN 3002 to a tunnel group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec and PAT are applied to all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator.

Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the assigned IP address of the public interface and also keeps track of these mappings so that it can forward replies to the correct device.

The network and addresses on the private side of the VPN 3002 are hidden, and cannot be accessed directly.

Network Extension Mode

Network Extension mode allows the VPN 3002 to present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the VPN 3002 private network to networks behind the central-site VPN Concentrator. PAT does not apply. Therefore, devices behind the VPN Concentrator have direct access to devices on the VPN 3002 private network over the tunnel, and only over the tunnel, and vice versa. The VPN 3002 must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

In this mode, the central-site VPN Concentrator does not assign an IP address for tunneled traffic (as it does in Client/PAT mode). The tunnel is terminated with the VPN 3002 private IP address (the assigned IP address). To use Network Extension mode, you must configure an IP address other than the default of 192.168.10.1 and disable PAT.

Network Extension Mode per Group

Software versions 3.6 and later let a network administrator restrict the use of network extension mode. On the VPN Concentrator, you enable network extension mode for VPN 3002 hardware clients on a group basis.

Note   If you disallow network extension mode, which is the default setting on the VPN Concentrator, the VPN 3002 can connect to that VPN Concentrator in PAT mode only. In this case, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 attempts to connect every 4 seconds, and every attempt is rejected. In this situation, the VPN 3002 puts an unnecessary processing load on the VPN Concentrator to which it connects; if large numbers of VPN 3002s are misconfigured in this way, the VPN Concentrator has a reduced ability to provide service.

Network Extension Mode with Split Tunneling

You always assign the VPN 3002 to a tunnel group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec operates on all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator. PAT does not apply.

Traffic from the VPN 3002 to any destination other than those within the network list on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices on the VPN 3002 private network to the address of the VPN 3002 public interface. Thus the network and addresses on the private side of the VPN 3002 are accessible over the tunnel, but are protected from the Internet, that is, they cannot be accessed directly.

IPSec

IPSec is the set of standards that enables the VPN 3002 to connect to a central-site VPN Concentrator over a secure VPN tunnel. Its security measures address data privacy, integrity, authentication, and key management, as well as tunneling.

IPSec over TCP

The VPN 3002 supports IPSec over TCP, which encapsulates encrypted data traffic within TCP packets. IPSec over TCP enables the VPN 3002 to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls.

Note   This feature does not work with proxy-based firewalls.

The VPN 3002 Hardware Client, which supports one tunnel at a time, can connect using standard IPSec, IPSec over NAT-T, IPSec over TCP, or IPSec over UDP, but only one for the same tunnel.

To use IPSec over TCP, both the VPN 3002 and the VPN Concentrator to which it connects must

- Be running version 3.5 or later software. A VPN 3002 running software earlier than version 3.5 can connect to a VPN Concentrator running version 3.5 software and using IPSec over TCP, with the VPN 3002 using either IPSec or IPSec over UDP.
- Enable IPSec over TCP.
- Configure the same port for IPSec over TCP on both the VPN 3002 and the VPN Concentrator.

IPSec over NAT-T

NAT-T (NAT Traversal) lets IPSec peers establish a connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPSec traffic when necessary.

The VPN 3002 hardware client supports NAT-T in software version 3.6 and later. It uses NAT-T by default, and requires no configuration. The VPN 3002 first attempts NAT-T, and then IPSec/UDP (if enabled) if a NAT device is not auto-detected, allowing IPSec traffic to pass through firewalls that disallow IPSec.

To use NAT-T you must:

- Open port 4500 on any firewall you have configured in front of a VPN 3002.
- Reconfigure any previous IPSec/UDP configuration using port 4500 to a different port.

• Select the second or third options for the Fragmentation Policy parameter in the Configuration | Interfaces | Public screen. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

IPSec over UDP

The VPN 3002 supports User Datagram Protocol (UDP) Network Address Translation/Firewall (NAT) Transparent IPSec, which encapsulates encrypted data traffic within UDP packets. IPSec over UDP enables secure transmission between the VPN 3002 Hardware Client and the VPN Concentrator at the central site through a device, such as a firewall, that is performing Network Address Translation (NAT). The VPN 3002 sends keepalives frequently, ensuring that the mappings on the NAT device are kept active.

You do not have to configure this feature on the VPN 3002, but the following requirements do apply:

• Both the VPN Concentrator and the VPN 3002 must be running Release 3.0.3 or higher software.

• You must configure IPSec over UDP for the group on the VPN Concentrator to which the VPN 3002 belongs. For an example, refer to the VPN 3000 Concentrator Manager, Configuration | User Management | Groups | IPSec tab (use the VPN Concentrator Manager Help, or refer to *VPN 3000 Concentrator Series Reference Volume I: Configuration*).

Note   We do not currently support a topology with multiple VPN 3002 Hardware Clients behind one NAT device.

Additional Software Features

The VPN 3002 software includes these features.

Interactive Hardware Client Authentication

Interactive hardware client authentication prevents users on the VPN 3002 private LAN from accessing the central site until the VPN 3002 authenticates.

When you enable interactive hardware client authentication, the VPN 3002 does not use a saved username and password. Instead you must manually enter a valid username and password for the VPN 3002 each time you connect. When the VPN 3002 initiates the tunnel, it sends the username and password to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication, on either the internal or an external server. If the username and password are valid, the tunnel is established.

You configure interactive hardware client authentication on the VPN Concentrator, which pushes the policy to the VPN 3002. For more information and configuration instructions, refer to the "User Management" chapter of the VPN 300 Series Concentrator Reference Volume 1: Configuration.

Enabling and Later Disabling Interactive Hardware Client Authentication

When you enable interactive hardware client authentication for a group, the VPN Concentrator pushes that policy to the VPN 3002s in the group. If you have previously set a username and password on the VPN 3002, the software deletes them from the configuration file. When you try to connect, the software prompts you for a username and password.

If, on the VPN Concentrator, you subsequently disable interactive hardware authentication for the group, it is enabled locally on the VPN 3002, and the software continues to prompt for a username and password. This lets the VPN 3002 connect, even though it lacks a saved username and password, and the VPN Concentrator has disabled interactive hardware client authentication.

If you subsequently configure a username and password (in the VPN 3002 Configuration | System | Tunneling Protocols | IPSec screen), the feature is disabled, and the prompt no longer displays. The VPN 3002 connects to the VPN Concentrator using the saved username and password.

Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the private network of the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists. The VPN 3002 directs the browser to the proper pages for login. When the user successfully logs in, the browser displays your default home page.

Note   You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

- If you have a default home page on the remote network behind the VPN Concentrator, or direct the browser to a website on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.

- If you try to access resources on the network behind the VPN Concentrator that are not web-based, for example, email, the connection fails until you authenticate with a browser.

- To authenticate, you must enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.

- One user can log in for a maximum of four sessions simultaneously.

- Individual users authenticate according to the order of authentication servers that you configure for a group on the VPN Concentrator.

You configure individual user authentication on the VPN Concentrator, which pushes the policy to the VPN 3002. For more information and configuration instructions, refer to the "User Management" chapter of the *VPN 3000 Series Concentrator Reference Volume 1: Configuration.*

LEAP Bypass

LEAP (Lightweight Extensible Authentication Protocol) Bypass lets LEAP packets from devices behind a VPN 3002 travel across a VPN tunnel prior to individual user authentication. This lets workstations using wireless access point devices establish LEAP authentication. Then they authenticate again per individual user authentication (if enabled).

Administrators enable LEAP Bypass on a group basis at the central site, via a checkbox on the VPN Concentrator HW Client tab on the Group configuration page.

LEAP Overview

IEEE 802.1X is a standard for authentication on wired and wireless networks. It provides wireless LANs with strong mutual authentication between clients and authentication servers, which can provide dynamic per-user, per-session wireless encryption privacy (WEP) keys, removing administrative burdens and security issues that are present with static WEP keys.

Cisco Systems has developed an 802.1X wireless authentication type called Cisco LEAP. LEAP implements mutual authentication between a wireless client on one side of a connection and a RADIUS server on the other side. The credentials used for authentication, including a password, are always encrypted before they are transmitted over the wireless medium.

LEAP Bypass Overview

LEAP users behind a VPN 3002 have a circular dilemma: they cannot negotiate LEAP authentication because they cannot send their credentials to the RADIUS server behind the central site device over the tunnel. The reason why they can't send credentials over the tunnel is because they have not authenticated on the wireless network. To solve this problem, LEAP Bypass lets LEAP packets, and only LEAP packets, traverse the tunnel to authenticate the wireless connection to a RADIUS server before individual users authenticate. Then the users proceed with individual user authentication.

LEAP Bypass works as intended under the following conditions:

- The interactive unit authentication feature (intended for wired devices) must be disabled. If interactive unit authentication is enabled, a non-LEAP (wired) device must authenticate the VPN 3002 before LEAP devices can connect using that tunnel.

- Individual user authentication is enabled (if it is not, you don't need LEAP Bypass).

- Access points in the wireless environment must be Cisco Aironet Access Points. The wireless NIC cards for PCs can be other brands.

- The Cisco Aironet Access Point must be running Cisco Discovery Protocol (CDP).

- The VPN 3002 can operate in either client mode or network extension mode.

- For LEAP authentication, packets travel over the tunnel to a RADIUS server via ports 1645 or 1812.

⚠️

Caution   There may be security risks in allowing any unauthenticated traffic to traverse the tunnel.

Summary of VPN 3002 Authentication Features

Table 1-1 summarizes how authentication of the VPN 3002 works by default, and how it works with interactive hardware client authentication and individual user authentication enabled. Be aware that you can use both interactive hardware client authentication or individual user authentication simultaneously, or either one and not the other.

*Table 1-1   Authenticating the VPN 3002 Hardware Client and Users*

Authentication with Saved Username and Password	Interactive Hardware Client Authentication	Individual User Authentication	LEAP Bypass
Authenticates the VPN 3002.	Authenticates the VPN 3002.	Authenticates a user or device on the private LAN behind the VPN 3002.	Authenticates a wireless user or device on the private LAN behind the VPN 3002.
On the VPN 3002, you configure the username and password in either of these screens: • Configuration	Quick	IPSec. • Configuration	System	Tunneling Protocols	IPSec.	You do not configure the username and password on the VPN 3002.	You do not configure the username and password on the VPN 3002.	You configure the Aironet Client Utility to use a saved username and password, or to prompt for a username and password each time a client connects. For more information, refer to the *Cisco Aironet Wireless LAN Adapters Installation and Configuration Guide*.
The VPN 3002 saves the username and password.	The VPN 3002 does not save the username and password.	The VPN 3002 does not save the username and password.	
Requires no user interaction subsequent to initial configuration.	You are prompted to enter a username and password each time the VPN 3002 initiates the tunnel.	You open a web browser and enter a username and password when prompted, even though the tunnel already exists. You cannot use the command-line interface.	If you use a saved username and password, LEAP requires no user interaction subsequent to initial configuration. Otherwise the Aironet Client Utility prompts you to enter a username and password.
The default option.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.	You enable on the VPN Concentrator. The VPN Concentrator pushes the policy to the VPN 3002.
The VPN 3002 authenticates on the first server of the type that you configure. If the VPN 3002 cannot reach that server, it authenticates on the next server of that type in the list of authentication servers.		Individual users authenticate according to the order of authentication servers configured, regardless of type.	Individual users authenticate to RADIUS servers according to how the authentication servers are configured on the Aironet Access Point.
		Individual users can authenticate according to the values of an embedded group rather than the tunnel group. See the next section.	

IPSec Backup Servers

IPSec backup servers let a VPN 3002 hardware client connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002, or on a group basis at the central-site VPN Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group.

Figure 1-1 illustrates how the backup server feature works.

Figure 1-1   Backup Server Implementation
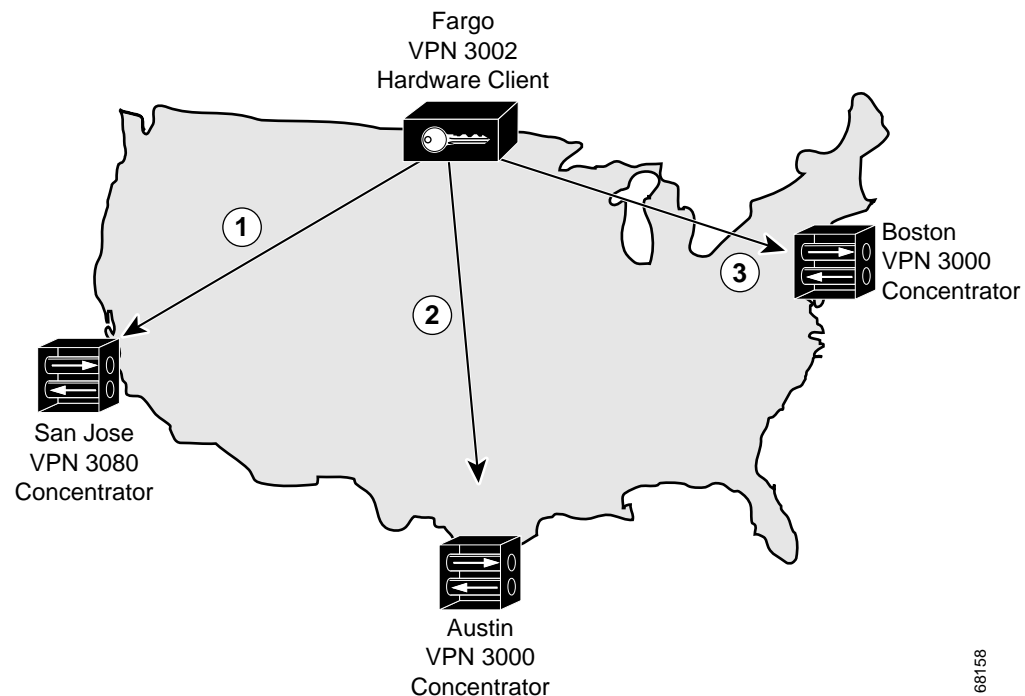
XYZ corporation has large sites in three cities: San Jose, California; Austin, Texas; and Boston, Massachusetts. They just opened a regional sales office in Fargo, North Dakota. To provide access to the corporate network from Fargo, they use a VPN 3002 that connects to a VPN 3080 in San Jose (1). If the VPN 3002 is unable to contact the corporate network, Fargo cannot place orders. The IPSec backup server feature lets the VPN 3002 connect to one of several sites, in this case using Austin (2) and Boston (3) as backup servers, in that order.

The VPN 3002 in Fargo first tries to reach San Jose. If the initial IKE packet for that connection (1) times out (8 seconds), it tries to connect to Austin (2). Should this negotiation also time out, it tries to connect to Boston (3). These attempts continue until the VPN 3002 has tried all servers on its backup server list, to a maximum of 10.

Be aware of the following characteristics of the backup server feature:

- If the VPN 3002 cannot connect after trying all backup servers on the list, it does not automatically retry.

    - In Network Extension mode, the VPN 3002 attempts a new connection after 4 seconds.

- In Client mode, the VPN 3002 attempts a new connection when the user clicks the Connect Now button on the Monitoring | System Status screen, or when data passes from the VPN 3002 to the VPN Concentrator.

• A VPN 3002 must connect to the primary VPN Concentrator to download a backup server list configured on the primary VPN Concentrator. If that VPN Concentrator is unavailable, and if the VPN 3002 has a previously configured backup server list, it can connect to the servers on that list.

• It can download a backup server list only from the primary VPN Concentrator. The VPN 3002 cannot download a backup server list from a backup server.

• The VPN Concentrators that you configure as backup servers do not have to be aware of each other.

• If you change the configuration of backup servers, or delete a backup server during an active session between a VPN 3002 and a backup server, the session continues without adopting that change. New settings take effect the next time the VPN 3002 connects to its primary VPN Concentrator.

You can configure the backup server feature from the primary VPN Concentrator or the VPN 3002. From the VPN Concentrator configure backup servers on either of the Configuration | User Management | Base Group or Groups | Mode Configuration screens. On the VPN 3002, configure backup servers on the Configuration | System | Tunneling Protocols | IPSec screen.

The list you configure on the VPN 3002 applies only if the option, Use Client Configured List, is set. To set this option, go to the IPSec Backup Servers parameter on the Mode Configuration tab of the Configuration | User Management | Groups | Add/Modify screen of the primary VPN Concentrator to which the VPN 3002 connects.
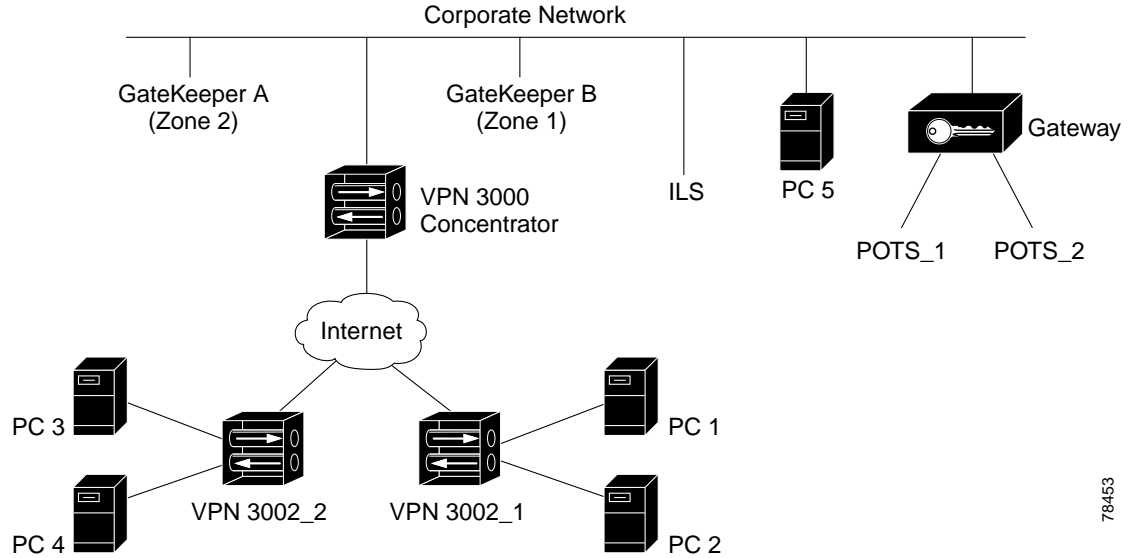
> **Note** The group name, username, and passwords that you configure for the VPN 3002 must be identical for the primary VPN Concentrator and all backup servers. Also, if you require interactive hardware client authentication and/or individual user authentication for the VPN 3002 on the primary VPN Concentrator, be sure to configure it on backup servers as well.

H.323 in PAT Mode

H.323 is the packet-based multimedia communications standard written by the ITU. A variety of applications use this standard to effect real-time audio, video and data communications. It lets the VPN 3002 support Microsoft NetMeeting. Figure 1-2 is a network diagram that illustrates H.323 services the VPN 3002 supports. H.323 requires no configuration on the VPN 3002.

Figure 1-2   H.323 Network Example

The following sections describe H.323 features, referring to Figure 1-2.

H.323 Element	Description
NetMeeting	Microsoft conferencing and collaboration software. Features include video and audio conferencing, whiteboard, chat, file transfer, program sharing, and remote desktop sharing.
	VPN 3002 H.323 services support NetMeeting. PCs 1, 2, 3, 4, and 5 and POTS_1 and 2 can communicate using NetMeeting applications. This includes PC3 communicating with PC 4, and PC1 communicating with PC2. Any PC can host a NetMeeting conference.
GateKeeper	A Cisco IOS H.323 GateKeeper, for example, a Cisco 2620 router. GateKeepers provide registration, call control, and status management for H.323 endpoints and gateways.
	• GateKeeper services must reside on the corporate network.
	• Multiple NetMeeting PCs behind the same VPN 3002 can simultaneously register and place H.323 calls to one or more GateKeeper zones. For example, PC 3 and PC 4 can both register to either GateKeeper A or GateKeeper B, and PC3 can register to GateKeeper A at the same time that PC 4 registers to GateKeeper B.
	• Two or more PCs behind a VPN 3002 that register to a GateKeeper can make or receive simultaneous calls between two or more endpoints. For example, PC 1 can call PC3 at the same time that a call from PC 2 to PC 4 and PC 5 is in progress.
ILS (Internet Locator Directory Services)	Microsoft software that uses the LDAP protocol to provide registration and status management for H.323 endpoints.
	• ILS services must reside on the corporate network.
	• Multiple PCs behind the same VPN 3002 cannot register to an ILS server. For example, PC 3 and PC 4 cannot both register to the same ILS server. PC 1 and PC 4 can both register to the same ILS server.
	• ILS registration for NetMeeting on Windows 9x PCs defaults to LDAP port 389, and for Windows 2000 PCs to port 1002. If your ILS server cannot use port 1002, you need to reconfigure Windows 2000 PCs for LDAP port 389.
Note	A PC can register with either a GateKeeper or with an ILS server, but not both simultaneously.
Gateway	A Cisco IOS H.323 Gateway, for example, a Cisco 3620 router. Gateways let H.323 devices, in this case NetMeeting PCs, communicate with non-H.323 devices, such as POTS phones.
POTS	Plain old telephone system. Any PC can initiate a NetMeeting call to a POTS phone and exchange audio. However, a POTS phone cannot initiate a call to a NetMeeting PC behind a VPN 3002.
	In this example, PCs 1, 2, 3, 4, or 5 can initiate calls to POTS_1 or POTS_2, but POTS_1 and POTS_2 can only receive calls.
MCU	Multipoint control units. The VPN Concentrator H.323 implementation does not support MCUs.
H.323 Endpoint	A PC running NetMeeting or an H.323 Gateway.

Notes on H.323 GateKeepers

Be aware of the following characteristics of NetMeeting GateKeepers.

NetMeeting Displays Names of Previous Meeting Callers

When an H.323 call is disconnected, the NetMeeting application still displays the names of the meeting callers in the Call window. Before you place a new call, perform a Hangup operation to remove these names.

VPN Tunnel Disconnects or a Network Failure Occurs with NetMeeting Active

When a VPN tunnel disconnects without the PC behind the VPN 3002 logging off from the GateKeeper, problems may occur. This is so whether the VPN session terminates gracefully, or because of a network failure (NetMeeting PC reboots or VPN 3002 reboots).

Because of the failure to log off, a registration mismatch may occur between the GateKeeper and the NetMeeting application. The GateKeeper maintains a NetMeeting registration based on a configurable inactivity timeout period, with the default being one hour. If a PC attempts registration after a disconnect and before the timeout period has expired, the GateKeeper rejects the request.

The solutions are two:

1. Log off from the GateKeeper before disconnecting the tunnel.

2. Set the GateKeeper registration timeout value to a shorter time period. We recommend 15 minutes. Use the 'endpoint ttl' command on the Cisco GateKeeper to set this value.

RADIUS with Password Expiry

RADIUS with password expiry is an IPSec authentication method that you configure for a VPN 3002 on on the VPN Concentrator to which it connects. This option lets the VPN Concentrator that is attempting to authenticate an IPSec client to an external RADIUS server (acting as a proxy to an NT server) determine when a user's password has expired and prompt for a new password. By default, this option is disabled.

Enabling this option allows the VPN Concentrator to use MS-CHAP-v2 when authenticating an IPSec client to an external RADIUS server. That RADIUS server must support both MS-CHAP-v2 and the Microsoft Vendor Specific Attributes. Refer to the documentation for your RADIUS server to verify that it supports these capabilities.

Because of the use of MS-CHAP-v2, when this option is enabled, the VPN Concentrator can provide enhanced login failure messages that describe specific error conditions. These conditions are:

- Restricted login hours.
- Account disabled.
- No dialin permission.
- Error changing password.
- Authentication failure.

The "password expired" message appears when the user whose password has expired first attempts to log in. The other messages appear only after three unsuccessful login attempts.

Note   To use RADIUS password expiry with a VPN 3002, you must enable interactive hardware client authentication. This feature does not work for individual user authentication.

Load Balancing

Load balancing lets you distribute sessions among two or more VPN Concentrators connected on the same network to handle remote sessions. Load balancing directs sessions to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability. Load balancing requires no configuration on the VPN 3002.

Simple Certificate Enrollment Protocol (SCEP)

You can enroll and install digital certificates on the VPN 3002 automatically or manually. The automatic method is a new feature that uses the Simple Certificate Enrollment Protocol (SCEP) to streamline enrollment and installation. SCEP is a secure messaging protocol that requires minimal user intervention. This method is quicker than enrolling and installing digital certificates manually, but it is available only if you are both enrolling with a CA that supports SCEP and enrolling via the web. If your CA does not support SCEP, or if you enroll with digital certificates by a means other than the web (such as through email or by a diskette), then you cannot use the automatic method; you must use the manual method.

Reset/Restore Monitoring Statistics

You can now reset and restore statistical data to better note changes in that data. When you click Reset on a monitoring or administration screen, the system temporarily resets a counter for the chosen statistics without affecting the operation of the VPN 3002. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer. Click Restore to return to the actual statistical values.

XML Management

The VPN 3002 now supports an XML-based interface that lets you use an external management application.

Cisco management applications, third-party applications that manage our products, and customers who want to manage their devices using their own infrastructure can use this interface. This feature is enabled by default; you do not have to configure it.

The XML data can be sent to or uploaded from the VPN Concentrator using HTTPS, SSH, or standard file transfer mechanisms such as FTP or TFTP.

Reverse Route Injection (RRI)

You can configure the VPN Concentrator to add routes to its routing table for remote hardware or software clients. The VPN Concentrator can then advertise these routes to its private network via RIP or OSPF. This feature is called reverse route injection (RRI).

For example, with a VPN 3002 in network extension mode, network extension RRI automatically adds hosts on the VPN 3002 private network to the VPN Concentrator's routing table for distribution by either RIP or OSPF.

RRI requires no configuration on the VPN 3002.

AES with Diffie-Hellman Group 5

Software version 3.6 adds support for Advanced Encryption Standard (AES), which is more secure than DES and more efficient than triple DES. AES has 128-, 192-, and 256-bit key strengths. This software version also adds support for Diffie-Hellman Group 5. You select an encryption algorithm as part of IPSec configuration on the VPN Concentrator.

Push Banner to VPN 3002

An administrator can create a banner on the VPN 3000 Concentrator and push it to the VPN 3002. This lets an organization provide information to users about their network, terms for use, liability, and other issues. The banner displays only when individual user authentication is enabled.

Delete with Reason

The VPN Concentrator sends reasons for VPN Concentrator-initiated disconnects to both software clients and VPN 3002 hardware clients. The client decodes the reason, and displays it in the event log.

The VPN 3002 sends reasons for VPN3002-initiated disconnects to the VPN Concentrator at the central site. The VPN Concentrator decodes the reason, and displays it in the event log.

This feature does not work with the Cisco PIX Firewall.

This feature is active by default, but an administrator can disable it.

Memory Statistics

The VPN 3002 hardware client lets you monitor memory usage in terms of block size and free and used blocks.

Management Interfaces

The VPN 3002 offers multiple management interfaces. You can use each of these interfaces to fully configure, administer, and monitor the device.

- The VPN 3002 Hardware Client Manager is an HTML-based interface that lets you manage the system remotely with a standard web browser using one of the following:
  - HTTP connections
  - HTTPS (HTTP over SSL) secure connections
- The VPN 3002 Hardware Client command-line interface is a menu- and command-line based interface that you can use with the local system console or remotely using one of the following:
  - Telnet connections
  - Telnet over SSL secure connections
  - SSH (Secure Shell)

VPN Software Features Summary

The VPN 3002 incorporates the following software features:

VPN Feature	Description
Tunneling protocols	IPSec Protocol. The VPN 3002 uses the IKE and XAUTH protocols for secure key exchange and authentication, and to create secure VPN tunnels. The VPN 3002 can connect to the VPN Concentrator using standard IPSec, NAT-T, IPSec over TCP, or IPSec over UDP.
Encryption algorithms	• 56-bit DES (Data Encryption Standard) • 168-bit Triple DES • 128-, 192-, and 256-bit AES
Authentication algorithms	• HMAC (hashed message authentication coding) with MD5 (message digest 5) • HMAC with SHA-1 (secure hash algorithm)
Key management	• IKE (Internet Key Exchange, formerly called ISAKMP/Oakley) with Diffie-Hellman key technique
Network addressing support	• DNS (Domain Name System) • DHCP (Dynamic Host Configuration Protocol) • PPP over Ethernet (PPPoE)
Certificate authorities	• Baltimore • Entrust • Microsoft Windows 2000 • Netscape • RSA Keon • VeriSign

VPN Feature	Description
System administration	• Session monitoring and management • Backup IPSec servers • Load balancing • Software image update • System reset and reboot • Ping • Configurable system administrator profiles • File Management, including TFTP transfer • Digital certificate management
Monitoring	• Event logging and notification via system console, syslog, and SNMP traps • SNMP MIB-II support • System status • Session data • Extensive statistics

Physical Specifications

The VPN 3002 has the following physical specifications:

Width	8.85 inches (22.48 cm)
Depth	7 inches (17.78 cm)
Height	2.12 inches (5.38 cm)
Weight	2.25 lbs (1.02 kg)
External power supply	• Input: 100 to 240 VAC at 50/60 Hz (autosensing) • Output: 3.3 v @ 4 amps
Temperature	Normal operating environment, 32º to 104ºF (0º to 40ºC), convection only
Temperature	Non-operating environment, -4 to 149ºF (-20º to 65ºC)
Humidity	Normal operating environment, 5 to 95%, noncondensing
Cabling distances	Approximately 328 feet (100 meters) from an active network device
Compliance	FCC, E.U., and VCCI Class B

C H A P T E R **2**

Installing and Powering Up the VPN 3002

This chapter tells you how to prepare for, unpack, install, and power up the VPN 3002, and how to begin quick configuration.

Preparing to Install

To install the VPN 3002, you need the following skills:

- Familiarity with Windows configuration and management, and with Microsoft Internet Explorer or Netscape Navigator browsers.
- Normal computing-equipment power. For maximum protection, we recommend connecting the VPN 3002 to a conditioned power source or uninterruptible power supply (UPS). Be sure that the power source provides a reliable Earth ground.
- At least 3 inches (75 mm) of unobstructed space on all sides to accommodate cooling intake vents on the sides and top.
- Standard UTP/STP twisted-pair network cables, Category 5, with RJ-45 8-pin modular connectors. Cisco supplies two with the system.
- A standard straight-through RJ-45 serial cable with a female DB-9 connector, which Cisco supplies with the system.

Configuring and Managing the VPN 3002

You can configure and manage the VPN 3002 using the command-line interface from the console or a Telnet or SSH client. However, for ease of use, we strongly recommend using the VPN 3002 hardware Client Manager, which is HTML-based, from a PC and browser.

The PC must be able to run the recommended browser. The console can be the same PC that runs the browser.

Browser Requirements

The VPN Hardware Client Manager requires either Microsoft Internet Explorer version 4.0 or higher, or Netscape Navigator version 4.5-4.7 or 6.0. For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

JavaScript and Cookies

Be sure JavaScript and Cookies are enabled in the browser. Refer to the documentation for your browser.

Navigation Toolbar

Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh / Reload with the VPN 3002 Hardware Client Manager unless instructed to do so. To protect access security, clicking Refresh / Reload automatically logs out the Manager session. Clicking Back or Forward may display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN 3002 Hardware Client Manager.

Recommended PC Monitor / Display Settings

For ease of use, we recommend setting your monitor or display:

- Desktop area—1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette—256 colors or higher.

Unpacking

The VPN 3002 Hardware Client ships with the listed in Table 2-1. Carefully unpack your device and check your contents against this list:

Table 2-1   VPN 3002 Hardware Client Packing List

Quantity	Item
1	CVPN 3002
1	External 15W power supply and power cord
1	RJ-45 to RJ-45 console cable (black)
1	RJ45 to DB9 console port adapter
1	RJ45 to DB25 console port adapter
4	Self-adhesive rubber feet
1	Wall mount kit 2 10-16x1 & 2 10-16x1.5 screws and 2 wall anchors
1	Power cord retention bracket and instructions
1	6' RJ-45 to RJ-45 Ethernet cable (yellow)
1	VPN 3000 Concentrator Series Software CD
1	*VPN 3002 Basic Information* label
1	*VPN 3002 Quick Start* card
1	VPN Client Software License Agreement
1	*VPN 3002 Hardware Client Release Notes*
1	Export Compliance Information document

Table 2-1   VPN 3002 Hardware Client Packing List (continued)

Quantity	Item
1	Warranty card and product information packet
1	Hard copy documentation ordering flyer

Installing the VPN 3002

You can place the VPN 3002 on a table or shelf, or you can hang it on the wall.

Connecting the PC/Console

Connect the RJ45 straight-through serial cable between the console port on the back of the VPN 3002 and the COM1 or serial port on the PC.

If you are using a PC with a browser to manage the VPN 3002, be sure the PC is connected to the same private LAN as the VPN 3002.

If you are using a PC with a browser to manage the VPN 3002-8E, be sure the PC is connected to a switch port that is configured on the same private LAN as the VPN 3002-8E.

Connecting Network Cables

Connect network cables between the Ethernet interface on the back of the VPN 3002 and their respective public and private network hub, switch, or device.

The interfaces are (left to right):

  • Public = the VPN 3002 interface to the public network.

  • Private = the VPN 3002 interface to your private network (internal LAN).

Powering Up

Power up the PC/console and the VPN 3002 in the following sequence:

Step 1   Turn on the PC/console.

Step 2   If you want to use the command-line interface, start a terminal emulator (HyperTerminal) on the PC. Configure a connection to COM1, with the following port settings:

  • 9600 bits per second

  • 8 data bits

  • No parity

  • 1 stop bit

   Set the emulator for VT100 emulation, or let it autodetect the emulation type.

Step 3   Plug in the VPN 3002, which turns on the VPN 3002.

Step 4   The LED(s) on the front panel will blink and change color as the system executes diagnostics.

Step 5   Watch for these LEDs on the VPN 3002 front panel to stabilize and display as follows:

- PWR = green when unit is on.
- SYS = flashes amber when unit is performing diagnostics, flashes green until either the DHCP or PPPoE session is up (if you are using DHCP or PPPoE), and solid green when operational.
- VPN = green when tunnel is established.

Step 6   Watch for LEDs on the private and public interface ports on the back of the device to display as follows:

- Green = the interface is connected to the network.
- Flashing amber = data is traveling across the network.

   If LEDs that should be green are amber or off, see Appendix A, "Troubleshooting and System Errors."

Step 7   If connected, the console displays initialization and boot messages such as:

```
Boot-ROM Initializing...
Boot configured 16 MB of RAM.
...
Loading image ..........
Verifying image checksum ...........
Active image loaded and verified...
Starting loaded image...

Image Loader Initializing...
Decompressing & loading image ............
Verifying image checksum ...........
Active image loaded and verified...
Starting loaded image...

Starting power-up diagnostics...

pSH+ Copyright (c) Integrated Systems, Inc., 1992.
Cisco Systems, Inc./VPN 3002 Hardware Client Version 4.0(REL) Apr 06 2003 09:53:35
Features:
Initializing VPN 3002 Hardware Client ...
Initialization Complete...Waiting for Network...

Login:_
```

VPN 3002 Reset Button

The VPN 3002 includes a Reset button, so labelled, on the back of the unit. When used carefully, the Reset button resets the VPN 3002 configuration file to factory default values. That is, it eliminates both the configuration (config) file and the backup configuration (config.bak) file, and you have to perform the configuration process from the beginning.

To reset the VPN 3002 to factory default values, perform the following steps:

Step 1   Connect the VPN 3002 to a PC using the console cable, and use a hyperterminal to view the command line interface.

Step 2   Disconnect the VPN 3002 power supply cord.

Step 3   Reconnect the power supply cord.

Step 4   Immediately insert a thin, pointed object, such as an untwisted paper clip, into the reset button.

Step 5   The VPN 3002 displays messages like those below. In particular, notice the three dots (...) on the line prior to `Loading with default configuration`.

```
Resetting System...

Boot-ROM Initializing
Boot configured 16Mb of RAM.

...
Loading with default configuration.

Loading image........
Verifying image checksum.......
Active image loaded and verified...
Starting loaded image...

Image Loader Initializing...
Decompressing & load image...........
```

Step 6   Keep the paper clip in the reset button until the system displays the line, `Loading with default configuration`, just after the line with the three dots.

The VPN 3002 is rest to factory defaults.

Beginning Quick Configuration

You are now ready to begin quick configuration: configuring minimal parameters to make the VPN 3002 operational. You can use a browser for quick configuration with the VPN 3002 Hardware Client Manager (see Chapter 3, "Using the VPN 3002 Hardware Client Manager for Quick Configuration"). While you can use the console instead (see Chapter 4, "Using the Command-Line Interface for Quick Configuration"), we recommend using a browser.

Quick configuration consists of these steps:

Step 1   Set the system time, date, time zone, and Daylight Savings Time (DST) support.

Step 2   Optionally upload an already existing configuration file.

Step 3   Configure the VPN 3002 private interface. To use Network Extension mode, you must configure an IP address other than the default, which is 192.168.10.1. For Client mode, you do not need to change this address.

Step 4   Configure the DHCP server to assign IP addresses for PCs located on the private network. The default IP address pool is 192.168.10.2–192.168.10.128. For Client mode, you do not need to modify this parameter.

Step 5   Configure the VPN 3002 public interface, using DHCP, PPPoE, or static address assignment. Note that the DHCP client is enabled by default on the public interface.

Step 6   Configure the IPSec parameters with group and usernames and passwords and the IP address of the central-site VPN Concentrator, also known as the IKE peer.

Step 7   Set the VPN 3002 to use either Client or Network Extension mode. Client mode is enabled by default, using Port Address Translation (PAT).

Step 8   If you are using DNS, configure local ISP DNS information for the VPN 3002.

Step 9   Configure static routes.

Step 10   Change the **admin** password for security.

You are done!

Quick Configuration Using Default Values

The easiest way to configure the VPN 3002 is to accept default values for all parameters that have default values. The next sections on PAT mode and Network Extension mode list the information you need if you use default values for quick configuration.

PAT Mode

For PAT mode, if you accept default values for all parameters, you need:

- The IKE peer address, which is the public IP address of the VPN Concentrator to which this VPN 3002 connects.

- Group and usernames and passwords. The group and usernames and passwords must also be configured on the VPN Concentrator to which this VPN 3002 connects. On the central-site VPN Concentrator, see Configuration | User Management | Groups, and Configuration | User Management | Users.

Network Extension Mode

For Network Extension mode, if you accept default values for all parameters, you need:

- An IP address for the VPN 3002 private interface (supplied by your network administrator).

- The IKE peer address, which is the public IP address of the VPN Concentrator to which the VPN 3002 connects.

- Group and usernames and passwords. The group and usernames and passwords must also be configured on the VPN Concentrator to which this VPN 3002 connects. On the central-site VPN Concentrator, see Configuration | User Management | Groups, and Configuration | User Management | Users.

- Disable PAT.

Quick Configuration Using Nondefault Values

Table 2-2 provides the information you need to set all the parameters for quick configuration. Write your entries here now to save time as you enter data.

Table 2-2   VPN 3002 Quick Configuration Parameters

Parameter Name	Information You Need to Enter	Your Entries
Upload Config	*If you want to upload an already existing configuration file*, the path to and name of the file.	
Private Interface	Both of the following: • The IP address and subnet mask for the VPN 3002 interface to your private network. The default IP address is 192.168.10.1. Note that to use Network Extension mode, you *must* configure this private interface IP address to something other than the default. • The IP address pool range to assign, *if you use DHCP for address assignment, and you do not want to accept default values.* The default range is 192.168.10.2 to 192.168.10.128. If you change the IP address for the private interface, the default is *<Private IP address>* + 1 to *<Private IP address>* + 127.	
Public Interface	One of the following: • *If statically assigned*, the IP address, subnet mask, and default gateway for the VPN 3002 interface to the public network. • *If you use DHCP to obtain an IP address*, a system name (also called a hostname). • *If you use PPPoE to connect to a public network*, a PPPoE username and password.	
IPSec *If you use digital certificates, you do not need to enter this information.*	Both of the following: • The IKE peer address, that is, the IP address for the public interface of the central-site VPN Concentrator to which this VPN 3002 connects. • IPSec group names, usernames, and passwords. These must match the group names, usernames, and passwords configured on the central-site VPN Concentrator.	
PAT	*If you want to use Network Extension mode*, an IP address for the private interface other than the default.	
DNS	*If you use DNS*, both of the following: • The IP address of your local Internet Service Provider's DNS server. • The registered Internet domain name to use with DNS (such as cisco.com), obtained from your Internet Service Provider (ISP).	
Static Routes	*If you want to configure one or more static routes*, the IP address(es), subnet mask(s), and metric(s) that apply to the static route(s), and destination router address(es).	

Using the VPN 3002 Hardware Client Manager for Quick Configuration

This chapter tells you how to complete quick configuration of the system using the VPN 3002 Hardware Client Manager.

The VPN 3002 Hardware Client Manager is an HTML-based configuration, administration, and monitoring system built into the VPN 3002. To use it, you need only connect to the VPN 3002 using a PC and browser on the same private network as the VPN 3002.

As you proceed, refer to the data you recorded in Table 2-2.

The figures that follow show only the main frame of the Manager window. To use features in the other frames, see the "Understanding the VPN 3002 Hardware Client Manager Window" section.

Logging into the VPN 3002 Hardware Client Manager

Access and log into the VPN 3002 Hardware Client Manager using these steps:

Step 1 Start the browser. See the "Browser Requirements" section. We recommend using Microsoft Internet Explorer for best results. Maximize the browser window for easiest reading.

Step 2 With the browser, connect to the IP address of the VPN 3002 on your private interface. Enter the IP address (for example, 192.168.10.1) in the Address or Location field. The browser displays the login screen.

The Manager displays the VPN 3002 Hardware Client Manager Loginscreen.

Figure 3-1   VPN 3002 Hardware Client Login Screen

Step 3   Log in. Entries are case-sensitive, so type them exactly as shown. With Microsoft Internet Explorer, you can click the Tab key to move from field to field; with other browsers, you may have to change fields with the mouse. If you make a mistake, click the Clear button and start over.

- Click in the Login field and type admin. (Do not press Enter.)
- Click in the Password field and type admin. (The field shows *****.)
- Click the Login button.

Starting Quick Configuration

The Manager displays the VPN 3002 Hardware Client Manager Main screen.

Figure 3-2   VPN 3002 Hardware Client Manager Main Screen
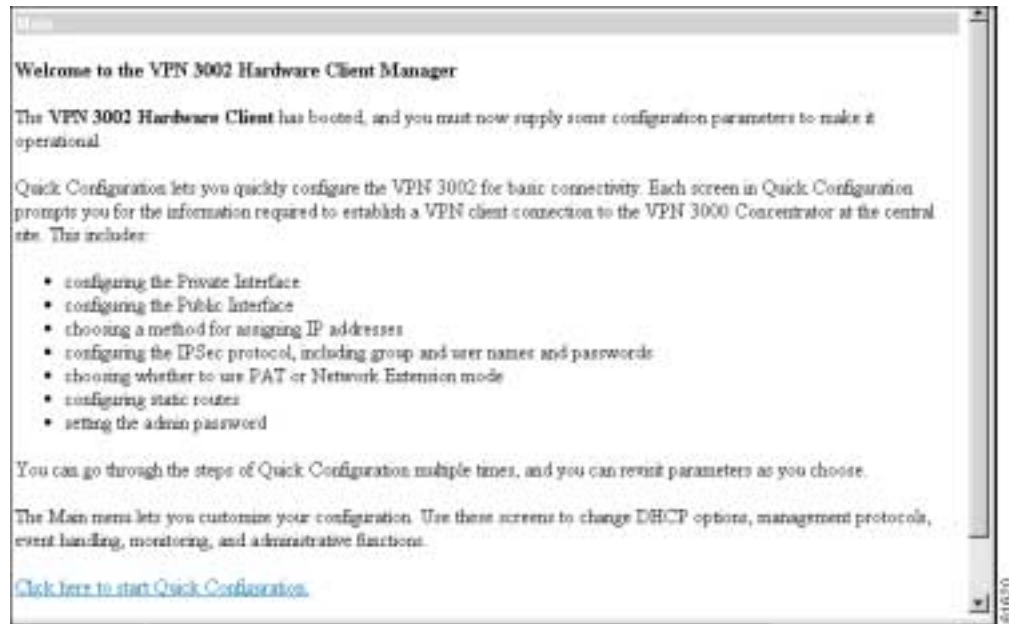
To start quick configuration, click the underlined link that says *Click here to start Quick Configuration*. The Manager displays the Time and Date screen, which is the first of the quick configuration screens.

About Quick Configuration

Text entries are case-sensitive; that is, admin and ADMIN are different passwords.

After you make an entry in a field, do not press the keyboard Enter key. Just move the cursor from field to field. With Microsoft Internet Explorer, you can press the Tab key to move from field to field; other browsers may work differently.

On any screen where it appears, click the **Back** button to return to the previous screen.

Configuration entries take effect as soon as you click the **Apply** or **Continue** button, and they constitute the active or running configuration.

The banner across the top of the screen indicates the parameter currently displayed, both by showing in the top line the complete path to that parameter, for example, Configuration | Quick | Time and Date, and also by highlighting an abbreviated name of the parameter in the line below, such as Time. For configured parameters, the Manager adds a checkmark to the side of its abbreviated name.

You can go through the steps of quick configuration as many times as you want, and you do not have to proceed sequentially. You can also revisit individual parameters. To reach a screen, click either

- the abbreviated parameter name at the top of the screen.

- the Back button to return to a previous screen.

If you make a mistake and see an Error screen with the message, "An error has occurred while attempting to perform the operation," and you return to the screen where you were working, carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost. See Appendix A, "Troubleshooting and System Errors" for more details.

Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh / Reload with the VPN 3002 Hardware Client Manager unless instructed to do so. To protect access security, clicking Refresh / Reload automatically logs out the Manager session. Clicking Back or Forward may display stale Manager screens with incorrect data or settings. We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN Hardware Client Manager.

Setting the Time and Date

The Manager displays the Configuration | Quick | Time and Date screen.

Figure 3-3   VPN 3002 Configuration | Quick | Time and Date Screen.
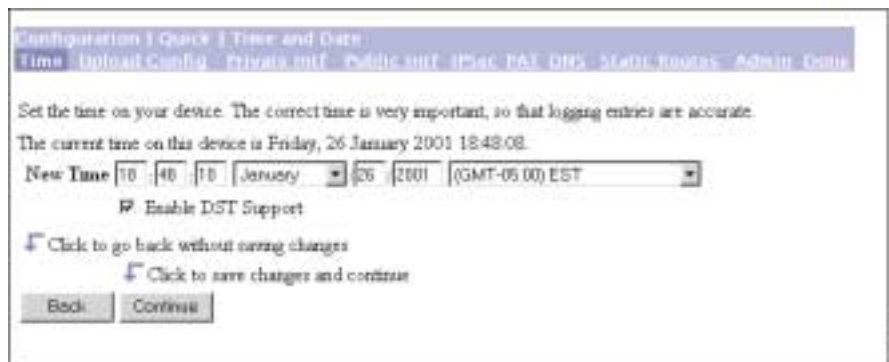
This screen lets you set the time and date on this device.

Step 1   The screen shows the current time and date on the device. The values in the New Time fields are the time on the browser PC, but any entries you make apply to the VPN 3002.

- Use the pull-down menus to make any changes. The fields are, in order: **Hour : Minute : Second AM/PM Month / Day / Year Time Zone**.

- The time zone selections are offsets in hours relative to Greenwich Mean Time (GMT), which is the basis for Internet time synchronization. Enter the Year as a four-digit number.

- To enable DST Support, check the box. During Daylight-Saving Time (DST), clocks are set one hour ahead of standard time. Enabling DST support means that the VPN 3002 automatically adjusts the time zone for DST or standard time. If your system is in a time zone that uses DST, you must enable DST support.

Step 2   Click Continue to save your changes and proceed with quick configuration.

Uploading an Existing Configuration File

The Manager displays the Configuration | Quick | Upload Config screen.

Figure 3-4   VPN 3002 Configuration | Quick | Upload Config Screen

This feature enables you to use HTTP or HTTPS to transfer (upload) configuration files from your PC, or from a system accessible to your PC, to the VPN 3002 flash memory.

Step 1   If you do not want to upload a configuration file, click **No**, and continue to the next section.

Step 2   To upload an already existing configuration file, click **Yes**.

The Manager displays the Configuration | Quick | Upload Config | Browse screen.

Figure 3-5   VPN 3002 Configuration | Quick | Upload Config | Browse Screen

.

Step 1   In the Config File field, either enter the path to or use the Browse button to find the path to and name of the configuration file you want to upload.

Step 2   Click **Upload** to use this file as your configuration file, or click **Back** to return to the Configuration | Quick | Upload Config screen.

Configuring the Private Interface

The VPN 3002 Configuration | Quick | Private Interface screen displays.

Figure 3-6   Configuration | Quick | Private Interface Screen
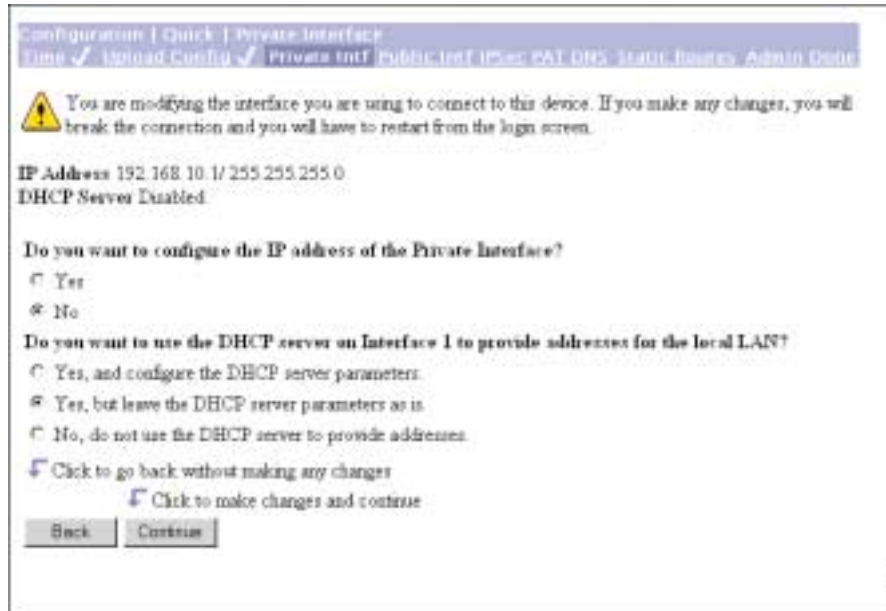
This screen lets you configure the VPN 3002 private interface, which is the interface to your private network (internal LAN).

The screen displays the current configuration settings.

> **Note**   For the VPN 3002 to operate in Network Extension mode, you must change the private interface IP address from the default of 192.168.10.1.

> **Caution**   If you modify any parameters of the interface that you are currently using to connect to the VPN 3002, you will break the connection, and you will have to restart the Manager and quick configuration from the login screen.

Step 1   To reconfigure the IP address for the private interface, select **Yes**. The Manager displays the Configuration | Quick | Private Interface | Address screen. See Figure 3-7 and perform the steps in that section.

Step 2   To use the VPN 3002 DHCP server to provide addresses for the local LAN, select one of the Yes options. If you select Yes, and configure the DHCP server parameters, the Manager displays the Configuration | Quick | Private Interface | DHCP Server screen. See Figure 3-8 and perform the steps in that section.

Step 3   When you have made your selections, click **Continue** to apply your changes and proceed. Click **Back** if you do not want to save your changes; you return to the Configuration | Quick | Private Interface screen.

Configuration | Quick | Private Interface | Address

The Configuration | Quick | Private Interface | Address screen lets you enter a new IP address and subnet mask for the private interface.

Figure 3-7   Configuration | Quick | Private Interface | Address Screen

Step 1   In the IP Address field, enter the IP address for this interface, using dotted decimal notation (for example, `192.168.12.34`). Be sure no other device is using this address on the network.

Step 2   In the Subnet Mask field, enter the subnet mask for this interface, using dotted decimal notation (for example, `255.255.255.0`). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, an IP address of `192.168.12.34` is a Class C address, and the standard subnet mask is `255.255.255.0`. You can accept this entry or change it.

Step 3   Click **Continue** to save your changes. You must now restart the Manager and quick configuration from the login screen.

Click **Back** if you don't want to save your changes. You return to the Configuration | Quick | Private Interface screen.

Configuration | Quick | Private Interface | DHCP Server

The Configuration | Quick | Private Interface | DHCP Server screen lets you enable and configure the VPN 3002 to serve as a Dynamic Host Configuration Protocol (DHCP) server for the private network.

The DHCP server for the Private interface lets IP hosts in its network automatically obtain IP addresses from a limited pool of addresses for a fixed length of time, or lease period. Before the lease period expires, the VPN 3002 displays a message offering to renew it. If the lease is not renewed, the connection terminates when the lease expires, and the IP address becomes available for reuse. Using DHCP simplifies configuration since you do not need to know what IP addresses are considered valid on a particular network.

Figure 3-8   Configuration | Quick | Private Interface | DHCP Server Screen

Step 1   Check the **Enabled** box to enable DHCP services for this interface.

Step 2   In the Lease Timeout field, enter the amount of time, in minutes, that DHCP clients own the IP address the DHCP server assigns. The minimum is 5, maximum is 500,000 and default is 120 minutes.

The Lease Timeout period you configure applies only when the tunnel to the VPN Concentrator is established. When the tunnel is not established, the Lease Timeout period is 5 minutes.

Step 3   In the Address Pool Start/End fields enter the range of IP addresses that this DHCP server can assign, using dotted decimal notation (for example, 10.10.99.51 - 10.10.99.178). Be sure no other device is using these addresses on the network. The default address pool is 127 IP addresses, and the start of the range is next IP address after that of the private interface. You can configure another range of IP addresses for the pool, but in no case can the pool have more than 127 addresses.

Step 4   Click **Continue** to save your changes.The Manager displays the Configuration | Quick | Private Interface | DHCP server address pool screen.

Figure 3-9   Configuration | Quick | Private Interface | DHCP Server Address Pool Screen

This screen confirms the DHCP server address pool range you entered.

Step 5   Click **Continue** to apply your choice and proceed. Click **Back** to return to the Configuration | Quick | Private Interface | DHCP Server screen.

Step 6   You might need to restart the Manager and quick configuration from the login screen.

Configuring the Public Interface

The Manager displays the Configuration | Quick | Public Interface screen.

Figure 3-10   Configuration | Quick | Public Interface Screen

The public interface can obtain an IP address in one of three ways: using DHCP, PPPoE, or by static addressing. You configure *one* of these methods; depending on the method you choose, complete Step 2, *or* Steps 3 and 4, *or* Steps 5–8.

Step 1   Assign a System Name, also known as a hostname. This is optional unless you use DHCP to obtain an IP address *and* your ISP requires a hostname.

Step 2   To have the DHCP server assign the public interface IP address, subnet mask, and default gateway, accept the default value, **Obtain an IP address from a DHCP server**.

Step 3   To have Point-to-Point Protocol over Ethernet (PPPoE) establish the connection between the VPN 3002 and the central-site VPN Concentrator, select **Use PPPoE to connect to a public network**.

Step 4   For a PPPoE connection, enter the PPPoE username and password. Verify the password by reentering it. The maximum number of characters for either username or password is 64.

Step 5   To assign a static IP address, subnet mask, and default gateway, select **Specify an IP address**.

Step 6   To specify an IP address, in the IP Address field, enter the IP address for this interface, using dotted decimal notation (for example, 192.168.12.34). Be sure no other device is using this address on the network.

Step 7   If you specify an IP address, in the Subnet Mask field, enter the subnet mask for this interface, using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, an IP address of 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it.

Step 8   If you specify an IP address, in the Default Gateway field, enter the IP address or hostname of the system to which the VPN 3002 should forward packets that do not have a static route. The default gateway must be accessible from the VPN 3002 public network. If you are using DHCP to acquire the public IP address, DHCP usually supplies the default gateway, and you should leave this field blank.

To specify no default gateway—which means the VPN 3002 drops unrouted packets—leave this field at 0.0.0.0.

Step 9   Click **Continue** to apply your choices to the interface and proceed. Click **Back** to return to the Configuration | Quick | Private Interface screen.

See the sections that follow for more information about DHCP, PPPoE, and static addressing.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets IP hosts in its network automatically obtain IP addresses from a limited pool of addresses for a fixed length of time, or lease period. Using DHCP simplifies configuration since you can manage the assignment of IP addresses from a central point. You do not need to manually enter an IP address for the public interface, and you do not need to know what IP addresses are considered valid on a particular network.

The DHCP server for the Public interface resides on the public network.

PPPoE

PPP over Ethernet (PPPoE) is a proposal that specifies how a network client interacts with a service provider's equipment, such as a broadband modem—xDSL, cable, or wireless—to achieve access to high-speed data networks. It relies on the Ethernet and PPP standards. It includes an authentication strategy that requires a username and password to create a PPPoE session on the VPN 3002.

If a PPPoE session fails due to a PPP authentication failure, the VPN 3002 does not attempt a new session until 30 seconds have passed.

Specify an IP address

This option enables you to set a static IP address, subnet mask, and default gateway for the public interface.

Configuring IPSec

After you click **Continue** to apply your changes to the Public Interface parameters, the Manager displays the Configuration | Quick | IPSec screen.

Figure 3-11   Configuration | Quick | IPSec Screen

This screen lets you configure the IPSec parameters. IPSec is the protocol that enables the VPN 3002 to connect to the VPN Concentrator over a secure VPN tunnel. The VPN 3002 can also establish IPSec tunnels to other IPSec security gateways, including the Cisco PIX firewall, and Cisco IOS routers.

Step 1   In the Remote Server field, enter the IP address or hostname of the VPN Concentrator to which this VPN 3002 hardware client connects. Note that to enter a hostname, a DNS server must be configured.

Step 2   Check the IPSec over TCP box if you want to connect using IPSec over TCP. This feature must also be enabled on the VPN Concentrator to which this VPN 3002 connects.

Step 3   Enter the IPSec over TCP port number. You can enter only one port. The port that you configure on this VPN 3002 must also be configured on the VPN Concentrator to which this VPN 3002 connects.

> **Note**   If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning to notify you that the protocol associated with that port will no longer work on the public interface, with the consequence that you can no longer use a browser to manage the VPN 3002 through the public interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

Step 4   Check the Use Certificate box to use digital certificates for authentication. If you are using digital certificates, there is no need to enter a group name and group password.

Step 5   Select a Certificate Transmission option. If you want the VPN 3002 to send the peer the identity certificate and all issuing certificates (including the root certificate and any subordinate CA certificates), click **Entire certificate chain**. If you want to send the peer only the identity certificate, click **Identity certificate only**.

Step 6 If you are not using digital certificates, in the Group Name field, enter a unique name for this group (maximum is 32 characters, case-sensitive). This is the same group name that you configure for this VPN 3002 on the central-site VPN Concentrator.

Step 7 If you are not using digital certificates, in the Group Password field, enter a unique password for this group (minimum is 4 characters, maximum is 32, case-sensitive). This is the same group password that you configure for this VPN 3002 on the central-site VPN Concentrator. The field displays only asterisks.

Step 8 In the Group Verify field, reenter the group password to verify it. The field displays only asterisks.

Step 9 If you are not using digital certificates, in the User Name field, enter a unique name for the user in this group (maximum is 32 characters, case-sensitive). This is the same username that you configure for this VPN 3002 on the central-site VPN Concentrator.

Step 10 In the User Password field, enter the password for this user (maximum is 32 characters). This is the same user password that you configure for the VPN 3002 on the central-site VPN Concentrator.

Step 11 In the User Verify field, reenter the user password to verify it. The field displays only asterisks.

Note When you enable interactive hardware client authentication for a group, the VPN Concentrator pushes that policy to the VPN 3002s in the group. If you set a username and password on the VPN 3002 and later enable interactive hardware client authentication for the group to which the VPN 3002 belongs, the software deletes the username and password from the configuration file, and from the password field in the html interface. When you try to connect, the software prompts you for a username and password.

Step 12 Click **Continue** to apply your changes and proceed. Click **Back** if you want to return to the Configuration | Quick | Public Interface screen.

Configuring PAT or Network Extension Mode

The Manager displays the Configuration | Quick | PAT screen.

Figure 3-12   Configuration | Quick | PAT Screen
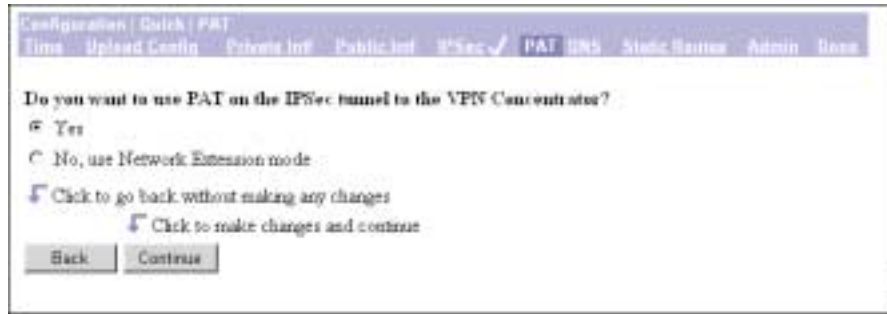
You use this screen to configure this VPN 3002 to use either PAT or Network Extension mode.

Step 1   Accept the default, Yes, if you want to use PAT. Otherwise, check **No, use Network Extension mode**. Note that you cannot disable PAT if you have not changed the IP address for the private interface.

Step 2   Click **Continue** to proceed with quick configuration, or click **Back** to return to the Configuration | Quick | IPSec screen.

See the sections below for more information about PAT and Network Extension mode.

Online Technical Snapshot Explains PAT and Network Extension Modes

To view a brief interactive multimedia piece that explains the differences between the two modes, go to this url:

http://www.cisco.com/mm/techsnap/VPN3002_techsnap.html

Your web browser must be equipped with a current version of the Macromedia Flash Player to view the content. If you are unsure whether your browser has the most recent version, you may want to download and install a free copy from:

http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash

Client Mode (PAT)

Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the VPN 3002 private network from those on the corporate network. In PAT mode:

- IPSec encapsulates all traffic going from the private network of the VPN 3002 to the network(s) behind the Internet Key Exchange (IKE) peer, that is, the central-site VPN Concentrator.

- PAT mode employs NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the IP address of the VPN 3002 public interface. The central-site VPN Concentrator assigns this address. NAT also keeps track of these mappings so that it can forward replies to the correct device.

All traffic from the private network appears on the network behind the central-site VPN Concentrator (the IKE peer) with a single source IP address. This IP address is the one the central-site VPN Concentrator assigns to the VPN 3002. The IP addresses of the computers on the VPN 3002 private network are hidden. You cannot ping or access a device on the VPN 3002 private network from outside of that private network, or directly from a device on the private network at the central site.

Client Mode with Split Tunneling

You assign the VPN 3002 to a client group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec and PAT are applied to all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator.

Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the assigned IP address of the public interface and also keeps track of these mappings so that it can forward replies to the correct device.

The network and addresses on the private side of the VPN 3002 are hidden, and cannot be accessed directly.

VPN Concentrator Settings Required for PAT

For the VPN 3002 to use PAT, you must meet these requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.x or later.

2. Address assignment must be enabled, by whatever method you choose to assign addresses (the options are DHCP, address pools, per user, or client-specified). If the central-site VPN Concentrator uses address pools for address assignment, make sure to configure the address pools your network requires. Refer to the chapter, "Address Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

3. Configure a group to which you assign this VPN 3002. This includes assigning a group name and password. Refer to the chapter, "User Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

4. Configure one or more users for the group, including usernames and passwords.

Network Extension Mode

Network Extension mode allows the VPN 3002 to present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the VPN 3002 private network to networks behind the central-site VPN Concentrator. PAT does not apply. Therefore, devices behind the VPN Concentrator have direct access to devices on the VPN 3002 private network over the tunnel, and only over the tunnel, and vice versa. The VPN 3002 must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

In this mode, the central-site VPN Concentrator does not assign an IP address for tunneled traffic (as it does in Client/PAT mode). The tunnel is terminated with the VPN 3002 private IP address (the assigned IP address). To use Network Extension mode, you must configure an IP address other than the default of 192.168.10.1 and disable PAT.

In Network Extension mode, the VPN 3002 automatically attempts to establish a tunnel to the VPN Concentrator. However, if you enable interactive unit authentication in either Client or Network Extension mode, the tunnel establishes when you perform the following steps.

Step 1   Click the **Connection/Login Status** button on the VPN 3002 Hardware Client login screen. The Connection/Login screen displays.

Step 2   Click **Connect Now** in the Connection/Login screen.

Step 3   Enter the username and password for the VPN 3002.

Alternatively, you can initiate a tunnel by clicking **Connect Now** on the in the Monitoring | System Status screen.

Network Extension Mode per Group

VPN Concentrator software versions 3.6 and later let a network administrator restrict the use of network extension mode. On the VPN Concentrator, you enable network extension mode for VPN 3002 hardware clients on a group basis.

Note   If you disallow network extension mode, which is the default setting on the VPN Concentrator, the VPN 3002 can connect to that VPN Concentrator in PAT mode only. In this case, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 will attempt to connect every 4 seconds, and every attempt will be rejected; this is the equivalent of denial of service attack.

Network Extension Mode with Split Tunneling

You always assign the VPN 3002 to a client group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec operates on all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator. PAT does not apply.

Traffic from the VPN 3002 to any other destination than those within the network list on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices on the VPN 3002 private network to the address of the VPN 3002 public interface. Thus the network and addresses on the private side of the VPN 3002 are accessible over the tunnel, but are protected from the Internet, that is, they cannot be accessed directly.

VPN Concentrator Settings Required for Network Extension Mode

For the VPN 3002 to use Network Extension mode, you must meet these requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.x or later.

2. Configure a group to which you assign this VPN 3002. This includes assigning a group name and password. Refer to the chapter, "User Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

3. Configure one or more users for the group, including usernames and passwords.

4. Configure either a default gateway or a static route to the VPN 3002 private network. Refer to the chapter, "IP Routing," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

5. If you want the VPN 3002 to be able to reach devices on other networks that connect to the VPN Concentrator, review your Network Lists. Refer to the chapter, "Policy Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

6. For version 3.6, check the box in the Allow Network Extension mode parameter for the Group (IPSec tab).

Tunnel Initiation

The VPN 3002 always initiates the tunnel to the central-site VPN Concentrator. The central-site VPN Concentrator cannot initiate a tunnel to a VPN 3002. The VPN 3002 creates only one IPSec tunnel to the central-site VPN Concentrator, in either PAT or Network Extension mode. The tunnel can support multiple encrypted data streams between users behind the VPN 3002 and the central site. With split tunneling enabled, it can also support multiple unencrypted data streams to the internet.

In PAT mode, the tunnel establishes when data passes to the VPN Concentrator, or when you click **Connect Now** in the Monitoring | System Status screen.

In Network Extension mode, the VPN 3002 automatically attempts to establish a tunnel to the VPN Concentrator.

Tunnel Initiation with Interactive Unit Authentication

In either Client or Network Extension mode, when you enable interactive unit authentication, the tunnel establishes when you perform the following steps.

Step 1   In the VPN 3002 Hardware Client login screen, click the **Connection/Login Status** button. The Connection/Login screen displays.

Step 2   Click **Connect Now**.

Step 3   Enter the username and password for the VPN 3002.

Refer to the section, "Logging in With Interactive Unit and Individual User Authentication," in Chapter 1 of the *VPN 3002 Hardware Client Reference* for detailed instructions.

Alternatively, you can click **Connect Now** on the in the Monitoring | System Status screen, after which the system prompts you to enter the username and password for the VPN 3002. Refer to the section, Monitoring | System Status in the "Monitoring" chapter of the *VPN 3002 Hardware Client Reference* for detailed instructions.

Data Initiation

After the tunnel is established between the VPN 3002 and the central-site VPN Concentrator, the VPN Concentrator can initiate data exchange only in Network Extension mode with all traffic travelling through the tunnel. If you want the tunnel to remain up indefinitely, you should configure the VPN 3002 for Network Extension mode and not use split tunneling.

Table 3-1 summarizes instances in which the VPN 3002 and the central-site VPN Concentrator can initiate data exchange.

Table 3-1   Data Initiation: VPN 3002 and Central-Site VPN Concentrator

Mode	Tunneling Policy	VPN 3002 Can Send Data First	Central-Site VPN Concentrator Can Send Data First (after VPN 3002 initiates the tunnel)
PAT	All traffic tunneled	Yes	No
PAT	Split tunneling enabled	Yes	No
Network Extension	All traffic tunneled	Yes	Yes
Network Extension	Split tunneling enabled	Yes	No

Configuring DNS

The Manager displays the Configuration | Quick | DNS screen.

Figure 3-13   Configuration | Quick | DNS Screen

This screen lets you specify a Domain Name System (DNS) server for your local ISP, which lets you enter Internet hostnames (for example, `mail01`) rather than IP addresses for servers as you configure and manage the VPN 3002. While hostnames are easier to remember, using IP addresses avoids problems that might occur with the DNS server offline or congested. If you use a hostname to identify the central-site VPN Concentrator, you must configure a DNS server on the VPN 3002 (see Configuration | System | Servers | DNS).

Step 1   In the DNS Server field, enter the IP address of your local DNS server, using dotted decimal notation (for example, 10.10.0.11).

Step 2   In the Domain field, enter the local ISP domain name.

Step 3   Click **Continue** to proceed.

Configuring Static Routes

The Manager displays the Configuration | Quick | Static Routes screen. The Static Routes list shows manual IP routes that have been configured. The format is [destination network address/subnet mask -> outbound destination].

Figure 3-14   Configuration | Quick | Static Routes Screen

You use this screen to add or delete static routes for IP routing.

Step 1   Click **Add** to add a route to the routing table. The Manager displays the Configuration | Quick | Static Routes | Add screen.

Step 2   To delete a route, select it, and click **Delete**. The Manager deletes the route instantly, and there is no confirmation.

Step 3   Click **Continue** to proceed.

Adding a Static Route

This screen lets you add a new static route to the IP routing table.

Figure 3-15 Configuration | Quick | Static Routes | Add Screen

Step 1 In the Network Address field, enter the network IP address for this static route. Packets with this address will be sent to the Destination below. Use dotted decimal notation; for example, 192.168.12.0.

Step 2 In the Subnet Mask field, enter the subnet mask for the network IP address, using dotted decimal notation (such as 255.255.255.0). The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it.

Step 3 In the Metric field, enter the cost for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Step 4 In the Destination Router Address or Interface fields, click a radio button to select the outbound destination for these packets. You can select only one destination: either a specific router or gateway, or a VPN 3002 interface.

For Router Address, enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN 3002 and the packet's ultimate destination. Use dotted decimal notation; for example, 10.10.0.2.

For Interface, click the drop-down menu button and select a configured VPN 3002 interface as the outbound destination.

Step 5 To add a new static route to the list of configured routes, click **Add**. The new route displays at the bottom of the Static Routes list.

To discard your entry, click **Cancel**. The Manager returns to the Configuration | Quick | Static Routes screen, and the Static Routes list is unchanged.

Changing admin Password

The Manager displays the Configuration | Quick | Admin Password screen.

Figure 3-16   Configuration | Quick | Admin Password | Screen

This screen lets you change the password for the admin administrator user. For ease of use during startup, the default admin password supplied with the VPN 3002 is also admin. Since the admin user has full access to all management and administration functions on the device, *we strongly recommend you change this password to improve device security.* You can further configure all administrator users on the regular Administration | Access Rights | Administrators Manager screen.

Step 1   In the Password field, enter a new password. For maximum security, the password should be at least 8 characters long, a mixture of upper- and lower-case alphabetic and numeric characters, and not easily guessed; for example, `W8j9Haq3`. (The field shows only asterisks.)

Step 2   In the Verify field, reenter the new password to verify it.

Step 3   Click **Continue** to proceed.

Finishing Quick Configuration

The Manager displays the Configuration | Quick | Done screen.

Figure 3-17   Configuration | Quick | Done Screen

You have finished quick configuration, and your entries constitute the active or running configuration. *This configuration has now been saved as the boot configuration.* The VPN 3002 now has enough information, and it is operational. The VPN 3002 can now establish a secure VPN tunnel to the central-site VPN Concentrator.

What Next?

Now that the VPN 3002 is operational, you can:

- Explore the Manager window and other VPN 3002 functions; see the "Using Other VPN 3002 Hardware Client Manager Functions" section.

- Proceed to a more detailed and complete system configuration. Refer to the *VPN 3002 Hardware Client Reference* for assistance (online only).

Using Other VPN 3002 Hardware Client Manager Functions

To use other VPN 3002 Hardware Client Manager functions, click the section you want in the left frame of the Manager window or on the Manager toolbar in the top frame of the Manager window.

- **Configuration**—Configures all the features of the VPN 3002.

- **Administration**—Controls administrative functions of this device.

- **Monitoring**—Displays status, statistics, and event logs on this device.

- **Save, Save Needed**—Saves the active configuration and makes it the boot configuration.

- **Main**—Returns to the main Manager screen.

- **Help**—Opens another browser window and lets you view online help for the current Manager screen.

- **Support**—Opens a Manager screen with links to Cisco support and documentation resources.

- **Logout**—Logs out of this Manager session and returns to the login screen.

For details on the frames, functions, and icons in the Manager window, see the next section, "Understanding the VPN 3002 Hardware Client Manager Window."

For details on the VPN 3002 hardware, all the functions available in the VPN 3002 Hardware Client Manager, or using the command-line interface, refer to the *VPN 3002 Hardware Client Reference* (online only).

Understanding the VPN 3002 Hardware Client Manager Window

The VPN 3002 Hardware Client Manager window on your browser consists of three frames—top, left, and main—and it provides helpful messages and tips as you move the mouse pointer over window items. The title bar and status bar also provide useful information.

Figure 3-18   VPN 3002 Hardware Client Manager Window
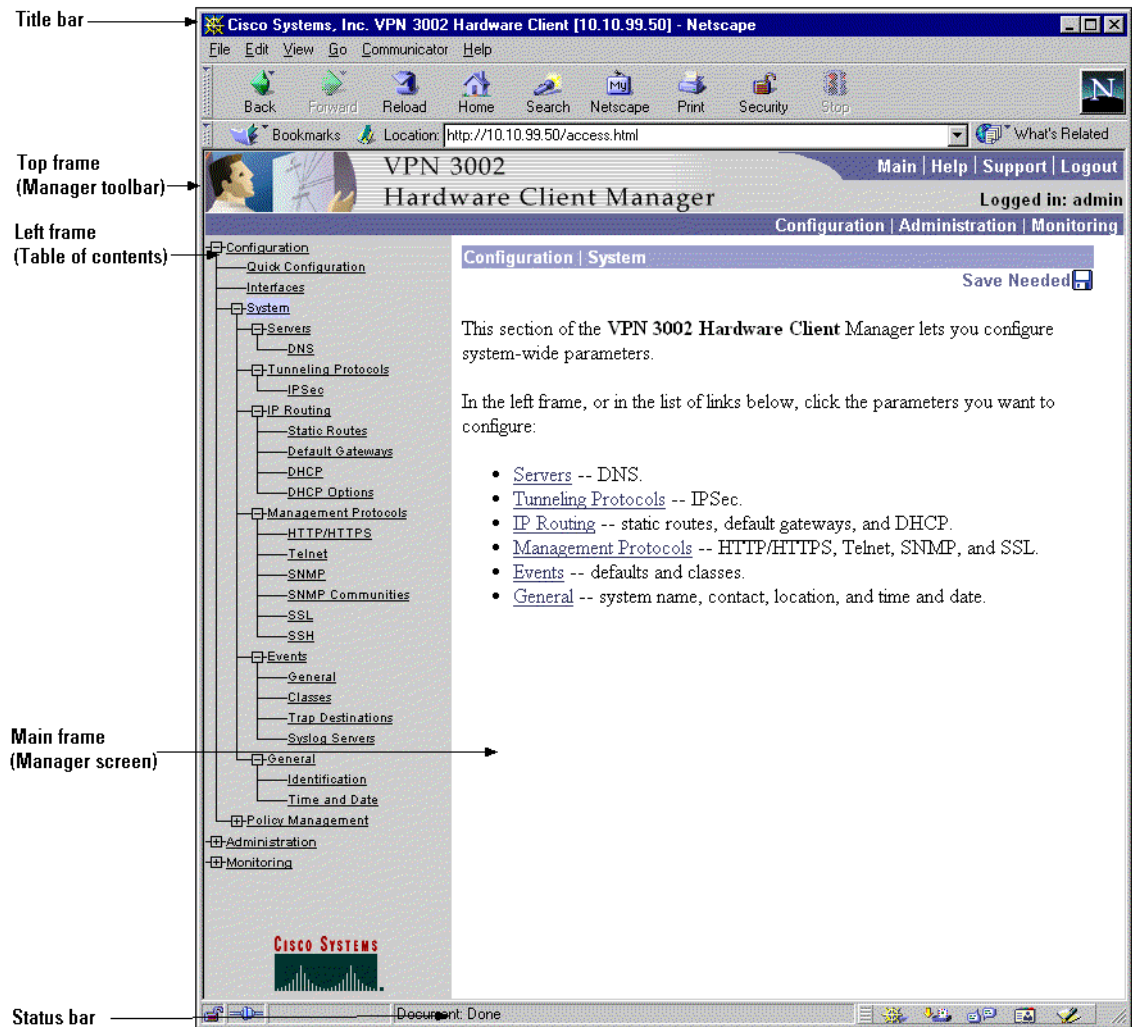
Title bar	The title bar at the top of the browser window includes the VPN 3002 device name or IP address in brackets, for example, [10.10.4.6].
Status bar	The status bar at the bottom of the browser window displays Manager activity and explanatory messages for some items.

Mouse pointer and tips	As you move the mouse pointer over an active area, the pointer changes shape and icons change color. A description also appears in the status bar area. If you momentarily rest the pointer on an icon, a descriptive tip appears for that icon.
Top frame (Manager toolbar)	The Manager toolbar in the top frame provides quick access to Manager features. These include the following icons:
Main	Click the Main tab to go to the main Manager screen, and to close all subordinate sections and titles in the left frame.
Help	Click the Help tab to open context-sensitive online help. Help opens in a separate browser window that yo can move or resize as you want. Close the help window when you are finished.
Support	Click the Support tab to open a Manager screen with links to Cisco support and documentation resources.
Logout	Click the Logout tab to log out of the Manager and return to the login screen.
Logged in: [username]	The administrator username you used to log in to this Manager session.
Configuration	Click the Configuration tab to go to the main Configuration screen, to open the first level of subordinate Configuration pages in the left frame if they are not already open, and to close any open Administration or Monitoring pages in the left frame.
Administration	Click the Administration tab to go to the main Administration screen, to open the first level of subordinate Administration pages in the left frame if they are not already open, and to close any open Configuration or Monitoring pages in the left frame.
Monitoring	Click the Monitoring tab to go to the main Monitoring screen, to open the first level of subordinate Monitoring pages in the left frame if they are not already open, and to close any open Configuration or Administration pages in the left frame.
Save 🖫	Click the Save icon to save the active configuration and make it the boot configuration. In this state, the reminder indicates that the active configuration is the same as the boot configuration, but you can save it anyway. When you change the configuration, the reminder changes to Save Needed.

Save Needed 💾

This reminder indicates that yo have changed the active configuration. Click the Save Needed icon to save the active configuration and make it the boot configuration. As you make configuration entries, they take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN 3002 without saving the active configuration, and configuration changes are lost. Clicking on this reminder saves the active configuration as the boot configuration and restores the **Save** reminder.

Refresh 🔄

Click the Refresh icon to refresh (update) the screen contents on screens where it appears (mostly in the Monitoring section). The date and time above this reminder indicate when the screen was last updated.

Reset

Click the Reset icon to reset, or start anew, the screen contents on screens where it appears (mostly in the Monitoring section).

Restore

Click the Restore icon to restore the screen contents to their status prior to when you last clicked the Reset icon.

CISCO SYSTEMS

Click the Cisco Systems logo to open a browser and go to the Cisco.com web site, www.cisco.com

**Left frame
(Table of Contents)**

On Manager screens, the left frame provides a table of contents. The table of contents uses the familiar Windows Explorer metaphor of collapsed and expanded entries.

**Main section titles
(Configuration, Administration, Monitoring**

Click a title to open subordinate sections and titles, and to go to that Manager screen in the main frame.

Closed or collapsed ⊞

Click the closed/collapsed icon to open subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.

Open or expanded ⊟

Click the open/expanded icon to close subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.

**Main frame
(Manager screen)**

The main frame displays the current VPN 3002 Hardware Client Manager screen.

Many screens include a bullet list of links and descriptions of subordinate sections and titles. you can click a link to go to that Manager screen, and open subordinate sections and titles in the table of contents.

Using the Command-Line Interface for Quick Configuration

This chapter tells you how to complete quick configuration of the system using the VPN 3002 command-line interface (CLI).

Quick configuration supplies the minimal parameters needed to make the VPN3002 operational.

The CLI is a menu-based configuration, administration, and monitoring system built into the VPN 3002. You can use it from the console or in a Telnet or SSH session.

As you proceed, refer to the data you recorded in Table 2-2 on page 2-7.

About Quick Configuration

You can go through quick configuration multiple times, and although it is easiest to configure its parameters in sequence, you can set and revisit parameters in whatever order you choose.

Entries are case-sensitive; for example, `admin` and `ADMIN` are different passwords.

The system displays more tips and examples than appear in the dialog here.

The system shows current or default entries in brackets; for example, `[ 10.10.4.6 ]`.

After each entry, press the **Enter** key on the console keyboard.

Configuration entries take effect as soon as you enter them, and they constitute the active, or running, configuration. The system automatically saves your entries when you press the **Enter** key.

If you make a mistake, the system displays an error message and repeats the previous prompt. You can often enter a correct value and proceed, but in some cases you may need to restart the section to correct an earlier error. See Appendix A, "Troubleshooting and System Errors" for more details.

Starting Quick Configuration

To use the command-line interface (CLI) for quick configuration of the VPN 3002:

Step 1   After booting the VPN 3002, start either the console or a Telnet or SSH session, and connect to the private interface of the VPN 3002 by entering the IP address for that interface.

The system displays initialization and boot messages such as:

```
Boot-ROM Initializing...
Boot configured 16 MB of RAM.

...
Loading image ..........
Verifying image checksum ...........
Active image loaded and verified...
Starting loaded image...

Image Loader Initializing...
Decompressing & loading image ............
Verifying image checksum ...........
Active image loaded and verified...
Starting loaded image...

Starting power-up diagnostics...

pSH+ Copyright (c) Integrated Systems, Inc., 1992.
Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0(REL) Feb 02 2001 09:53:35
Features:
Initializing VPN 3002 Hardware Client ...
Initialization Complete...Waiting for Network...

Login:_
```

Step 2   At the cursor, enter the login name: **admin**. At the password prompt, enter the default password: **admin**.

```
Login: admin

Password: admin
```

The system displays the opening message and prompts you to select an administrative task.

```
            Welcome to
          Cisco Systems
      VPN 3002 Hardware Client
       Command Line Interface
Copyright (C) 1998-2001 Cisco Systems, Inc.


1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main -> _
```

Step 3   At the cursor, enter **1** for Configuration.

Step 4   The system prompts you to select a configuration task.

```
1) Quick Configuration
2) Interface Configuration
3) System Management
4) Policy Management
5) Back

Config -> _
```

At the cursor, enter **1** to start quick configuration.

Setting the Time and Date

To set the time and date on the VPN 3002:

Step 1   The system prompts you to set the time on your device. The time in brackets is the current device time.

```
-- : Set the time on your device. The correct time is very important,
-- : so that logging entries are accurate.

 -- : Enter the system time in the following format:
 -- :        HH:MM:SS.  Example  21:30:00  for 9:30 PM

> Time

Quick -> [ 10:34:17 ] _
```

At the cursor, enter the correct device time in the format HH:MM:SS, using 24-hour notation. For example, enter 4:24 p.m. as 16:24:00.

Step 2   The system prompts you to set the date. The number in brackets is the current device date.

```
 -- : Enter the date in the following format.
 -- : MM/DD/YYYY  Example 06/12/1999  for June 12th 1999.

> Date

Quick -> [ 01/18/2001 ] _
```

At the cursor, enter the correct date in the format MM/DD/YYYY. Use four digits to enter the year. For example, enter June 12, 2001 as 06/12/2001.

Step 3   The system prompts you to set the time zone. The time zone selections are offsets in hours relative to GMT (Greenwich Mean Time), which is the basis for Internet time synchronization. The number in brackets is the current time zone offset.

```
-- : Set the time zone on your device. The correct time zone is very
 -- : important so that logging entries are accurate.

 -- : Enter the time zone using the hour offset from GMT:
 -- : -12 : Kwajalein  -11 : Samoa     -10 : Hawaii       -9 : Alaska
 -- :  -8 : PST         -7 : MST        -6 : CST           -5 : EST
 -- :  -4 : Atlantic    -3 : Brasilia  -2 : Mid-Atlantic  -1 : Azores
 -- :   0 : GMT         +1 : Paris     +2 : Cairo         +3 : Kuwait
 -- :  +4 : Abu Dhabi   +5 : Karachi   +6 : Almaty        +7 : Bangkok
 -- :  +8 : Singapore   +9 : Tokyo     +10 : Sydney       +11 : Solomon Is.
```

```
 -- : +12 : Marshall Is.

> Time Zone

Quick -> [ -5 ] _
```

At the cursor, enter the time zone offset in the format +/- NN, or accept the default, -5, for U.S. Eastern Standard Time.

Step 4   The system prompts with a menu to enable DST (Daylight-Saving Time support. During DST, clocks are set one hour ahead of standard time. Enabling DST support means that the VPN 3002 automatically adjusts the time zone for DST or standard time. If your system is in a time zone that uses DST, you must enable DST support.

```
1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 1 ] _
```

At the cursor, enter **2** to disable DST support, or accept the default, **1**, to enable DST support, and continue to the next section.

Uploading Configuration

To use the local console PC terminal emulation package to transfer (upload) configuration files from your PC, or from a system accessible to your PC, to the VPN 3002 flash memory:

Step 1   The system prompts you to choose whether or not to upload a configuration file.

```
1) Upload Config File
2) Do Not Upload Config File
3) Back

Quick -> [2]
```

At the cursor, enter **1 Upload Config File** to transfer a configuration file. If you do not want to use an already existing configuration file, accept the default, **2, Do Not Upload Config File** and continue to the next section.

Configuring the Private Interface

To configure the VPN 3002 private interface, use these instructions:

For the VPN 3002 to become fully operational, you must configure the two interfaces you physically connected to your network in the "Connecting Network Cables" section on page 2-3.

- The private interface is the interface to your internal LAN (private network).
- The public interface is the interface to the public network.

Note If you do not change the private interface IP address, you cannot disable PAT mode. That is, you cannot use Network Extension mode unless you configure a private IP address other than the default, which is 192.168.10.1

Step 1 The system prompts you to configure the VPN 3002 private interface.

```
This table shows current IP addresses.

   Intf         Status       IP Address/Subnet Mask        MAC Address
-------------------------------------------------------------------------------
Pri Intf |      UP      |    192.168.10.1/255.255.255.0    | 00.90.A4.00.25.A8
Pub Intf |   Disabled   |        0.0.0.0/0.0.0.0           | 00.90.A4.00.25.A9
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
Default Gateway: 130.0.0.1

WARNING:-- The IP Address for the Private Interface is at the default value
WARNING:-- of 192.168.10.1. Keeping this Private Interface address will prevent
WARNING:-- Network Extension Mode from being enabled.

1) Configure the Private Interface
2) Skip the Private Interface Configuration
3) Back
Quick -> [ 2 ]
```

At the cursor, enter **1 Configure the Private Interface** if you want to change the private interface IP address or subnet mask. If you do not want to change the private interface address, accept the default, **2**, to continue with quick configuration. We assume that you enter **1**.

Step 2 The system prompts you to enter an IP address.

```
This table shows current IP addresses.

Intf           Status         IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
Pri Intf |      UP      |    192.168.10.1/255.255.255.0    | 00.90.A4.00.25.A8
Pub Intf |   Disabled   |        0.0.0.0/0.0.0.0           | 00.90.A4.00.25.A9
-------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
Default Gateway: 130.0.0.1

> Enter IP Address

Quick Private Interface -> [ 192.168.10.1 ] _
```

To reconfigure the IP address for the private interface, at the cursor enter the IP address for the VPN 3002 private interface, using dotted decimal notation; for example, 192.168.12.34. Be sure no other device is using this address on the network.

Step 3 The system prompts you for the private interface subnet mask. The entry in brackets is the standard subnet mask for the IP address you entered above. For example, an IP address of 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0.

```
> Enter Subnet Mask

Quick Private Interface -> [ 255.255.255.0 ]_
```

To reconfigure the subnet mask for the private interface, at the cursor enter the new subnet mask, using dotted decimal notation.

Step 4   The system gives you the option of configuring the DHCP server. The DHCP server for the private interface lets IP hosts in its network automatically obtain IP addresses from a limited pool of addresses for a fixed length of time, or lease period. Before the lease period expires, the VPN 3002 displays a message offering to renew it. If the lease is not renewed, the connection terminates when the lease expires, and the IP address becomes available for reuse. Using DHCP simplifies configuration since you do not need to know what IP addresses are considered valid on a particular network.

```
DHCP Server: Enabled
Address Pool: 192.168.10.2 - 192.168.10.128

1) Disable DHCP Server
2) Enable and Configure DHCP Server
3) Enable DHCP server with existing parameter values.
4) Back

Quick -> [ 3 ]
```

Choose one of the menu options listed.

- If you want to disable the DHCP server, at the prompt enter **1 Disable DHCP Server,** and continue with quick configuration.

- If you want to enable and configure the DHCP server, at the prompt enter **2 Enable and Configure DHCP Server,** and follow Steps 6 through 9 below.

- If you want to enable the DHCP server with existing parameters, at the prompt enter **3.**

Step 5   If you choose 2 Enable and Configure DHCP server, the system displays the server parameters.

```
1) Enable/Disable DHCP
2) Set DHCP Lease Timeout
3) Set DHCP Pool
4) Back
5) Continue

Quick -> [ 3 ]
```

Enter the number for the parameter you want to configure, and press **Enter** to continue with quick configuration.

Step 6   To Enable or disable DHCP, at the prompt, enter **1**. The system displays the Enable DHCP parameter.

```
1) Enable DHCP
2) Disable DHCP

Quick -> [ 1 ]
```

Choose 1 to enable the DHCP server, or 2 to disable it.

Step 7   The DHCP lease period is the amount of time, in minutes, that the private interface owns the IP address the DHCP server assigns. The minimum is 5, maximum is 500,000, and the default is 120 minutes.

To set the lease period, at the prompt, enter 2. The system displays the DHCP Lease Timeout parameter.

```
Quick -> [ 2 ]

> Lease Timeout (5-500000) minutes

Quick -> [ 120 ]
```

At the prompt, enter the number of minutes for the DHCP lease period, or press **Enter** to accept the default, 120 minutes, and continue with quick configuration.

Step 8   The DHCP pool is the range of IP addresses that this DHCP server can assign. The default address pool is 127 IP addresses, and the start of the range is the next IP address after that of the private interface. You can configure another range of IP addresses for the pool, but in no case can the pool have more than 127 addresses.

To configure the DHCP address pool, at the prompt enter 3 Set DHCP Pool. The system displays the DHCP Pool Start field.

```
Quick -> 3

> DHCP Pool Start

Quick -> [ 192.168.10.2 ]
```

Enter the IP address you want as the starting address in the pool, using dotted decimal notation, or accept the default (in brackets), and press **Enter**.

The System displays the DHCP Pool End field.

```
> DHCP Pool End

Quick -> [ 192.168.10.128 ]
```

Enter the IP address you want as the starting address in the pool, using dotted decimal notation, or accept the default (in brackets), and press **Enter**.

Step 9   The System redisplays the list of DHCP parameters.

```
1) Enable/Disable DHCP
2) Set DHCP Lease Timeout
3) Set DHCP Pool
4) Back
5) Continue

Quick ->
```

To revisit DHCP parameters, enter the number for the parameter you want. Click **Back** to revisit earlier sections of quick configuration, or click **Continue** to proceed. We assume that you want to continue.

Configuring the Public Interface

Next you set the system name, and configure a way for the public interface to obtain an IP address using DHCP, PPPoE, or static addressing. The system displays the tasks involved, and also displays current values, if any. Be aware that many ISPs require a system name or hostname if you use DHCP to obtain an IP address.

See the sections that follow for more information about DHCP, PPPoE, and static addressing.

Configuring a System Name

```
This table shows current IP addresses.

   Intf        Status        IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Pri Intf|      UP      |     10.10.99.50/255.255.0.0     |   00.90.A4.00.25.A8
Pub Intf|   Disabled   |        0.0.0.0/0.0.0.0          |   00.90.A4.00.25.A9
--------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name: ispdomain.com
Default Gateway: 130.0.0.1

1) Configure System Name (hostname)
2) Obtain address via DHCP for the Public Interface
3) Use PPPoE to Connect to a Public Network
4) Configure the Public Interface
5) Back

Quick ->
```

Step 1   To assign a system name to the VPN 3002, at the prompt, enter 1.

The system displays the System Name field.

```
-- : Assign a System Name (hostname) to this device.
-- : This may be required for DHCP.

> System Name

Quick -> _
```

Step 2   At the cursor, enter a name such as VPN01. This name must uniquely identify this device on your network. Press **Enter**. The system redisplays the table of current IP addresses and the current menu options.

Configuring DHCP

```
This table shows current IP addresses.

   Intf        Status        IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Pri Intf|      UP      |     10.10.99.50/255.255.0.0     |   00.90.A4.00.25.A8
Pub Intf|   Disabled   |        0.0.0.0/0.0.0.0          |   00.90.A4.00.25.A9
--------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name: ispdomain.com
Default Gateway: 130.0.0.1

1) Configure System Name (hostname)
2) Obtain address via DHCP for the Public Interface
3) Use PPPoE to Connect to a Public Network
4) Configure the Public Interface
```

```
5) Back

Quick -> [2]
```

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets IP hosts in its network automatically obtain IP addresses from a limited pool of addresses for a fixed length of time, or lease period. Using DHCP simplifies configuration since you can manage the assignment of IP addresses from a central point. You do not need to manually enter an IP address for the public interface, and you do not need to know what IP addresses are considered valid on a particular network.

The DHCP server for the Public interface resides on the central-site VPN Concentrator.

Step 1   To obtain an IP address for the public interface using DHCP, at the prompt enter **2** and press **Enter.** The system proceeds to the IPSec parameters; see the section, "Configuring IPSec."

Configuring PPPoE

```
This table shows current IP addresses.

  Intf        Status        IP Address/Subnet Mask        MAC Address
------------------------------------------------------------------------------
Pri Intf|     UP      |     10.10.99.50/255.255.0.0     |  00.90.A4.00.25.A8
Pub Intf|   Disabled  |        0.0.0.0/0.0.0.0          |  00.90.A4.00.25.A9
------------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name: ispdomain.com
Default Gateway: 130.0.0.1

1) Configure System Name (hostname)
2) Obtain address via DHCP for the Public Interface
3) Use PPPoE to Connect to a Public Network
4) Configure the Public Interface
5) Back

Quick ->
```

PPP over Ethernet (PPPoE) is a proposal that specifies how a host PC interacts with a broadband modem—xDSL, cable, wireless—to achieve access to high-speed data networks. It relies on the Ethernet and PPP standards. It includes an authentication strategy that requires a username and password to create a PPPoE session on the VPN 3002.

To configure the VPN 3002 to use PPPoE, follow these steps:

Step 1   At the prompt enter **3**, and press **Enter**. The system prompts for a PPPoE username.

```
Quick -> 3

> PPPoE User Name
```

Step 2 Enter a PPPoE username. The maximum length is 64 characters; however, only the first 17 characters display. Press **Enter**. The system prompts for a PPPoE password.

```
> PPPoE Password

Quick ->
```

Step 3 Enter a PPPoE password, maximum length 64 characters. Press **Enter**. The system prompts you to verify the password. The system proceeds to the IPSec parameters; see the section, "Configuring IPSec."

```
Verify ->
```

Configuring a Static IP Address

```
This table shows current IP addresses.

   Intf        Status        IP Address/Subnet Mask        MAC Address
   -------------------------------------------------------------------------
Pri Intf|       UP       |    10.10.99.50/255.255.0.0    |  00.90.A4.00.25.A8
Pub Intf|    Disabled    |       0.0.0.0/0.0.0.0         |  00.90.A4.00.25.A9
   -------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name: ispdomain.com
Default Gateway: 130.0.0.1

1) Configure System Name (hostname)
2) Obtain address via DHCP for the Public Interface
3) Use PPPoE to Connect to a Public Network
4) Configure the Public Interface
5) Back

Quick ->
```

To configure the VPN 3002 public interface with a static IP address, subnet mask, and default gateway for the public interface, follow these steps:

Step 1 At the prompt enter **4**. The system again displays the current IP addresses table.

```
This table shows current IP addresses.

   Intf        Status        IP Address/Subnet Mask        MAC Address
   -------------------------------------------------------------------------
Pri Intf|       UP       |    10.10.99.50/255.255.0.0    |  00.90.A4.00.25.A8
Pub Intf|    Disabled    |       0.0.0.0/0.0.0.0         |  00.90.A4.00.25.A9
   -------------------------------------------------------------------------
DNS Server(s): DNS Server Not Configured
DNS Domain Name: ispdomain.com
Default Gateway: 130.0.0.1

> Enter IP Address

Quick Public Interface -> [ 0.0.0.0 ]_
```

Step 2 Enter the IP address for this interface, using dotted decimal notation, and press **Enter**. Be sure no other device is using this address on the network.

Step 3   The system prompts for a subnet mask.

```
> Enter Subnet Mask

Quick Public Interface -> [ 255.0.0.0 ]
```

Enter the subnet mask for this interface, using dotted decimal notation. The default is a standard subnet mask appropriate for the IP address you just entered. For example, an IP address of 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it.

Step 4   When you press Enter, the system prompts you to specify a default gateway, which is the system to which the VPN 3002 should forward packets. In other words, if the VPN 3002 has no configured static routes that specify where to send packets, it sends them to this gateway. (When you first start the VPN 3002, it has no static routes.)

```
> Default Gateway

Quick -> _
```

At the cursor, enter the IP address of the default gateway (for example, `10.10.0.1`). This address must *not* be the same as the IP address configured on any VPN 3002 interface. To specify no default gateway, which means the VPN 3002 drops unrouted packets, leave this entry blank. If you are using DHCP to acquire the public IP address, DHCP usually supplies the default gateway, and you should leave this field blank.

The system proceeds to the IPSec parameters; see the section," Configuring IPSec."

Configuring IPSec

The VPN 3002 connects to the remote VPN Concentrator using the IPSec remote server address, group name and password, and username and password. Note that these are the same group and usernames and passwords that you configure on the central-site VPN Concentrator for this VPN 3002.

If you are using digital certificates, the group name and group password are not required.

To configure IPSec:

Step 1   In the IPSec Remote Server parameter, enter the IP address or hostname of the VPN Concentrator to which this VPN 3002 hardware client connects. Note that to enter a hostname, a DNS server must be configured.

```
> IPSec Remote Server

Quick -> [ 130.0.0.1 ]
```

Step 2   The system prompts you to enable or disable IPSec over TCP.

```
1) Enable IPSec over TCP
2) Disable IPSec over TCP

Quick -> [ 2 ]
```

At the cursor, enter 1 to enable IPSec over TCP, or accept the default, 2, to disable IPSec over TCP.

Step 3   The system prompts you to enter the IPSec group name.

```
> IPSec Group Name

Quick -> _
```

At the cursor, enter a unique name for this group. Maximum is 32 characters, case-sensitive; for example, `Group1`.

Step 4   The system prompts you to enter the group password.

```
> IPSec Group Password

Quick -> _
```

At the cursor, enter a unique password for this group. Minimum is 4, maximum is 32 characters, case-sensitive. The system displays only asterisks.

Step 5   The system prompts you to reenter the group password to verify it.

```
Verify -> _
```

At the cursor, reenter the group password. The system displays only asterisks.

Step 6   The system prompts you to enter a username.

```
> IPSec User Name

Quick -> _
```

Enter a unique name within the group for this user. Maximum is 32 characters, case-sensitive.

Step 7   The system prompts you to enter the user password. Minimum is 4, maximum is 32 characters, case-sensitive. The system displays only asterisks.

```
> IPSec User Password

Quick -> _
```

Step 8   The system prompts you to reenter the user password.

```
Verify -> _
```

Configuring PAT or Network Extension mode

This section lets you configure this VPN 3002 to use either PAT or Network Extension mode. You have this option only if you have changed the private interface IP address.

If you have not changed the private interface IP address, the system displays the following message:

```
NOTE:-- Because the IP Address of the Private Interface was not
NOTE:-- changed from the initial default value, you cannot disable
NOTE:-- PAT on the IPSec tunnel to the VPN Concentrator.
```

Client Mode (PAT)

Client mode, also called PAT (Port Address Translation) mode, isolates all devices on the private network from those on the public network. In PAT mode:

- IPSec encapsulates all traffic going from the private network of the VPN 3002 to the network(s) behind the IKE peer, i.e., the central-site VPN Concentrator.

- PAT includes NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the VPN Concentrator assigned IP address on the public interface, and also keeps track of these mappings so that it can forward replies to the correct device.

All traffic from the private network appears on the network behind the central-site VPN Concentrator (the IKE peer) with a single source IP address. This IP address is the one the central-site VPN Concentrator assigns to the VPN 3002. The IP addresses of the computers on the private network are hidden. You cannot ping or access a device on the VPN 3002 private network from outside of the private network, or directly from a device on the private network at the central site.

VPN 3000 Concentrator Settings Required for PAT

For the VPN 3002 to use PAT, follow these requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.0 or later.

2. Address assignment must be enabled, by whatever method you choose to assign addresses (for example, DHCP, address pools, per user, or client-specified). If the VPN Concentrator uses address pools for address assignment, make sure to configure the address pools your network requires. See Chapter 6, "Address Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

3. Configure a group to which you assign this VPN 3002. This includes assigning a group name and password. See Chapter 14, "User Management," in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

4. Configure one or more users for the group, including usernames and passwords.

5. For more information about PAT (Client) mode, see the "Configuring PAT or Network Extension Mode" section on page 3-13.

Network Extension Mode

Network Extension mode allows the VPN 3002 to present a full, routable network to the tunneled network. IPSec encapsulates all traffic from the VPN 3002 private network to networks behind the central-site VPN Concentrator, but PAT does not apply. Therefore, devices behind the VPN Concentrator have direct access to devices on the VPN 3002 private network via the tunnel, and only over the tunnel, and vice versa.

In this mode, the VPN Concentrator does not assign an IP address for tunneled traffic (as it does in Client/PAT mode). The tunnel is terminated with the VPN 3002 private IP address (i.e., the assigned IP address). To use Network Extension mode, you must configure an IP address other than the default of 192.168.10.1 and disable PAT.

VPN 3000 Concentrator Settings Required for Network Extension Mode

For the VPN 3002 to use Network Extension mode, these are the requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.0 or later.

2. Configure a group to which you assign this VPN 3002. This includes assigning a group name and password. See Chapter 14, "User Management," in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

3. Configure one or more users for the group, including usernames and passwords.

4. Configure either a default gateway or a static route to the VPN 3002 private network. See Chapter 8, "IP Routing," in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

5. If you want the VPN 3002 to be able to reach devices on other networks that connect to this VPN Concentrator, review your Network Lists. See Chapter 15, "Policy Management," in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

For more information about Network Extension mode, see the "Configuring PAT or Network Extension Mode" section on page 3-13.

Enabling or Disabling PAT

If you have changed the private interface IP address, the system prompts you to enable or disable PAT:

```
1) Enable PAT over the IPSec Tunnel
2) Disable PAT over the IPSec Tunnel (Network Extension)

Quick ->
```

To disable PAT, and use Network Extension mode, at the prompt enter **2**. Note that you can not disable PAT if you have not changed the IP address for the private interface.

Configuring DNS

You can specify a Domain Name System (DNS) server for your local ISP, which lets you enter Internet hostnames (for example, mail01) rather than IP addresses for servers as you configure and manage the VPN 3002. While hostnames are easier to remember, using IP addresses avoids problems that might arise with the DNS server offline or congested. If you use a hostname to identify the central-site VPN Concentrator, you must configure a DNS server:

Step 1   The system prompts you to specify a DNS server.

```
-- : Specify a local DNS server, which lets you enter hostnames
 -- : rather than IP addresses while configuring.

> DNS Server

Quick -> [ 0.0.0.0 ]
```

At the cursor, enter the IP address of your local DNS server in dotted decimal notation; for example, `10.10.0.11`.

Step 2   The system prompts you to enter the registered Internet domain name in which the VPN 3002 is located (sometimes called the domain name suffix or subdomain).

```
-- : Enter your ISP's domain name; e.g., ispdomain.com

> Domain

Quick -> _
```

Configuring Static Routes

You can add or delete manual IP routes for this VPN 3002. The system displays a current static routes table:

```
------------
Destination     Mask             Metric Destination
-----------------------------------------------------------
0.0.0.0         0.0.0.0          1 130.0.0.1

1) Add Static Route
2) Delete Static Route
3) Back
4) Continue

Quick -> _
```

Adding a Static Route

To add a static route:

Step 1   At the prompt, enter the number for the function you want.

If you selected 1 to add a static route, the system now prompts for the Net Address.

```
> Net Address

Quick ->
```

Enter the network IP address for this static route. Packets with this address are sent to the destination address below.

Step 2   The system prompts you for a subnet mask.

```
> Subnet Mask

Quick -> 255.0.0.0
```

Enter the subnet mask of this network IP address.

Step 3   The system prompts you to identify the outbound destination as either a router/gateway, or as this VPN 3002 private or public interface.

```
1) Destination is Router
2) Destination is Interface

Quick -> _
```

If you want to set a router for the outbound destination, at the prompt enter **1**. To select one for the VPN 3002 interfaces, at the prompt, enter **2**.

```
Enter destination address.
```

Step 4   In either case, the system prompts you for the destination address. If you selected Router, the system prompts for the router address.

```
> Router Address

Quick -> _
```

Enter the IP address of the router/gateway outbound destination.

Step 5   If you selected Interface, the system prompts you to choose either the private or public Interface.

```
Interfaces
----------
1. Private Interface (10.10.99.32)
2. Public Interface (0.0.0.0)

> Interface Number for this route

Quick ->_
```

Enter the number for the interface of the outbound destination for this route.

Step 6   The system prompts for the cost for this route; this is a number from 1 to 16 where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

```
Enter metric

> Route Metric (1 - 16)
```

```
Quick -> _
```

Step 7   The system redisplays the static routes.

```
Static Routes
-------------
Destination     Mask            Metric Destination
----------------------------------------------------------
0.0.0.0         0.0.0.0             1 130.0.0.1
192.44.55.6     255.0.0.0           1 10.10.99.10

1) Add Static Route
2) Delete Static Route
3) Back
4) Continue
```

Deleting a Static Route

Step 1   To delete a static route, at the prompt enter **2**. The system asks you which route you want to delete.

```
> Delete Which Route (net address)

Quick -> 192.44.55.6
3) Back
4) Continue
```

Enter the IP address of the network address for the route you want to delete.

The menu displays again, with the route you deleted no longer present. To continue with quick configuration, at the prompt enter **4**.

Changing admin Password

You can change the password for the **admin** administrator user. For ease of use during startup, the default **admin** password supplied with the VPN 3002 is also **admin**. Since the **admin** user has full access to all management and administration functions on the device, *we strongly recommend you change this password to improve device security*. You can further configure all administrators with the regular Administration menus.

Step 1   The system prompts you to change the **admin** password.

```
-- : We strongly recommend that you change the password ...

> Reset Admin Password

Quick -> [ ***** ] _
```

At the cursor, enter a new password for admin. Remember that entries are case sensitive. For maximum security, the password should be at least 8 characters long, a mixture of upper- and lower-case alphabetic and numeric characters, and not easily guessed; for example, `W8j9Haq3`. The system displays only asterisks. To keep the default, press **Enter**.

Step 2   The system prompts you to re-enter the password to verify it.

```
Verify -> _
```

At the cursor, reenter the new password. The system displays only asterisks. To keep the default, press **Enter**.

Completing Quick Configuration

You have completed quick configuration, and your entries constitute the active or running configuration. The VPN 3002 now has enough information, and it is operational. The system has saved your changes to the active configuration in the system configuration file as you have made them.

The system now displays the final quick configuration menu.

```
1) Goto Main Configuration Menu
2) Exit

Quick -> _
```

Step 1   At the cursor, enter **2** to exit quick configuration. The system displays:

```
Done
```

Step 2   If you want to use the CLI for other functions, enter **1** at the cursor. For information on using the CLI, see the *VPN 3002 Hardware Client Reference*.

What Next?

Now that the VPN is operational, you can:

Explore the CLI. The menus follow the same order, and let you perform the same functions, as the VPN 3002 Hardware Client Manager. See Chapter 14, "Using the Command-Line Interface," in the *VPN 3002 Hardware Client Reference* for explanations of parameters and entries.

Proceed to a more detailed and complete system configuration. See the *VPN 3002 Hardware Client Reference*.

Troubleshooting and System Errors

Appendix A describes files you can use to troubleshoot errors and problems on the VPN 3002 and LED indicators for the system. It also describes common errors that might occur while configuring and using the system, and how to correct them. It includes the following topics:

Files for Troubleshooting

The VPN 3002 Hardware Client creates several files that you can examine and that can assist Cisco support engineers when troubleshooting errors and problems:

- Event log—Record of system events.
- SAVELOG.TXT—Event log that is automatically saved when the system crashes and when it is rebooted.
- CRSHDUMP.TXT—Internal system data file that is written when the system crashes.
- CONFIG—Normal configuration file used to boot the system.
- CONFIG.BAK—Backup configuration file.

Event Logs

The VPN 3002 records system events in the event log, which is stored in nonvolatile memory (NVRAM). To troubleshoot operational problems, we recommend that you start by examining the event log. To view the event log, see Administration | File Management | View, and click **View Saved Log File**. To configure events, and to choose the events you want to view, see Configuration | System | Events and Monitoring | Filterable Event Log.

The VPN 3002 automatically saves the event log to a file in flash memory if it crashes, and when it is rebooted. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging. To view SAVELOG.TXT, see Administration | File Management | View, and click **View Saved Log File**.

Crash Dump File

If the VPN 3002 crashes during operation, it saves internal system data in nonvolatile memory (NVRAM), and then automatically writes this data to a CRSHDUMP.TXT file in flash memory when it is rebooted. This file contains the crash date and time, software version, tasks, stack, registers, memory, buffers, and timers that help Cisco support engineers diagnose the problem. In case of a crash, we ask that you send this file when you contact TAC for assistance. To view the CRSHDUMP.TXT file, see Administration | File Management | View, and click **View Saved Log Crash Dump File**.

Configuration Files

The VPN 3002 saves the current boot configuration file (CONFIG) and its predecessor (CONFIG.BAK) as files in flash memory. These files might be useful for troubleshooting. See Administration | File Management for information on managing files in flash memory.

LED Indicators

LED indicators on the VPN 3002 are normally green or flashing amber. LEDs that are solid amber or off might indicate an error condition.

Contact Cisco TAC if any LED indicates an error condition.

VPN 3002 Front LEDs

The LEDs on the front of the VPN 3002 are:

LED	Status	Explanation
PWR	Green	Unit is on and has power.
	Off	Unit is powered off.
SYS	Flashing amber	Unit is performing diagnostics.
	Solid amber	Unit has failed diagnostics.
	Flashing green	Unit is negotiating DHCP or PPPoE
	Green	Unit is operational.
VPN	Off	No VPN tunnel exists.
	Amber	Tunnel has failed.
	Green	Tunnel is established.

VPN 3002 Rear LEDs

The LEDs on the rear of the VPN 3002 indicate the status of the private and public interfaces.

LED	Explanation
Green	Interface is connected to the network.
OFF	Interface is not connected to the network.
Flashing amber	Traffic is traveling across the interface.

System Errors

If you have configured the VPN 3002, and you are unable to connect to or pass data to the central-site VPN Concentrator, use Table A-1 to analyze the problem. Also, use the section following Table A-1 to check the settings on the VPN Concentrator to which this VPN 3002 connects.

Table A-1   Analyzing System Errors

Problem or Symptom	Possible Solution
Tunnel is not up or not passing data.	
PWR LED is off.	Make sure that the power cable is plugged into the VPN 3002 and a power outlet.
SYS LED is solid amber.	Unit has failed diagnostics. Contact Cisco Support immediately.
You see this LED display: PWR = green SYS LED = green VPN LED = off.	1. Verify that the VPN Concentrator to which this VPN 3002 connects is running version 3.0 software or above. 2. Navigate to Monitoring > System Status. Click **Connect Now**.
Connect Now did not bring up the tunnel, and the public interface LED (rear of unit) is off.	1. Check that a LAN cable is properly attached to the public interface of the VPN 3002. 2. Make sure the IP address for the public interface is properly configured.
Public interface LED is on, but attempting to ping the default gateway (Administration > Ping) yields no response.	1. Make sure the default gateway is properly configured. 2. Contact your ISP.

Table A-1   Analyzing System Errors (continued)

Problem or Symptom	Possible Solution

VPN LED is solid amber (tunnel failed to establish to central-site VPN Concentrator).	1. Make sure the IPSec parameters are properly configured. Verify:
	  – Public IP Address of the IKE peer (central-site VPN Concentrator) is correct.
	  – Group name and password are correct.
	  – Username and password are correct.
	
	2. Make sure the group and usernames and passwords match those set for the VPN 3002 on the central-site VPN Concentrator.
	
	3. After you make any changes, navigate to Monitoring > System Status and click **Connect Now**.
	
	4. Study the event log files. To capture more events, and to interpret events, see Chapter 9, "Events," in the *VPN 3002 Hardware Client Reference*.

My PC cannot communicate with the remote network.	1. Verify that the VPN Concentrator to which this VPN 3002 connects is running version 3.0 software or above. 2. Navigate to Monitoring > System Status and click **Connect Now**.
Connect Now worked.	
LED(s) for the private interface/switch port are off.	Make sure that a LAN cable is properly attached to the private interface of the VPN 3002 and the PC.
LED(s) for the private interface/switch port are on.	1. Is this PC configured as a DHCP client? If so, verify that the DHCP server on the VPN 3002 is enabled. 2. With any method of address assignment, verify that the PC has an IP address and subnet mask.
Attempting to ping the default gateway (Administration > Ping) yields no response.	1. Make sure your PC has an appropriate IP address, reachable on this network. 2. Contact your network administrator.

Settings on the VPN Concentrator

If your VPN 3002 experiences connectivity problems, check the configuration of the VPN Concentrator.

Step 1   Configure the connection as a Client, *not* LAN-to-LAN.

Step 2   Assign this VPN 3002 to a group. Configure group and usernames and passwords. These must match the group and usernames and passwords that you set on the VPN 3002. Refer to Chapter 14, "User Management," in the *VPN 3000 Series Concentrator Series Reference Volume 1: Configuration*.

Step 3   If the VPN 3002 uses PAT mode, enable a method of address assignment for the VPN 3002: DHCP, address pools, per user, or client specified. Refer to Chapter 6, "Address Management," in the *VPN 3000 Series Concentrator Series Reference Volume 1: Configuration*.

Step 4   If you are using Network Extension mode, configure a default gateway or a static route to the private network of the VPN 3002. Refer to Chapter 8, "IP Routing," in the *VPN 3000 Series Concentrator Series Reference Volume 1: Configuration*.

Step 5   Check the Event log. Refer to Chapter 10, "Events," in the *VPN 3000 Series Concentrator Series Reference Volume 1: Configuration*.

VPN 3002 Hardware Client Manager Errors

The following sections describe errors that might occur while using the HTML-based VPN 3002 Hardware Client Manager with a browser.

Invalid Login or Session Timeout

The Manager displays the Invalid Login or Session Timeout screen (see Figure A-1).

Figure A-1   Invalid Login or Session Timeout Screen
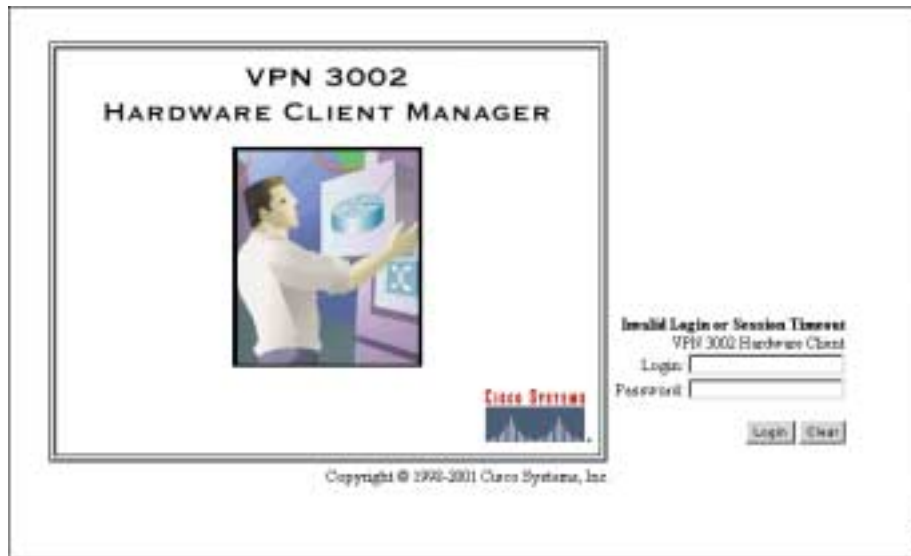
Table A-2   Invalid Login or Session Timeout Screen

Problem	Possible Cause	Solution
You entered an invalid administrator login-name and password combination	• Typing error. • Invalid (unrecognized) login name or password.	• Reenter the login name and password, and click **Login**. • Use a valid login name and password. • Verify your typing before clicking on **Login**.
The Manager session has been idle longer than the configured timeout interval. (The default timeout interval is 600 seconds, which equals 10 minutes).	• No activity has occurred for (interval) seconds. The Manager resets the inactivity time only when you click an action button such as **Apply, Add,** or **Cancel**, or a link on a screen that invokes a different screen. Entering values or setting parameters on a given screen does not reset the timer. • The timeout interval is set too low for normal use.	On the Administration	Access Rights	Access Settings screen, change the Session Timeout interval to a larger value and click **Apply**.

Manager Logs Out

The Manager logs out unexpectedly.

Table A-3   Browser Refresh or Reload Button Logs Out the Manager.

Problem	Possible Cause	Solution
You clicked on the **Refresh** or **Reload** button on the browser navigation toolbar, and the Manager logged out. The main login screen displays.	To protect access security, clicking on **Refresh** or **Reload** on the browser toolbar automatically logs out the Manager session.	Do not use the browser navigation toolbar buttons with the VPN 3002 Hardware Client Manager. Use only the Manager Refresh button where it appears on a screen. We recommend that you hide the browser navigation toolbar to prevent mistakes.

Incorrect Display

The Manager displays an incorrect screen or data when you click the browser back or forward button.

Table A-4   Browser Back or Forward Button Displays an Incorrect Screen or Incorrect Data

Problem	Possible Cause	Solution
You clicked on the **Back** or **Forward** button on the *browser* navigation toolbar, and the Manager displayed the wrong screen or incorrect data.	To protect security and the integrity of data entries, clicking on **Back** or **Forward** on the browser toolbar deletes pointers and values within the Manager.	Do not use the browser navigation toolbar buttons with the VPN 3002 Hardware Client Manager. Navigate using the location bar at the top of the Manager window, the table of contents in the left frame, or links on Manager screens. We recommend that you hide the browser navigation toolbar to prevent mistakes.

Error Message

The Manager displays a screen with the message: "Error/An error has occurred while attempting to perform the operation." An additional error message describes the erroneous operation (see Figure A-2).

Figure A-2   Error Screen
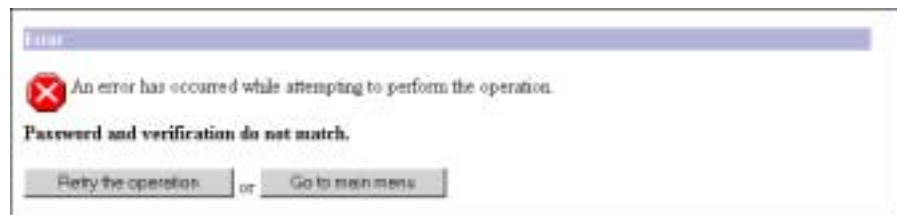
Table A-5   Error Message Displays

Problem	Possible cause	Solution
You tried to perform some operation that is not allowed.	The screen displays a message that describes the cause.	• Click **Retry the operation** to return to the screen where you were working and correct the mistake. Carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost. • Click **Go to main menu** to go to the main Manager screen.

Not Allowed Message

The Manager displays a screen with the message: "Not Allowed / You do not have sufficient authorization to access the specified page." (See Figure A-3.)

Figure A-3   Not Allowed Screen

Table A-6   Not Allowed Message Displays

Problem	Possible cause	Solution
You tried to access an area of the Manager that you do not have authorization to access.	• You logged in using an administrator login name that has limited privileges. • You logged in from a workstation that has limited access privileges.	• Log in using the system administrator login name and password. (Defaults are admin / admin.) • Log in from a workstation with greater access privileges. • Have the system administrator change your privileges on the Administration | Access Rights | Administrators screen. • Have the system administrator change the privileges of your workstation on the Administration | Access Rights | Access Control List screen.

Not Found

The Manager displays a screen with the message: "Not Found/An error has occurred while attempting to access the specified page." The screen includes additional information that identifies system activity and parameters.

Figure A-4   Not Found Screen

Table A-7   Not Found Message Displays

Problem	Possible cause	Solution
The Manager could not find a screen.	• You updated the software image and did not clear the browser's cache.	Clear the browser's cache: delete its temporary internet files, history files, and location bar references. Then try again.
	• There is an internal Manager error.	Please note the system information on the screen and contact Cisco support personnel for assistance.

Microsoft Internet Explorer Script Error: No such interface supported

Microsoft Internet Explorer displays a Script Error dialog box that includes the error message: "No such interface supported."

Table A-8   Microsoft Internet Explorer Script Error

Problem	Possible cause	Solution
While using a Manager function that opens another browser window (such as Save Needed, Help, Software Update, etc.), Internet Explorer cannot open the window and displays the error dialog box.	A bug in the Internet Explorer JavaScript interpreter.	1. Click **No** on the error dialog box. 2. Log out of the Manager. 3. Close Internet Explorer. 4. Reinstall Internet Explorer.

Command-Line Interface Errors

These errors may occur while using the menu-based command-line interface from a console or Telnet session.

Table A-9   Command-Line Interface Errors

Error	Problem	Possible Cause	Solution
ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID	The system expected a valid 4-byte dotted decimal entry, and the entry was not in that format.	• You entered something other than a 4-byte dotted decimal number. You might have omitted a byte position, or entered a number greater than 255 in a byte position. • You entered 0.0.0.0 instead of an appropriate address.	At the prompt, reenter a valid 4-byte dotted decimal number.
ERROR:-- Out of Range value entered. Try again.	The system expected a number within a certain range, and the entry was outside that range.	• You entered a letter instead of a number. • You entered a number greater than the possible menu numbers.	At the prompt, reenter a number in the appropriate range.
ERROR:-- The Passwords do not match. Please try again.	The entry for a password and the entry to verify the password do not match.	• You mistyped an entry. • You entered either a password or verify entry, but not the other.	At the Verify prompt, reenter the password. If the original password is incorrect, press **Enter** and reenter both the password and the verification at the prompts.

INDEX

A

active configuration

admin password

changing   3-21

changing (CLI)   4-17

default   3-21, 4-17

Admin Password (screen)   3-21

Advanced Encryption Standard (AES)   1-15

authentication features, summary of   1-8

B

Back (button)   3-3

backup servers   1-9

Bad IP Address (error)   A-10

banners on the VPN 3002   1-15

beginning Quick Configuration   2-5

boot messages, at startup   2-4, 4-2

brackets, default entries in   4-1

browser

Back or Forward button displays incorrect screen or incorrect data   A-7

navigation toolbar, don't use with Manager   2-2, 3-4

C

cables, connecting   2-3

cabling distances, specifications   1-17

case-sensitivity   3-3, 4-1

changing admin password   3-21

changing admin password (CLI)   4-17

CLI

errors   A-10

using for Quick Configuration   4-1

Client (PAT) mode

configuring with CLI   4-13

configuring with Manager   3-13

interactive multimedia explanation   3-13

c lient (PAT) mode

interactive multimedia explanation   1-2

client (PAT) mode

description   1-2

command line interface

exiting   4-18

using for Quick Configuration   4-1

completing Quick Configuration

with command line interface   4-1

with Manager   3-1

configuration, active or running   3-3, 4-1

configuration files

uploading   3-5

useful for troubleshooting   A-2

connecting

console   2-3

network cables   2-3

console

connecting   2-3

crash, system, saves log file   A-1

CRSHDUMP.TXT file   A-2

D

data

formats   xiii

needed for Quick Configuration   2-7