



VPN 3002 Hardware Client User Guide

Release 3.0
March 2001

Corporate Headquarters

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

<http://www.cisco.com>

Tel: 408 526-4000
800 553-NETS (6387)

Fax: 408 526-4100

Customer Order Number: OL-0874=
Text Part Number: OL-0874-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover AA That's Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

VPN 3002 Hardware Client User Guide
Copyright © 2001, Cisco Systems, Inc.
All rights reserved.



Table of contents

Preface

About this manual	xi
Additional documentation	xii
Documentation on VPN software distribution CDs	xiii
Obtaining documentation	xiii
Obtaining technical assistance	xiv
Other references	xv
Documentation conventions	xvi
Data formats	xvi

1 Using the VPN 3002 Hardware Client Manager

Browser requirements	1-1
Recommended PC monitor / display settings	1-3
Connecting to the VPN 3002 using HTTP	1-3
Installing the SSL certificate in your browser	1-3
Connecting to the VPN 3002 using HTTPS	1-16
Logging in the VPN 3002 Hardware Client Manager	1-17
Configuring HTTP, HTTPS, and SSL parameters	1-18
Understanding the VPN 3002 Hardware Client Manager window	1-19
Organization of the VPN 3002 Hardware Client Manager	1-22
Navigating the VPN 3002 Hardware Client Manager	1-23

2 Configuration

Configuration	2-1
---------------------	-----

3 Interfaces

Configuration Interfaces	3-1
Configuration Interfaces Private	3-3
Configuration Interfaces Public	3-5

4 System Configuration

Configuration System	4-1
------------------------------	-----

5 Servers

Configuration System Servers	5-1
Configuration System Servers DNS	5-1

6 Tunneling

Configuration System Tunneling Protocols	6-2
Configuration System Tunneling Protocols IPSec	6-2

7 IP Routing

Configuration System IP Routing	7-1
Configuration System IP Routing Static Routes	7-2
Configuration System IP Routing Static Routes Add or Modify	7-3
Configuration System IP Routing Default Gateways	7-4
Configuration System IP Routing DHCP	7-5
Configuration System IP Routing DHCP Options	7-7
Configuration System IP Routing DHCP Options Add or Modify	7-8

8 Management Protocols

Configuration System Management Protocols	8-1
Configuration System Management Protocols HTTP/HTTPS	8-2
Configuration System Management Protocols Telnet	8-4
Configuration System Management Protocols SNMP	8-5
Configuration System Management Protocols SNMP Communities	8-7
Configuration System Management Protocols SSL	8-9
Configuration System Management Protocols SSH	8-12

9 Events

Event class	9-1
Event severity level	9-4
Event log	9-5
Configuration System Events	9-6
Configuration System Events General	9-6
Configuration System Events Classes	9-8
Configuration System Events Classes Add or Modify	9-9
Configuration System Events Trap Destinations	9-11
Configuration System Events Trap Destinations Add or Modify	9-12
Configuration System Events Syslog Servers	9-13

Configuration | System | Events | Syslog Servers | Add or Modify 9-15

10 General

Configuration | System | General 10-1
 Configuration | System | General | Identification 10-2
 Configuration | System | General | Time and Date 10-3

11 Policy Management

Client mode/PAT 11-1
 Network Extension mode 11-2
 Configuration | Policy Management 11-3
 Configuration | Policy Management | Traffic Management 11-3
 Configuration | Policy Management | Traffic Management | PAT 11-4
 Configuration | Policy Management | Traffic Management | PAT | Enable 11-4

12 Administration

Administration 12-1
 Administration | Software Update 12-2
 Administration | System Reboot 12-5
 Administration | Ping 12-7
 Administration | Access Rights 12-8
 Administration | Access Rights | Administrators 12-9
 Administration | Access Rights | Access Settings 12-10
 Administration | File Management 12-11
 Administration | File Management | View 12-12
 Administration | File Management | Swap Config Files 12-13
 Administration | File Management | Config File Upload 12-13
 Administration | Certificate Management 12-15
 Administration | Certificate Management | Enrollment 12-17
 Administration | Certificate Management | Enrollment | Request Generated 12-20
 Administration | Certificate Management | Installation 12-21
 Administration | Certificate Management | Certificates 12-23
 Administration | Certificate Management | Certificates | View 12-24
 Administration | Certificate Management | Certificates | Delete 12-27

13 Monitoring

Monitoring 13-1
 Monitoring | Routing Table 13-2

Monitoring Filterable Event Log	13-3
Monitoring Live Event Log	13-8
Monitoring System Status	13-9
Monitoring System Status Private/Public Interface	13-12
Monitoring Statistics	13-14
Monitoring Statistics IPsec	13-15
Monitoring Statistics HTTP	13-21
Monitoring Statistics Telnet	13-22
Monitoring Statistics DNS	13-23
Monitoring Statistics SSL	13-24
Monitoring Statistics DHCP	13-26
Monitoring Statistics SSH	13-27
Monitoring Statistics MIB-II	13-28
Monitoring Statistics MIB-II Interfaces	13-28
Monitoring Statistics MIB-II TCP/UDP	13-30
Monitoring Statistics MIB-II IP	13-32
Monitoring Statistics MIB-II ICMP	13-35
Monitoring Statistics MIB-II ARP Table	13-37
Monitoring Statistics MIB-II Ethernet	13-39
Monitoring Statistics MIB-II SNMP	13-41

14 Using the Command Line Interface

Accessing the CLI	14-1
Starting the CLI	14-2
Using the CLI	14-3
CLI menu reference	14-7

A Errors and troubleshooting

Files for troubleshooting	A-1
LED indicators	A-2
Errors on the system	A-3
Settings on the VPN 3000 Series Concentrator	A-4
VPN 3002 Hardware Client Manager errors	A-5
Command Line Interface errors	A-10

B Copyrights, licenses, and notices

Software License Agreement of Cisco Systems, Inc.	B-1
Other licenses	B-3
Regulatory Standards Compliance	B-9

Index

Tables

Table 9-1: **VPN 3002 event classes** 9-1
Table 9-2: **VPN 3002 event severity levels** 9-4
Table 9-3: **Configuring “well-known” SNMP traps** 9-7



Preface

About this manual

The *VPN 3002 Hardware Client User Guide* provides guidelines for configuring the Cisco VPN 3002, details on all the functions available in the VPN 3002 Hardware Client Manager, and instructions for using the VPN 3002 Command Line Interface.

Prerequisites

We assume you have read the *VPN 3002 Hardware Client Getting Started* manual and have followed the minimal configuration steps in *Quick Configuration*. That section of the VPN Hardware Client Manager is not described here.

We also 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 may be new to you. You should be familiar with Windows® 95/98 or Windows NT® system configuration and management, and you should be familiar with Microsoft Internet Explorer or Netscape® Navigator® or Communicator browsers.

Organization

This manual is organized by the order in which sections appear in the VPN 3002 Hardware Client Manager table of contents (the left frame of the Manager browser window; see Figure 1-30 in Chapter 1.

Chapter 1, *Using the VPN 3002 Hardware Client Manager* explains how to log in, navigate, and use the VPN 3002 Hardware Client Manager with a browser. It explains both HTTP and HTTPS browser connections, and how to install the SSL certificate for a secure (HTTPS) connection.

Chapter 2, *Configuration* describes the main VPN 3002 Hardware Client Manager configuration screen.

Chapter 3, *Interfaces* explains how to configure the VPN 3002 Private and Public interfaces.

Chapter 4, *System Configuration* describes the system configuration screen of the VPN 3002 Hardware Client Manager.

Chapter 5, *Servers* explains how to configure the VPN 3002 to communicate with DNS servers to convert hostnames to IP addresses (DNS).

Chapter 6, *Tunneling* explains how to configure IPSec.

Chapter 7, *IP Routing* explains how to configure static routes, default gateways, and DHCP parameters and options.

Chapter 8, *Management Protocols* explains how to configure built-in VPN 3002 servers that provide management functions: HTTP and HTTPS, Telnet, SNMP, SNMP Community Strings, SSL and SSH.

Chapter 9, *Events* explains how to configure system events such as alarms, traps, error conditions, network problems, task completion, or status changes.

Chapter 10, *General* explains how to configure the system identification, date, and time.

Chapter 11, *Policy Management* explains how to configure PAT and use LAN Extension mode.

Chapter 12, *Administration* explains how to configure and use high-level VPN 3002 administrator activities such as who is allowed to configure the system, what software runs on it, rebooting and shutting down the system, managing its configuration files, and managing X.509 digital certificates.

Chapter 13, *Monitoring* explains the many status, statistics, sessions, and event log screens that you can use to monitor the VPN 3002.

Chapter 14, *Using the Command Line Interface* explains how to use the built-in menu- and command-line-based administrative management system via the system console or a Telnet session. With the CLI, you can access and configure all the same parameters as the HTML-based VPN 3002 Hardware Client Manager.

Appendix A, *Errors and troubleshooting* describes common errors that may occur while configuring the system, and how to correct them. It also describes all system and module LED indicators.

Appendix B, *Copyrights, licenses, and notices* provides all copyright and license information for Cisco software on the VPN 3002, and for software that the system uses under license from other firms.

Additional documentation

The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is online only.

The VPN 3002 Hardware Client Manager also includes extensive context-sensitive online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

The *VPN 3002 Hardware Client Quick Reference Card* summarizes 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 installing the VPN 3002 and beginning 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 if you want.

The *VPN 3000 Concentrator Series Getting Started* manual provides information to take you from unpacking and installing the VPN 3000, through configuring the minimal parameters to make it operational (called Quick Configuration).

The *VPN 3000 Concentrator Series User Guide* provides details on all the functions available in the VPN Concentrator Manager, and guidelines for configuring the VPN 3000 Concentrator.

The *VPN Client User Guide* explains how to install, configure, and use the VPN Client, which lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN 3000 Concentrator.

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

Documentation on VPN software distribution CDs

The VPN 3000 Concentrator and VPN 3002 Hardware Client documentation is 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 Adobe® Acrobat® Reader 3.0 or later; version 4.5 is included on the Cisco VPN 3000 Concentrator software distribution CD-ROM.

Obtaining documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships 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 as an annual subscription.

Ordering documentation

Cisco documentation is available in the following ways:

- Registered 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 corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining technical assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by using the Cisco TAC website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Other references

Other useful books and articles include:

Frequently Asked Questions about Microsoft VPN Security. Microsoft Corporation: 1998.
(Available from Microsoft web site, www.microsoft.com.)

Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.

Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.

Stallings, William. *Data and Computer Communications*, 5th ed. Prentice-Hall: 1997.

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.

Documentation conventions

We use these typographic conventions in this manual:

Font	Meaning
<i>This font</i>	Document, chapter, and section titles. Emphasized text.
This font	Command-line prompts and entries, data-entry-field entries, system displays, filenames, etc.
<u>This font</u>	Literal entries you should make exactly as shown.
<This font>	Variables that the system supplies. Ignore the angle brackets.
This font	Menus, menu items, keyboard keys, icons, screen names, data-entry field names, etc.

Data formats

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

IP addresses

IP addresses use 4-byte dotted decimal notation; for example, 192.168.12.34. 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. 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 host 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 alphanumeric characters, upper- and lower-case. Most text strings are case-sensitive; for example, *simon* and *Simon* represent different usernames. The maximum length of text strings is generally 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 VPN3002 always stores filenames as uppercase.

Port numbers

Port numbers use decimal numbers from 0 to 65535 with no commas or spaces.



Using the VPN 3002 Hardware Client Manager

The VPN 3002 Hardware Client Manager is an HTML-based interface that lets you configure, administer, monitor, and manage the VPN 3002 with a standard Web browser. To use it, you need only to connect to the VPN 3002 using a PC and browser on the same private network with the VPN 3002.

The Manager uses the standard Web client / server protocol, HTTP (Hypertext Transfer Protocol), which is a cleartext protocol. However, you can also use the Manager in a secure, encrypted HTTP connection over SSL (Secure Sockets Layer) protocol, which is known as HTTPS.

- To use a cleartext HTTP connection, see *Connecting to the VPN 3002 using HTTP*.
- To use HTTP over SSL (HTTPS) with the Manager:
 - 1 The first time, connect to the Manager using HTTP, and
 - 2 Install an SSL certificate in the browser; see *Installing the SSL certificate in your browser* on page 1-3.

Once the SSL certificate is installed, you can connect directly using HTTPS; see *Connecting to the VPN 3002 using HTTPS* on page 1-16.

Browser requirements

The VPN 3002 Hardware Client Manager requires either Microsoft Internet Explorer version 4.0 or higher, or Netscape Navigator / Communicator version 4.5-4.7. For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

Note: You cannot use the Live Event Log feature with Netscape navigator/Communicator version 4.0.

JavaScript

Be sure JavaScript is enabled in the browser. Check these settings:

- Internet Explorer 4.0:
 - On the **View** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom (for expert users)** then click **Settings**.
 - In the **Security Settings** window, scroll down to **Scripting**.
 - Click **Enable** under **Scripting of Java applets**.
 - Click **Enable** under **Active scripting**.
- Internet Explorer 5.0:
 - On the **Tools** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom Level**.
 - In the **Security Settings** window, scroll down to **Scripting**.
 - Click **Enable** under **Active scripting**.
 - Click **Enable** under **Scripting of Java applets**.
- Navigator / Communicator 4.x:
 - On the **Edit** menu, select **Preferences**.
 - On the **Advanced** screen, check the box for **Enable JavaScript**.

Cookies

Be sure cookies are enabled in the browser. Check these settings:

- Internet Explorer 4.0:
 - On the **View** menu, select **Internet Options**.
 - On the **Advanced** tab, scroll down to **Security** then **Cookies**.
 - Click **Always accept cookies**.
- Internet Explorer 5.0:
 - On the **Tools** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom Level**.
 - In the **Security Settings** window, scroll down to **Cookies**.
 - Click **Enable** under **Allow cookies that are stored on your computer**.
 - Click **Enable** under **Allow per-session cookies (not stored)**.
- Navigator / Communicator 4.5:
 - On the **Edit** menu, select **Preferences**.
 - On the **Advanced** screen, click one of the **Accept ... cookies** choices, and *do not* check **Warn me before accepting a cookie**.

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 best 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.

Connecting to the VPN 3002 using HTTP

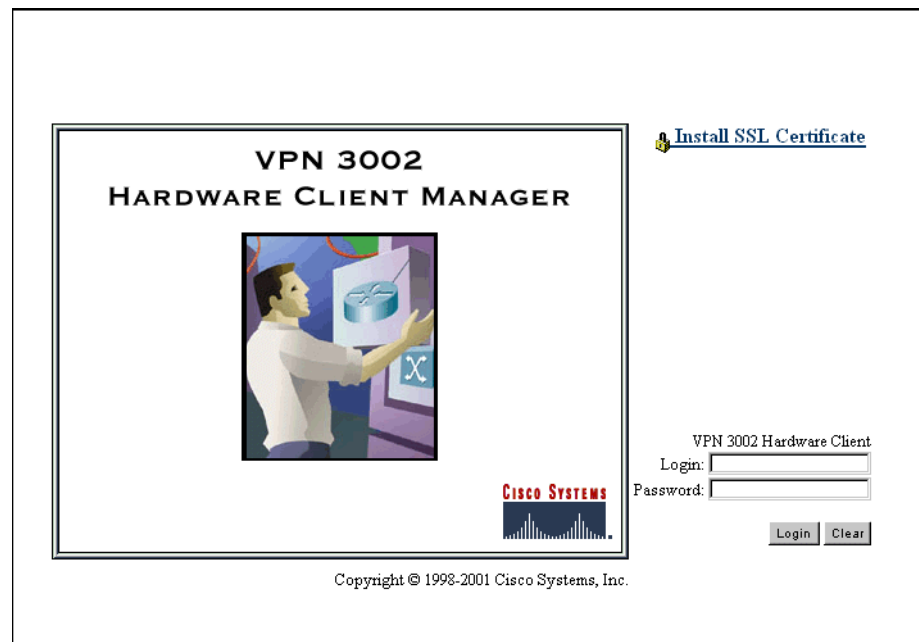
When your system administration tasks and network permit a cleartext connection between the VPN 3002 and your browser, you can use the standard HTTP protocol to connect to the system.

Even if you plan to use HTTPS, you use HTTP at first to install an SSL certificate in your browser.

- 1 Bring up the browser.
- 2 In the browser **Address** or **Location** field, you can just enter the VPN3002 Private interface IP address; e.g., 10.10.147.2. The browser automatically assumes and supplies an `http://` prefix.

The browser displays the VPN3002 Hardware Client Manager login screen.

Figure 1-1: VPN 3002 Hardware Client Manager login screen



To continue using HTTP for the whole session, skip to *Logging in the VPN 3002 Hardware Client Manager* on page 1-17.

Installing the SSL certificate in your browser

The Manager provides the option of using HTTP over SSL with the browser. SSL creates a secure session between your browser (VPN 3002 hardware client) and the VPN Concentrator (server). This protocol is known as HTTPS, and uses the `https://` prefix to connect to the server. The browser first authenticates the server, then encrypts all data passed during the session.

HTTPS is often confused with a similar protocol, S-HTTP (Secure HTTP), which encrypts only HTTP application-level data. SSL encrypts *all* data between client and server at the IP socket level, and is thus more secure.

SSL uses digital certificates for authentication. The VPN 3002 creates a self-signed SSL server certificate when it boots, and this certificate must be installed in the browser. Once the certificate is installed, you can connect using HTTPS. You need to install the certificate from a given VPN 3002 only once.

Managing the VPN 3002 is the same with or without SSL. Manager screens may take slightly longer to load with SSL because of encryption / decryption processing. When connected via SSL, the browser shows a locked-padlock icon on its status bar. Both Microsoft Internet Explorer and Netscape Navigator support SSL.

For HTTPS to work on the Public interface, you must enable HTTPS on the VPN 3002 through the CLI or from an HTTP session on the Private interface first. See

Follow these steps to install and use the SSL certificate for the first time. We provide separate instructions for Internet Explorer and Netscape Navigator when they diverge.

- 1 Connect to the VPN 3002 using HTTP as above.
- 2 On the login screen, click the **Install SSL Certificate** link.

The Manager displays the **Install SSL Certificate** screen and automatically begins to download and install its SSL certificate in your browser.

Figure 1-2: Install SSL Certificate screen



The installation sequence now differs depending on the browser. Continue below for Internet Explorer, or skip to *Installing the SSL certificate with Netscape* on page 1-9.

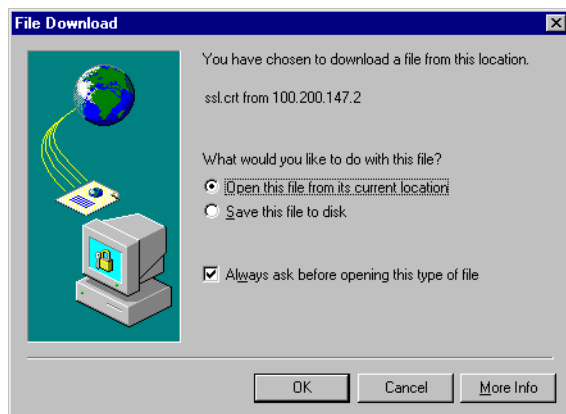
Installing the SSL certificate with Internet Explorer

This section describes SSL certificate installation using Microsoft Internet Explorer 5.0. (With Internet Explorer 4.0, some dialog boxes may differ but the process is similar.)

You need to install the SSL certificate from a given VPN 3002 only once. If you do reinstall it, the browser repeats all these steps each time.

A few seconds after the VPN 3002 Hardware Client Manager SSL screen appears, Internet Explorer displays a **File Download** dialog box that identifies the certificate filename and source, and asks whether to **Open** or **Save** the certificate. To immediately install the certificate in the browser, select **Open**. If you **Save** the file, the browser prompts for a location; you must then double-click on the file to install it.

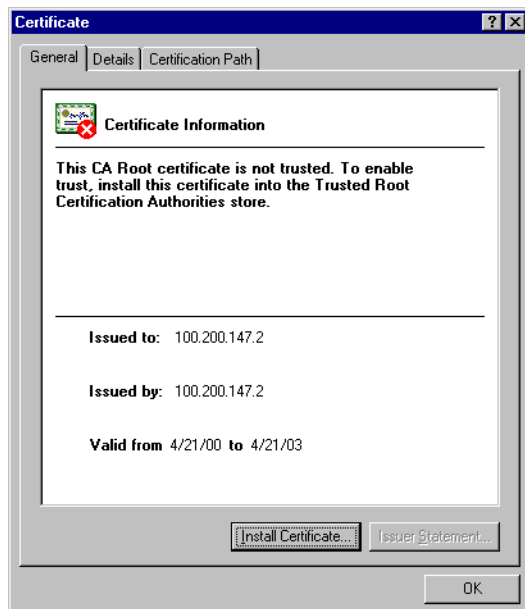
Figure 1-3: Internet Explorer File Download dialog box



3 Click the **Open this file from its current location** radio button, then click **OK**.

The browser displays the **Certificate** dialog box with information about the certificate. You must now install the certificate.

Figure 1-4: Internet Explorer Certificate dialog box



4 Click **Install Certificate**.

The browser starts a wizard to install the certificate. The certificate store is where such certificates are stored in Internet Explorer.

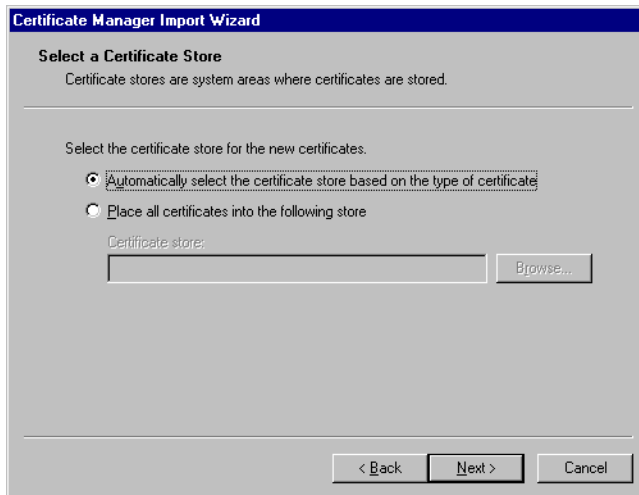
Figure 1-5: Internet Explorer Certificate Manager Import Wizard dialog box



5 Click **Next** to continue.

The wizard opens the next dialog box asking you to select a certificate store.

Figure 1-6: Internet Explorer Certificate Manager Import Wizard dialog box

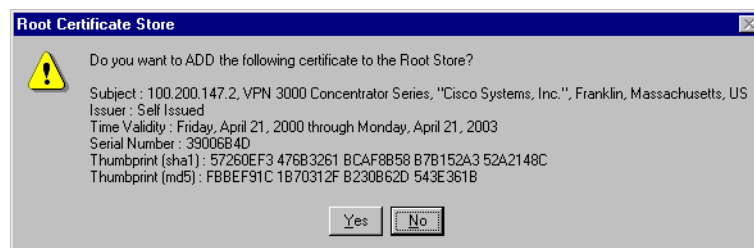
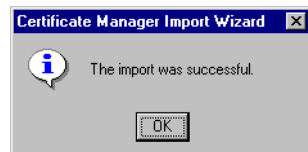


6 Let the wizard **Automatically select the certificate store**, and click **Next**.

The wizard opens a dialog box to complete the installation.

Figure 1-7: Internet Explorer Certificate Manager Import Wizard dialog box**7** Click **Finish**.

The wizard opens the **Root Certificate Store** dialog box asking you to confirm the installation.

Figure 1-8: Internet Explorer Root Certificate Store dialog box**8** To install the certificate, click **Yes**. This dialog box closes, and a final wizard confirmation dialog box opens.**Figure 1-9: Internet Explorer Certificate Manager Import Wizard final dialog box****9** Click **OK** to close this dialog box, and click **OK** on the **Certificate** dialog box (Figure 1-4) to close it. You can now connect to the VPN 3002 using HTTP over SSL (HTTPS).**10** On the Manager SSL screen (Figure 1-2), click the link that says, **After installing the SSL certificate, click here to connect to the VPN 3002 Hardware Client using SSL**.

Depending on how your browser is configured, you may see a **Security Alert** dialog box.

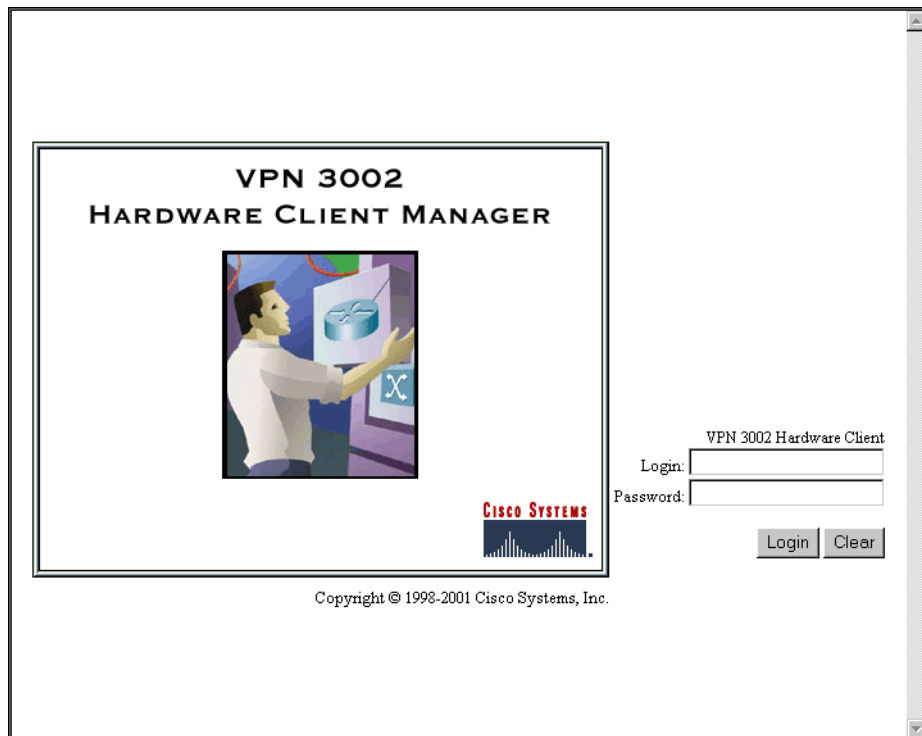
Figure 1-10: Internet Explorer Security Alert dialog box



11 Click **OK**.

The VPN 3002 Hardware Client displays the HTTPS version of the Manager login screen.

Figure 1-11: VPN 3002 Hardware Client Manager login screen using HTTPS (Internet Explorer)



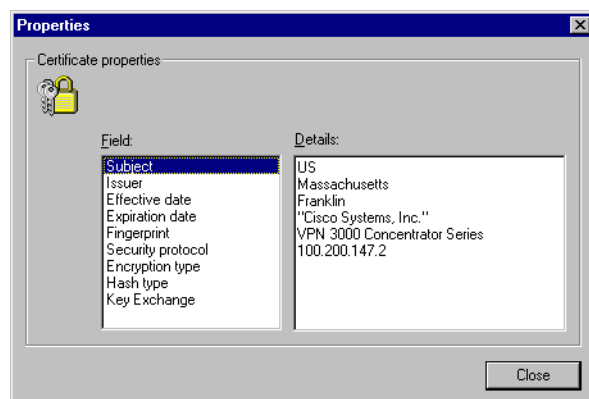
The browser maintains the HTTPS state until you close it or access an unsecure site; in the latter case you may see a **Security Alert** screen.

Proceed to *Logging in the VPN 3002 Hardware Client Manager* on page 1-17 to log in as usual.

Viewing certificates with Internet Explorer

There are (at least) two ways to examine certificates stored in Internet Explorer.

First, note the padlock icon on the browser status bar in Figure 1-11. If you double-click on the icon, the browser opens a **Certificate Properties** screen showing details of the specific certificate in use.

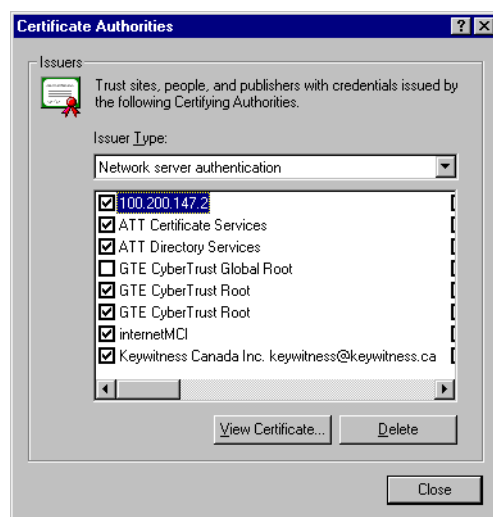
Figure 1-12: Internet Explorer 4.0 Certificate Properties screen

Click any of the **Field** items to see **Details**. Click **Close** when finished.

Second, you can view all the certificates that are stored in Internet Explorer 4.0. Click the browser **View** menu and select **Internet Options**. Click the **Content** tab, then click **Authorities** in the **Certificates** section.

In Internet Explorer 5.0, click the browser **Tools** menu and select **Internet Options**. Click the **Content** tab, then click **Certificates** in the **Certificates** section. On the **Certificate Manager**, click the **Trusted Root Certification Authorities** tab.

The VPN 3002 Hardware Client SSL certificate name is its Ethernet 1 (Private) IP address.

Figure 1-13: Internet Explorer 4.0 Certificate Authorities list

Select a certificate, then click **View Certificate**. The browser displays the **Certificate Properties** screen, as in Figure 1-12 above.

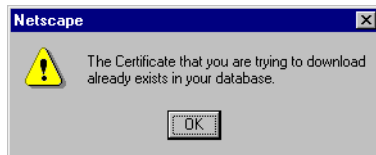
Installing the SSL certificate with Netscape

This section describes SSL certificate installation using Netscape Navigator / Communicator 4.5.

Reinstallation

You need to install the SSL certificate from a given VPN 3002 only once. If you try to reinstall it, Netscape displays the note in Figure 1-14. Click **OK** and just connect to the VPN 3002 using SSL (see Step 7 on page 1-13).

Figure 1-14: Netscape reinstallation note



First-time installation

The instructions below follow from Step 2 on page 1-4 and describe first-time certificate installation.

A few seconds after the VPN 3002 Hardware Client Manager SSL screen appears, Netscape displays a **New Certificate Authority** screen.

Figure 1-15: Netscape New Certificate Authority screen 1



1 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which further explains the process.

Figure 1-16: Netscape New Certificate Authority screen 2

2 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which lets you examine details of the VPN 3002 Hardware Client SSL certificate.

Figure 1-17: Netscape New Certificate Authority screen 3

3 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, with choices for using the certificate. No choices are checked by default.

Figure 1-18: Netscape New Certificate Authority screen 4



- 4 You must check at least the first box, **Accept this Certificate Authority for Certifying network sites**. Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which lets you choose to have the browser warn you about sending data to the VPN 3002.

Figure 1-19: Netscape New Certificate Authority screen 5



- 5 Checking the box is optional. Doing so means that you get a warning whenever you apply settings on a Manager screen, so it's probably less intrusive to manage the VPN 3002 without those warnings. Click **Next>** to proceed.

Netscape displays the final **New Certificate Authority** screen, which asks you to name the certificate.

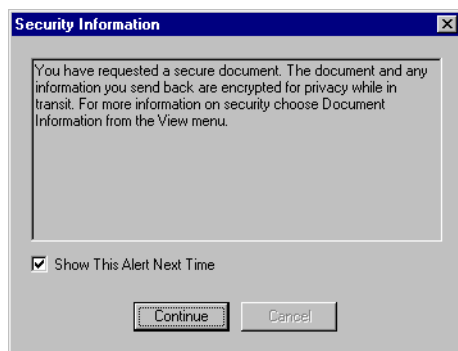
Figure 1-20: Netscape New Certificate Authority screen 6

- 6** In the **Nickname** field, enter a descriptive name for this certificate. “Nickname” is something of a misnomer. We suggest you use a clearly descriptive name such as `Cisco VPN 3002 10.10.147.2`. This name appears in the list of installed certificates; see *Viewing certificates with Netscape* below. Click **Finish**.

You can now connect to the VPN 3002 using HTTP over SSL (HTTPS).

- 7** On the Manager SSL screen (Figure 1-2), click the link that says, **After installing the SSL certificate, click here to connect to the VPN 3002 Hardware Client using SSL**.

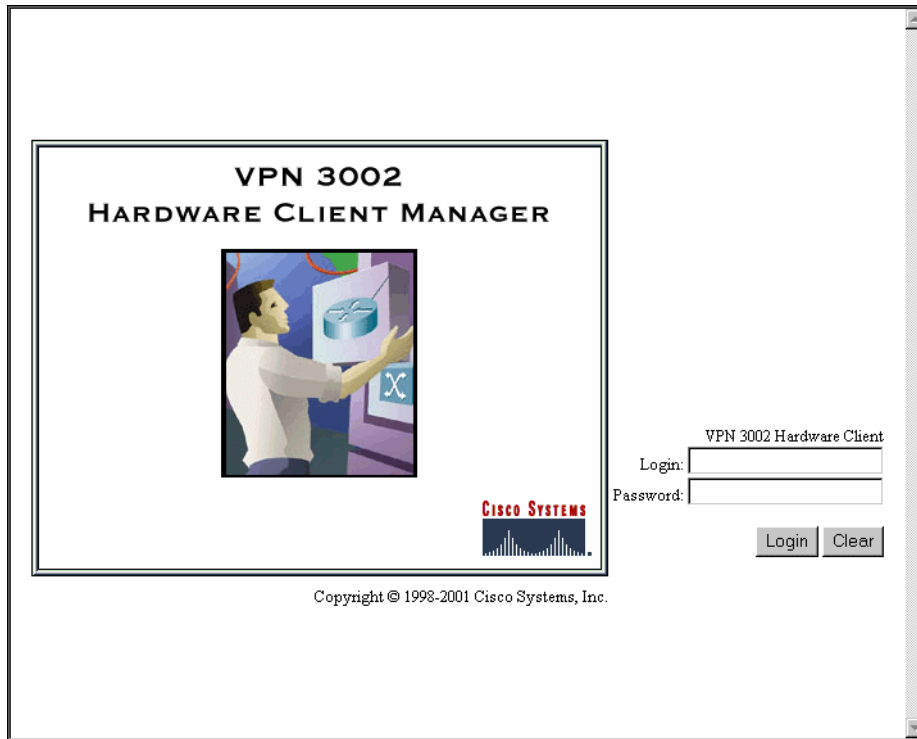
Depending on how your browser is configured, you may see a **Security Information Alert** dialog box.

Figure 1-21: Netscape Security Information Alert dialog box

- 8** Click **Continue**.

The VPN 3002 displays the HTTPS version of the Manager login screen.

Figure 1-22: VPN 3002 Hardware Client Manager login screen using HTTPS (Netscape)



The browser maintains the HTTPS state until you close it or access an unsecure site; in the latter case, you may see a **Security Information Alert** dialog box.

Proceed to *Logging in the VPN 3002 Hardware Client Manager* on page 1-17 to log in as usual.

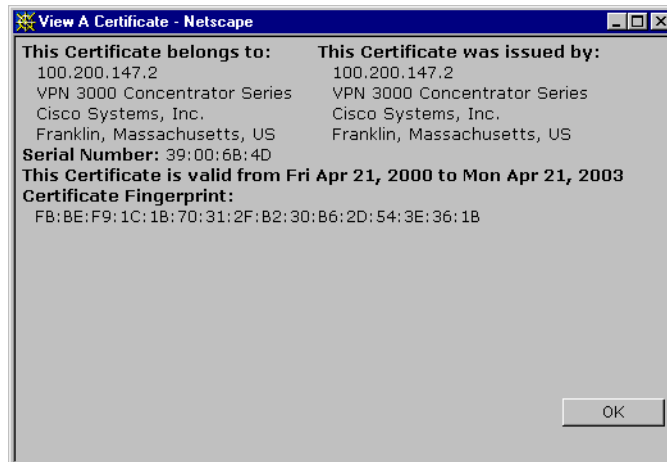
Viewing certificates with Netscape

There are (at least) two ways to examine certificates stored in Netscape Navigator / Communicator 4.5.

First, note the locked-padlock icon on the bottom status bar in Figure 1-22. If you click on the icon, Netscape opens a **Security Info** window. (You can also open this window by clicking **Security** on the Navigator Toolbar at the top of the Netscape window.)

Figure 1-23: Netscape Security Info window

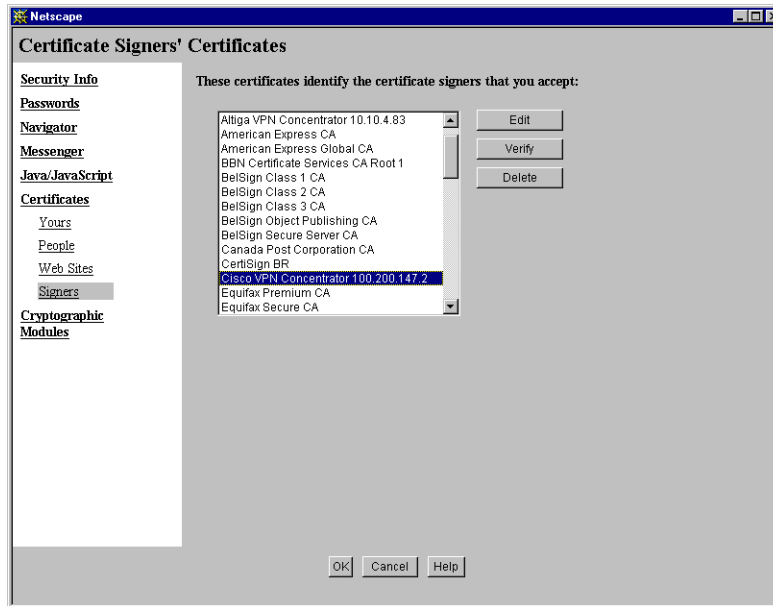
Click **View Certificate** to see details of the specific certificate in use.

Figure 1-24: Netscape View Certificate screen

Click **OK** when finished.

Second, you can view all the certificates that are stored in Netscape. On the **Security Info** window, select **Certificates** then **Signers**. The “nickname” you entered in Step 6 identifies the VPN 3002 Hardware Client SSL certificate.

Figure 1-25: Netscape Certificates Signers list



Select a certificate, then click **Edit**, **Verify**, or **Delete**. Click **OK** when finished.

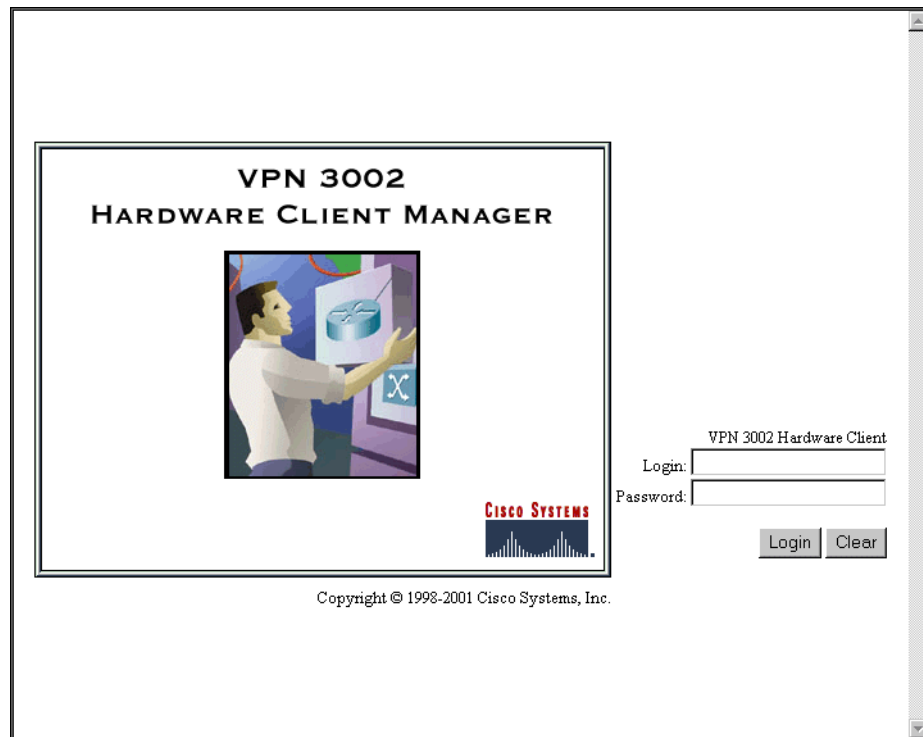
Connecting to the VPN 3002 using HTTPS

Once you have installed the SSL certificate in the browser, you can connect directly using HTTPS.

- 1 Bring up the browser.
- 2 In the browser **Address** or **Location** field, enter `https://` plus the VPN 3002 private interface IP address; for example, `https://10.10.147.2`.

The browser displays the VPN 3002 Hardware Client Manager HTTPS login screen.

A locked-padlock icon on the browser status bar indicates an HTTPS session. Also, this login screen does not include the **Install SSL Certificate** link.

Figure 1-26: VPN Hardware Client Manager HTTPS login screen

Logging in the VPN 3002 Hardware Client Manager

Logging in the VPN 3002 Hardware Client Manager is the same for both types of connections: cleartext HTTP or secure HTTPS.

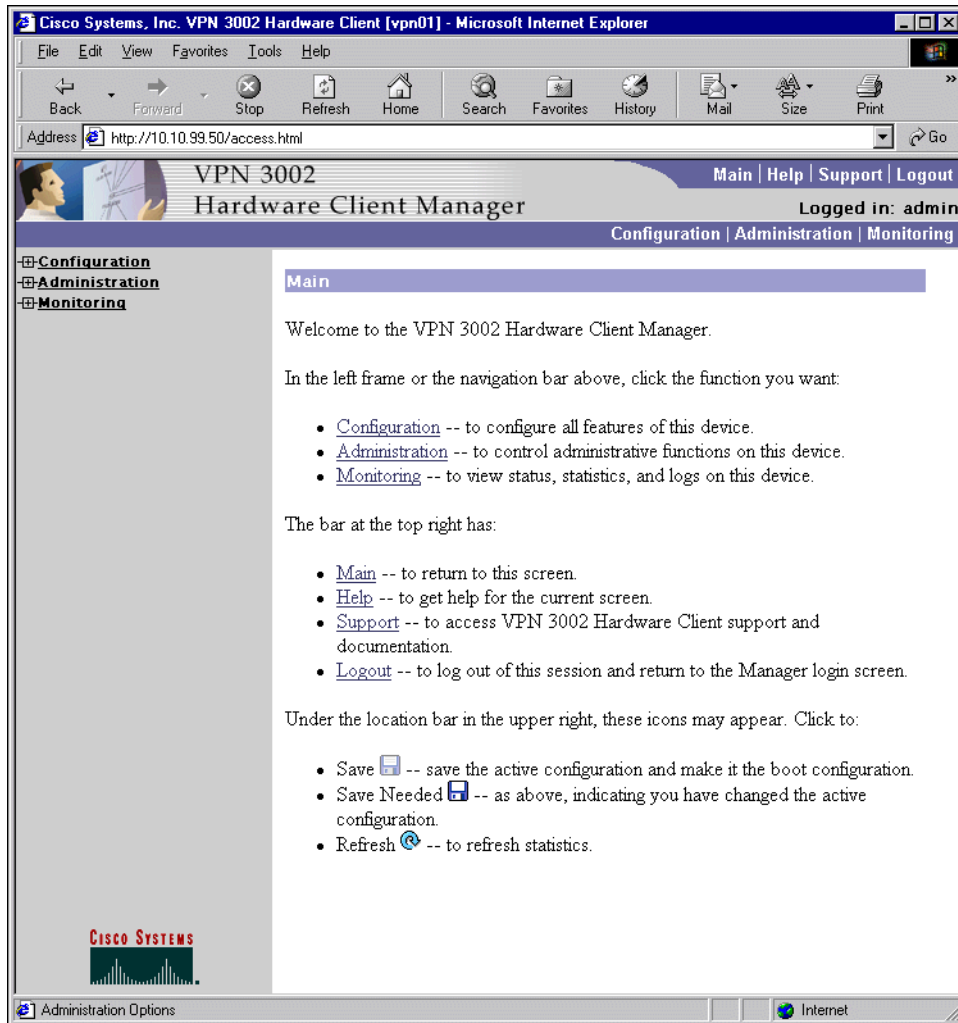
Entries are case-sensitive. With Microsoft Internet Explorer, you can press the **Tab** key to move from field to field; other browsers may work differently. If you make a mistake, click the **Clear** button and start over.

The entries that follow are the factory-supplied default entries. If you have changed them, use your entries.

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

The Manager displays the main welcome screen.

Figure 1-27: Manager Main Welcome screen



From here you can navigate the Manager using either the table of contents in the left frame, or the Manager toolbar in the top frame.

Configuring HTTP, HTTPS, and SSL parameters

HTTP, HTTPS, and SSL are enabled by default on the VPN 3002, and they are configured with recommended parameters that should suit most administration tasks and security requirements.

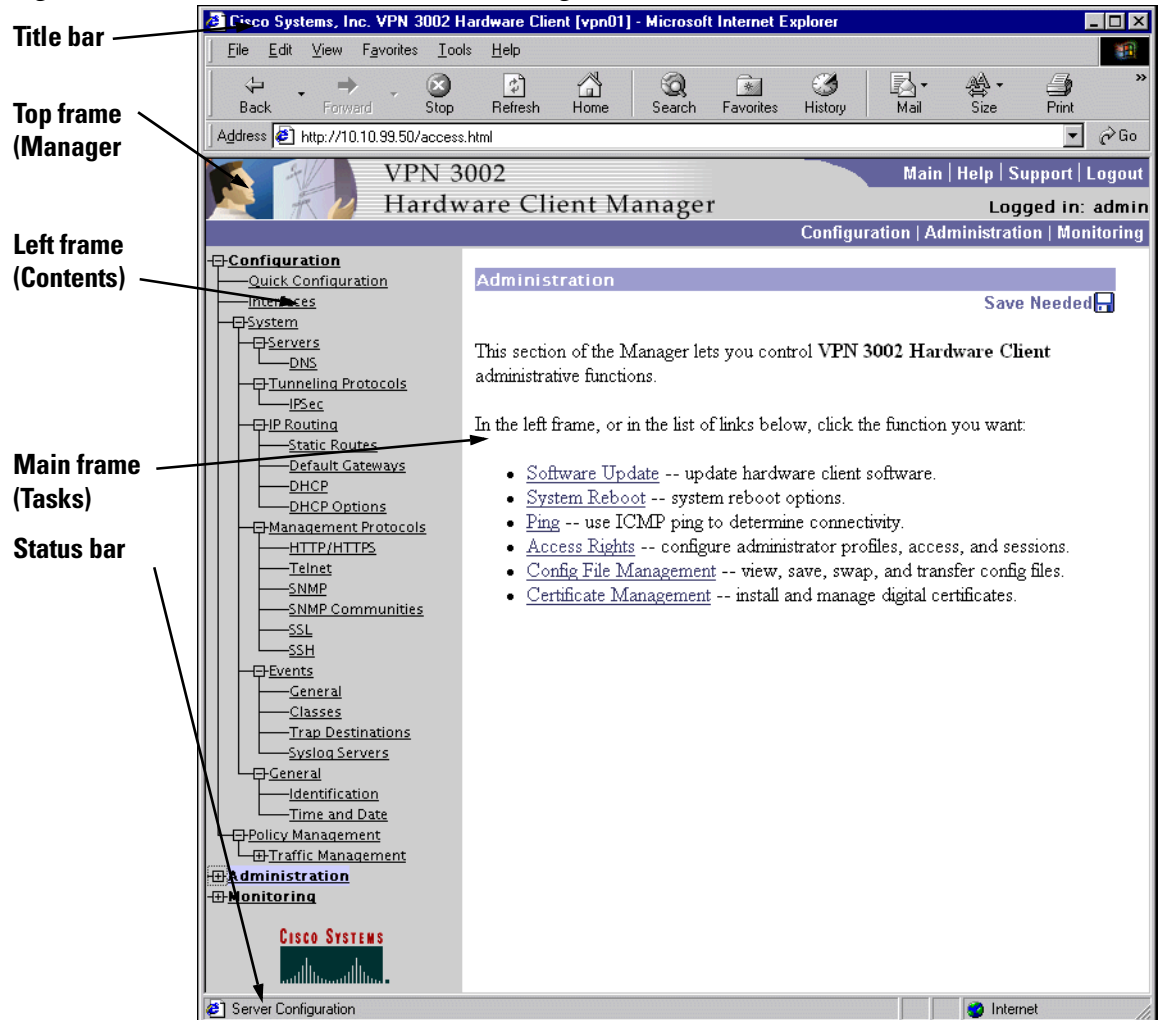
To configure HTTP and HTTPS parameters, see the **Configuration | System | Management Protocols | HTTP/HTTPS** screen.

To configure SSL parameters, see the **Configuration | System | Management Protocols | SSL** screen.

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 1-28: VPN 3002 Hardware Client Manager window.



Title bar

The title bar at the top of the browser window includes the VPN3002 device name or IP address in brackets; e.g., [10.10.104.7].

Status bar

The status bar at the bottom of the browser window displays explanatory messages for selected items and Manager activity.

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.

Main tab **Main**

Click to go to the main Manager screen, and to close all subordinate sections and titles in the left frame.

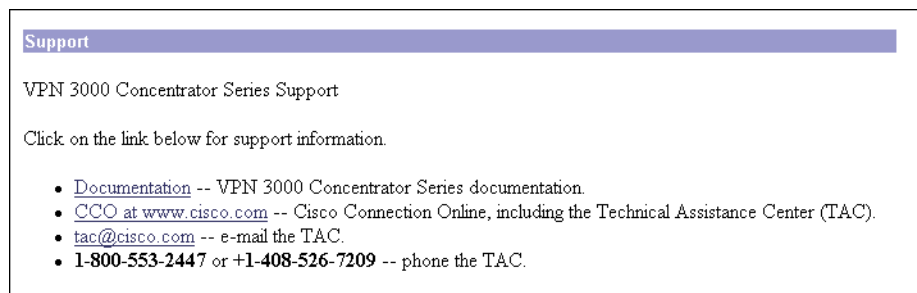
Help tab **Help**

Click to open context-sensitive online help. Help opens in a separate browser window that you can move or resize as you wish. Close the help window when you are finished.

Support tab **Support**

Click to open a Manager screen with links to Cisco support and documentation resources.

Figure 1-29: Support screen



Documentation

Click this link to open a browser window on the Cisco Technical Documentation Web page for Virtual Private Networks. That page has links to VPN 3000 Concentrator Series and VPN 3002 Hardware Client documentation in PDF format. (To view the PDF files, you need Adobe® Acrobat® Reader 3.0 or later, and version 4.0 is included on the VPN 3000 Concentrator Series software CD-ROM.) When you finish, close the documentation browser window and return to the Manager.

CCO at www.cisco.com

Click this link to open a browser window on the main Cisco Web page, Cisco Connection Online (CCO). From that page, you can browse to all Cisco resources, including the Technical Assistance Center (TAC). When you finish, close the CCO browser window and return to the Manager.

tac@cisco.com

Click this link to open your configured email application and compose an email message to Cisco's Technical Assistance Center (TAC). When you finish, the application closes and returns to this **Support** screen.

Logout tab

Click 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 tab

Click 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 Administration or Monitoring pages in the left frame.

Administration tab

Click 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 Configuration or Monitoring pages in the left frame.

Monitoring tab

Click 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 Configuration or Administration pages in the left frame.

Save

The Save button displays in the detailed configuration screens. Click 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 you have changed the active configuration. Click 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 Hardware Client without **saving** the active configuration, any configuration changes are lost.* Clicking this reminder saves the active configuration as the boot configuration and restores the **Save** reminder.

In Quick Configuration, as in the detailed configuration screens, you changes take effect immediately and become the active configuration. There is a difference, however, in that the Manager saves the new

configuration automatically when you reach the **Done** screen, and there is neither the **Save** or **Save Needed** button.

Refresh

Click 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.



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

Left frame (Table of contents)

The left frame provides a table of contents to Manager screens. 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 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 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.

Organization of the VPN 3002 Hardware Client Manager

The VPN 3002 Hardware Client Manager consists of three major sections and many subsections:

- **Configuration:** setting all the parameters for the VPN 3002 that govern its use and functionality as a VPN device:
 - **Quick Configuration:** supplying the minimal parameters needed to make the VPN 3002 operational.
 - **Interfaces:** Ethernet parameters.

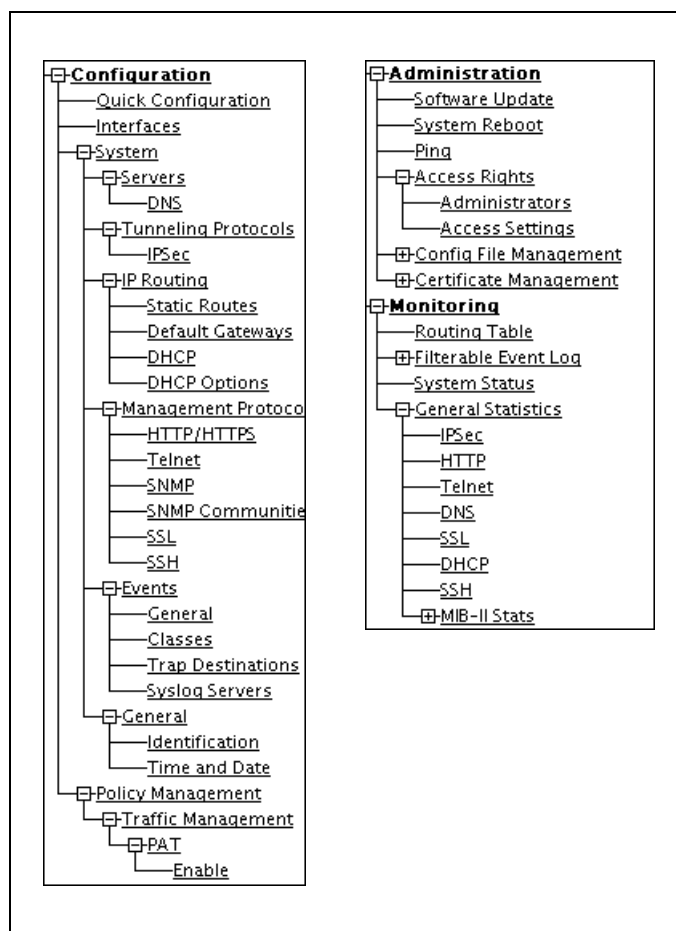
- **System:** parameters for system-wide functions such as server access, IPSec tunneling protocol, built-in management servers, event handling, and system identification.
- **Policy Management:** enabling PAT (Port Address Translation).
- **Administration:** managing higher level functions that keep the VPN3002 operational and secure, such as who is allowed to configure the system, what software runs on it, and managing its configuration files and digital certificates.
- **Monitoring:** viewing routing tables, event logs, system LEDs and status, and data on user sessions

This manual covers all these topics. For Quick Configuration, see the *VPN 3002 Hardware Client Getting Started* manual.

Navigating the VPN 3002 Hardware Client Manager

Your primary tool for navigating the VPN 3002 Hardware Client Manager is the table of contents in the left frame. Figure 1-30 shows all its entries, completely expanded. (The figure shows the frame in multiple columns, but the actual frame is a single column. Use the scroll controls to move up and down the frame.)

Figure 1-30: Complete Manager Table of Contents





Configuration

Configuring the VPN 3002 means setting all the parameters that govern its use and functionality as a VPN device.

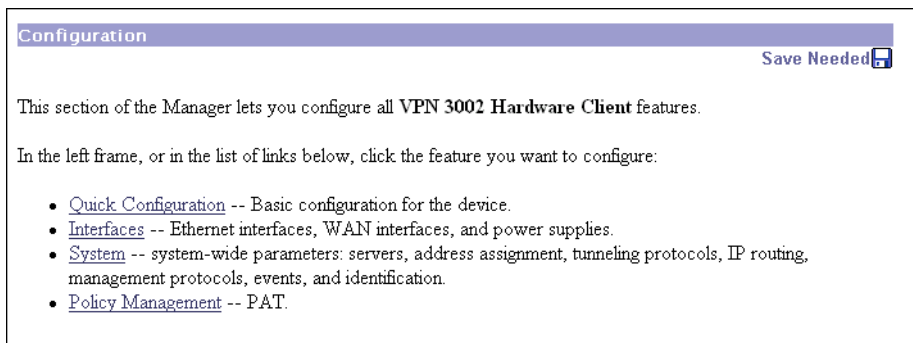
Cisco supplies default parameters that cover typical installations and uses; and once you supply minimal parameters in Quick Configuration, the system is operational. But to tailor the system to your needs, and to provide an appropriate level of system security, you can configure the system in detail.

Configuration

This section of the Manager lets you configure all VPN 3002 features and functions.

- **Quick Configuration:** the minimal parameters needed to make the VPN 3002 operational. For more information, use online Help, or see the *VPN 3002 Getting Started* manual, available online only.
- **Interfaces:** parameters specific to the Private and Public interfaces.
- **System:** parameters for system-wide functions: server access, IPSec, IP routing, built-in management servers, system events, and system identification.
- **Policy Management:** enabling or disabling PAT (Protocol Address Translation).

Figure 2-1: Configuration screen



See the appropriate chapter in this manual for each section of the Manager. Online help is available for all sections.



Interfaces

This section of the VPN 3002 Hardware Client Manager applies functions that are interface-specific, rather than system-wide.

You configure two network interfaces for the VPN 3002 to operate as a VPN device: the Private interface and the Public interface. If you used Quick Configuration as described in the *VPN 3002 Hardware Client Getting Started* manual, the system supplied many default parameters for the interfaces. Here you can configure them explicitly.

The VPN 3002 includes some IP routing functions: static routes, and DHCP. You configure static routes, the default gateway, and DHCP in the IP Routing section; see the **Configuration | System | IP Routing** screens.

Configuration | Interfaces

This section lets you configure the Private and Public interfaces.

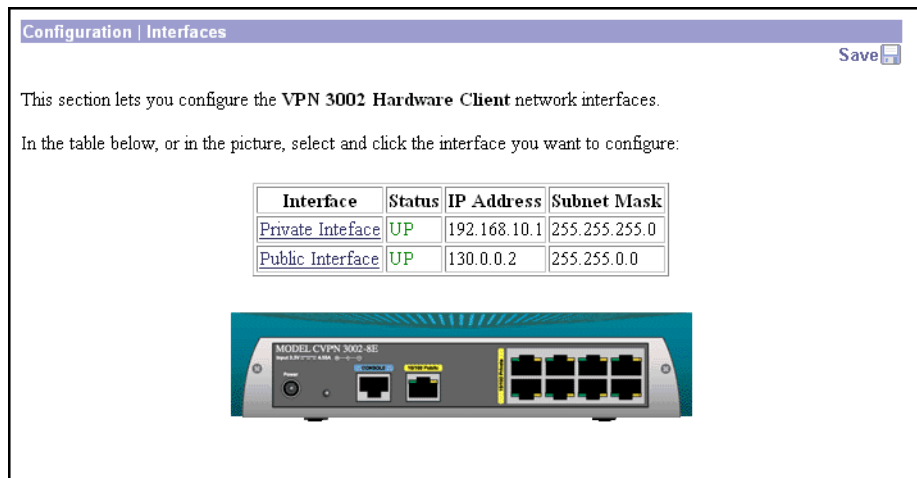
- Private is the interface to your private network (internal LAN).
- Public is the interface to the public network.

Configuring an Ethernet interface includes supplying an IP address and subnet mask, and setting speed and transmission mode.

Note: Interface settings take effect as soon as you apply them. If the system is in active use, changes may affect tunnel traffic.

The table shows all installed interfaces and their status.

Figure 3-1: VPN 3002-8E Configuration | Interfaces screen



To configure a module, either click the appropriate link in the status table; or use the mouse pointer to select the module on the back-panel image, and click anywhere in the highlighted area.

Interface

The VPN3002 interface installed in the system. To configure an interface, click the appropriate link.

Private, Public

To configure Ethernet interface parameters, click the appropriate highlighted link in the table or click in a highlighted module on the back-panel image. See **Configuration | Interfaces | Private/Public**.

Status

The operational status of this interface

PWR green = Configured, enabled, and operational; ready to pass data traffic.

SYS flashing amber = Configured but disabled or disconnected.

Testing = In test mode; no regular data traffic can pass.

Dormant = (Red) Configured and enabled but waiting for an external action, such as an incoming connection.

Not Present = (Red) Missing hardware components.

Lower Layer Down = (Red) Not operational because a lower-layer interface is down.

Unknown = (Red) Not configured or not able to determine status.

Not Configured = Present but not configured.

Waiting for DHCP = Waiting for DHCP to assign an IP address.

IP Address

The IP address configured on this interface.

Subnet Mask

The subnet mask configured on this interface.

Configuration | Interfaces | Private

This screen lets you configure parameters for the Private Interface. It displays the current parameters, if any.

Figure 3-2: Configuration | Interfaces | Private screen

The screenshot shows a configuration window titled "Configuration | Interfaces | Private". At the top, there is a warning icon and a message: "You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen." Below this, the section "Configuring the Private Interface." contains several settings:

- Enabled**: A checked checkbox with the instruction "Check to enable this interface."
- IP Address**: A text input field containing "10.10.99.50" with the instruction "Enter the IP address for this interface."
- Subnet Mask**: A text input field containing "255.255.0.0" with the instruction "Enter the subnet mask for this interface."
- MAC Address**: A text input field containing "00.90.A4.00.25.A8" with the instruction "The MAC address for this interface."
- Speed**: A dropdown menu set to "10/100 auto" with the instruction "Select the speed for this interface."
- Duplex**: A dropdown menu set to "Auto" with the instruction "Select the duplex mode for this interface."

At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

Caution:

If you modify any parameters of the Private 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 from the login screen.

Enabled

To make the interface functional and online, check **Enabled**. If not enabled, the interface is offline; this state lets you retain or change its configuration parameters while it is offline.

If the interface is configured but disabled (offline), the appropriate **Ethernet Link Status** LED blinks green on the VPN 3002 front panel.

IP Address

Enter the IP address for this interface, using dotted decimal notation (e.g., 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (e.g., 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 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. Note that 0.0.0.0 is not allowed.

MAC Address

This is the unique hardware MAC (Medium Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Speed

Click the drop-down menu button and select the interface speed:

10 Mbps = Fix the speed at 10 megabits per second (10Base-T networks)

100 Mbps = Fix the speed at 100 megabits per second (100Base-T networks)

10/100 auto = Let the VPN 3002 automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Duplex

Click the drop-down menu button and select the interface transmission mode:

Auto = Let the VPN 3002 automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.

Full-Duplex = Fix the transmission mode as full duplex: transmits and receives at the same time.

Half-Duplex = Fix the transmission mode as half duplex: transmits or receives, but not at the same time.

Apply / Cancel

To apply your settings to the system and include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | Interfaces** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Interfaces** screen.

Configuration | Interfaces | Public

This screen lets you configure general interface parameters for the Public interface.

Figure 3-3: Configuration | Interfaces | Public screen

The screenshot shows the 'Configuration | Interfaces | Public' screen. At the top, there is a title bar with the text 'Configuration | Interfaces | Public'. Below the title bar, the main heading is 'Configuring the Public Interface.' The screen contains several configuration options:

- Enabled**: A checkbox that is checked. To its right is the text 'Check to enable this interface.'
- DHCP Client**: A checkbox that is checked. To its right is the text 'Check to obtain/renew the IP Address, Subnet Mask and Default Gateway via DHCP. Uncheck to disable/release these DHCP parameters.'
- No DHCP Lease Acquired**: A text label positioned above the IP and Subnet Mask fields.
- IP Address**: A text input field containing '0.0.0.0'. To its right is the text 'Enter the IP address for this interface.'
- Subnet Mask**: A text input field containing '0.0.0.0'. To its right is the text 'Enter the subnet mask for this interface.'
- MAC Address**: A text input field containing '00.90.A4.00.25.A9'. To its right is the text 'The MAC address for this interface.'
- Speed**: A dropdown menu with '10/100 auto' selected. To its right is the text 'Select the speed for this interface.'
- Duplex**: A dropdown menu with 'Auto' selected. To its right is the text 'Select the duplex mode for this interface.'

At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

Enabled

To make the interface functional and online, check **Enabled**. If not enabled, the interface is offline; this state lets you retain or change its configuration parameters while it is offline.

DHCP Client

Check this box if you want to obtain the IP address and subnet mask for this interface via DHCP. If you check this box, you don't make entries in the IP address and subnet mask parameters that follow.

IP Address

Enter the IP address for this interface, using dotted decimal notation (e.g., 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (e.g., 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 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. Note that 0.0.0.0 is not allowed.

MAC Address

This is the unique hardware MAC (Medium Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Speed

Click the drop-down menu button and select the interface speed:

10 Mbps = Fix the speed at 10 megabits per second (10Base-T networks)

100 Mbps = Fix the speed at 100 megabits per second (100Base-T networks)

10/100 auto = Let the VPN 3002 automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Duplex

Click the drop-down menu button and select the interface transmission mode:

Auto = Let the VPN 3002 automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.

Full-Duplex = Fix the transmission mode as full duplex: transmits and receives at the same time.

Half-Duplex = Fix the transmission mode as half duplex: transmits or receives, but not at the same time.

Apply / Cancel

To apply your settings to this interface and include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | Interfaces** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Interfaces** screen.



System Configuration

System configuration means configuring parameters for system-wide functions in the VPN 3002.

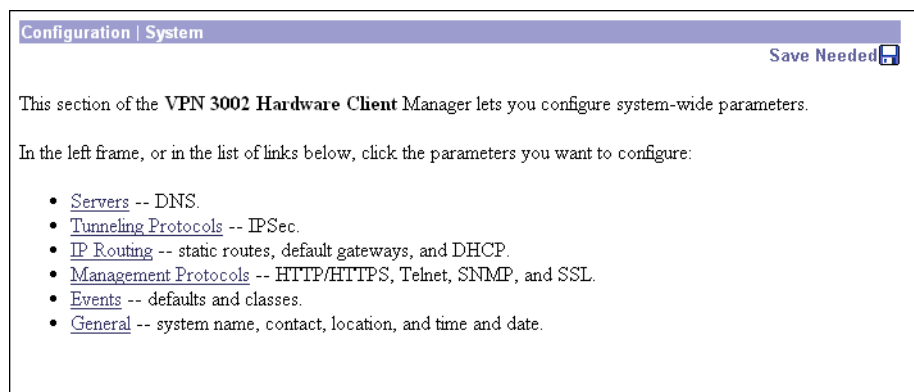
Configuration | System

This section of the Manager lets you configure parameters for:

- **Servers:** identifying servers for DNS information for the VPN 3002.
- **Tunneling Protocols:** configuring IPSec connections.
- **IP Routing:** configuring static routes, default gateways, and DHCP.
- **Management Protocols:** configuring and enabling built-in servers for HTTP/HTTPS, Telnet, SNMP, SSL and SSH.
- **Events:** handling system events via logs, SNMP traps, and syslog.
- **General:** identifying the system and setting the time and date.

See the appropriate chapter in this manual or the online help for each section.

Figure 4-1: Configuration | System screen





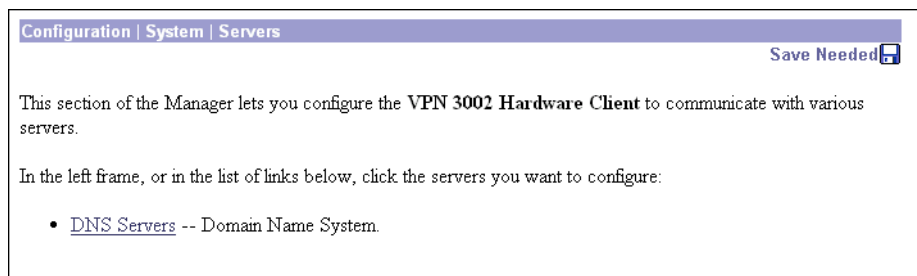
Servers

Configuring servers means identifying them to the VPN 3002 so it can communicate with them correctly. For the VPN 3002, these are DNS servers that convert hostnames to IP addresses. The VPN 3002 functions as a client of these servers.

Configuration | System | Servers

This section of the Manager lets you configure the VPN 3002 to communicate with DNS servers.

Figure 5-1: Configuration | System | Servers screen



Configuration | System | Servers | DNS

This screen lets you configure the Domain Name System (DNS) servers for the VPN 3002. DNS servers convert domain names to IP addresses. Configuring DNS servers here lets you enter hostnames (e.g., mail01) rather than IP addresses as you configure and manage the VPN 3002.

You can configure up to three DNS servers that the system queries in order.

Note:

DNS information that you add here is for the VPN 3002 only. PCs located behind the VPN 3002 on the private network get DNS information that is configured on the central-site Concentrator in the Group settings for the VPN 3002.

Figure 5-2: Configuration | System | Servers | DNS screen

Configuration | System | Servers | DNS

Configure system-wide DNS (Domain Name System) servers.

i Configuring DNS is optional, but it lets you use hostnames rather than IP addresses.

Enabled

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Timeout Period seconds

Timeout Retries

Apply Cancel

Enabled

To use DNS functions, check **Enabled** (the default). To disable DNS, clear the box.

Domain

Enter the name of the registered domain of the ISP for the VPN 3002; e.g., `yourisp.com`. Maximum 48 characters. This entry is sometimes called the domain name suffix or sub-domain. The DNS system within the VPN 3002 automatically appends this domain name to hostnames before sending them to a DNS server for resolution.

Primary DNS Server

Enter the IP address of the primary DNS server, using dotted decimal notation; e.g., `192.168.12.34`. Be sure this entry is correct to avoid DNS resolution delays.

Secondary DNS Server

Enter the IP address of the secondary (first backup) DNS server, using dotted decimal notation. If the primary DNS server doesn't respond to a query within the **Timeout Period** specified below, the system queries this server.

Tertiary DNS Server

Enter the IP address of the tertiary (second backup) DNS server, using dotted decimal notation. If the secondary DNS server doesn't respond to a query within the **Timeout Period** specified below, the system queries this server.

Timeout Period

Enter the initial time in seconds to wait for a response to a DNS query before sending the query to the next server. Minimum is 1, default is 2, maximum is 30 seconds. This time doubles with each retry cycle through the list of servers.

Timeout Retries

Enter the number of times to retry sending a DNS query to the configured servers, in order. In other words, this is the number of times to cycle through the list of servers before returning an error. Minimum is 0, default is 2, maximum is 10 retries.

Apply / Cancel

To apply your settings for DNS servers and include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Servers** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Servers** screen.



Tunneling

Tunneling is the heart of virtual private networking. The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

The secure connection is called a tunnel, and the VPN 3002 uses the IPSec tunneling protocol to:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint.

The VPN 3002 functions as a bidirectional tunnel endpoint: it can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination; or it can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

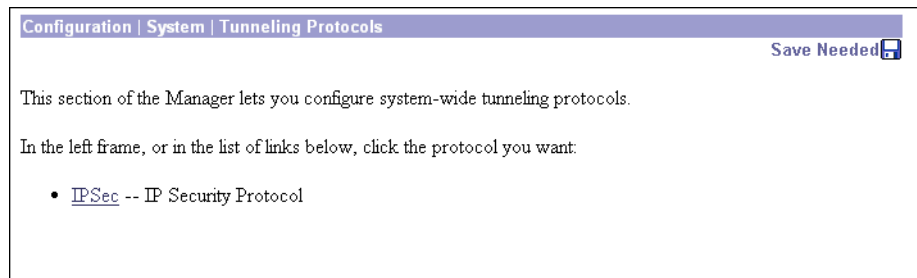
This section explains how to configure the IPSec tunneling protocol.

Configuration | System | Tunneling Protocols

This section lets you configure the IPSec tunneling protocol.

- 1 Click **IPSec**.

Figure 6-1: Configuration | System | Tunneling Protocols screen



Configuration | System | Tunneling Protocols | IPSec

The VPN 3002 complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol.

In IPSec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPSec SA).

The VPN 3002 initiates all tunnels with the VPN Concentrator; the Concentrator functions only as responder. The VPN 3002 as initiator propose SAs; the responder accepts, rejects, or makes counter-proposals—all according to configured SA parameters. To establish a connection, both entities must agree on the SAs.

The Cisco VPN 3002 supports these IPSec attributes, but they are configurable on the central-site Concentrator, not on the VPN 3002:

- Main mode for negotiating phase one of establishing ISAKMP Secure Associations (SAs)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1 and 2
- Encryption Algorithms:
 - DES-56
 - 3DES-168
- Extended Authentication (XAuth)

- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode

Figure 6-2: Configuration | System | Tunneling Protocols | IPSec screen

Configuration | System | Tunneling Protocols | IPSec

Enter the information needed to connect to the central-site VPN Concentrator peer.

Peer Address

Use Certificate [Click to use the installed certificate.](#)

	Name	Password	Verify
Group	<input type="text" value="3002Group"/>	<input type="password" value="*****"/>	<input type="password" value="*****"/>
User	<input type="text" value="3002user"/>	<input type="password" value="*****"/>	<input type="password" value="*****"/>

Peer Address

Enter the IP address or hostname of the remote IKE peer. This is the IP address or hostname of the public interface on the VPN Concentrator to which this VPN 3002 connects. Use dotted decimal notation; e.g., 192.168.34.56.

Use Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under **Administration | Certificate Management**, which is where you install digital certificates on the VPN 3002.

Check the box to use digital certificates.

Group

The VPN 3002 connects to the VPN 3000 Series Concentrator using this Group name and password, which must be configured on the central-site Concentrator. Group and user names and passwords must be identical on the VPN 3002 and on the Concentrator to which it connects.

Name

In the **Group Name** field, enter a unique name for the group to which this VPN 3002 belongs. This is the group name configured on the central-site Concentrator to which this VPN 3002 connects. Maximum is 32 characters, case-sensitive.

Password

In the **Group Password** field, enter a unique password for this group. This is the group password configured on the Concentrator to which this VPN 3002 connects. Minimum is 4, maximum is 32 characters, case-sensitive. The field displays only asterisks.

Verify

In the **Group Verify** field, re-enter the group password to verify it. The field displays only asterisks.

User

You must also enter a username and password, and they must match the username and password configured on the central-site Concentrator to which this VPN 3002 connects.

Name

In the **User Name** field, enter a unique name for the user in this group. Maximum is 32 characters, case-sensitive. This is the user name configured on the central-site Concentrator to which this VPN 3002 connects. Maximum is 32 characters, case-sensitive.

Password

In the **User Password** field, enter the password for this user. This is the user password configured on the central-site Concentrator to which this VPN 3002 connects. Minimum is 4, maximum is 32 characters, case-sensitive.

Verify

In the **User Verify** field, re-enter the user password to verify it. The field displays only asterisks.



IP Routing

The VPN 3002 itself includes an IP routing subsystem with static routing, default gateways, and DHCP.

To route packets, the subsystem uses static routes and the default gateway. If you don't configure the default gateway, the subsystem drops packets that it can't otherwise route.

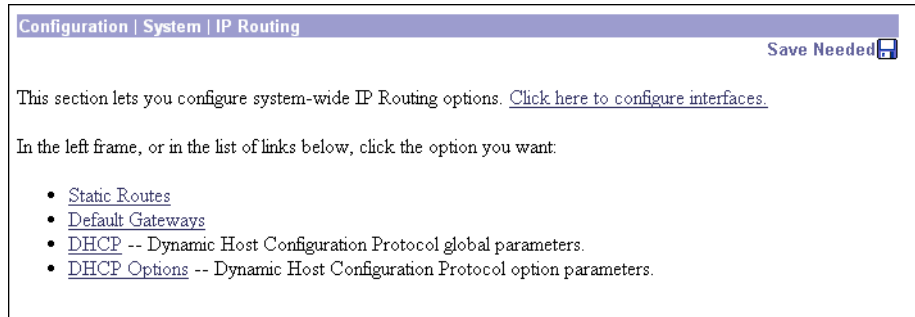
You configure static routes and default gateways in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) server parameters.

Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters.

- **Static Routes:** manually configured routing tables.
- **Default Gateways:** routes for otherwise unrouted traffic.
- **DHCP:** Dynamic Host Configuration Protocol global parameters.
- **DHCP Options:** facilities that allow the VPN 3002 DHCP server to respond with configurable parameters for specific kinds of devices such as PCs, IP telephones, print servers, etc., as well as an IP address.

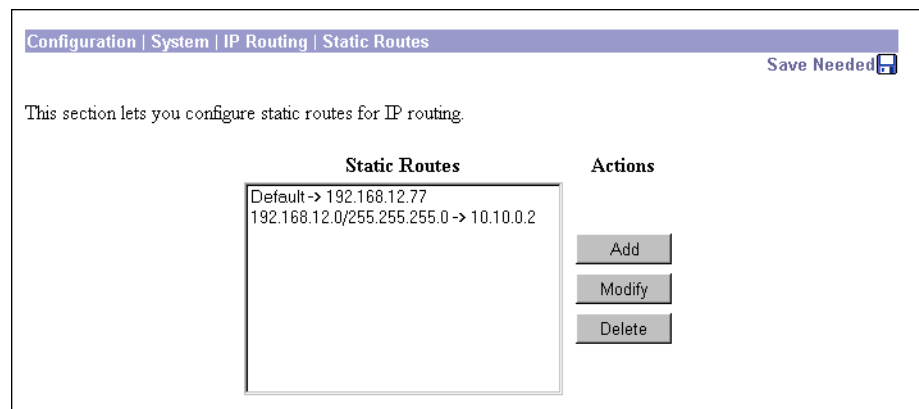
Figure 7-1: Configuration | System | IP Routing screen



Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing.

Figure 7-2: Configuration | System | IP Routing | Static Routes screen



Static Routes

The **Static Routes** list shows manual IP routes that have been configured. The format is [destination network address/subnet mask -> outbound destination]; e.g., 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as [Default -> default router address]. If no static routes have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the **Configuration | System | IP Routing | Static Routes | Add** screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the **Configuration | System | IP Routing | Static Routes | Modify** screen. If you select the default gateway, the Manager opens the **Configuration | System | IP Routing | Default Gateways** screen.

To delete a configured static route, select the route from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the **Configuration | System | IP Routing | Default Gateways** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

Add: Configure and add a new static, or manual, route to the IP routing table.

Modify: Modify the parameters for a configured static route.

Figure 7-3: Configuration | System | IP Routing | Static Routes | Add or Modify screen

The screenshot shows two overlapping windows. The top window is titled 'Configuration | System | IP Routing | Static Routes | Modify' and contains the text 'Modify a configured static route.' The bottom window is titled 'Configuration | System | IP Routing | Static Routes | Add' and contains the text 'Configure and add a static route.' Below this text are several input fields: 'Network Address' with a text box and the instruction 'Enter the network address.'; 'Subnet Mask' with a text box and the instruction 'Enter the subnet mask.'; 'Metric' with a text box and the instruction 'Enter the numeric metric for this route (1 through 16).'; 'Destination Router Address' with a text box and the instruction 'Enter the router/gateway IP address.'; and 'Interface' with a dropdown menu showing 'Ethernet1 (Private) (10.10.147.2)' and the instruction 'Select the interface to route to.' At the bottom of the 'Add' window are 'Add' and 'Cancel' buttons.

Network Address

Enter the destination network IP address that this static route applies to. Packets with this destination address will be sent to the **Destination** below. Used dotted decimal notation; e.g., 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address, using dotted decimal notation (e.g., 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. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

Enter the metric, or 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.

Destination

Click a radio button to select the outbound destination for these packets. You can select only one destination: either a specific router/gateway, or a VPN 3002 interface.

Destination 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; e.g., 10.10.0.2. We recommend that you select this option.

Interface

Click the drop-down menu button and select a configured VPN 3002 interface as the outbound destination. We do not recommend this option; enter a destination router address above.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the **Configuration | System | IP Routing | Static Routes** screen. Any new route appears at the bottom of the **Static Routes** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing | Static Routes** screen, and the **Static Routes** list is unchanged.

Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the **Configuration | Quick | System Info** screen.

The IP routing subsystem routes data packets first using static routes, then the default gateway. If you don't specify a default gateway, the system drops packets it can't otherwise route.

Figure 7-4: Configuration | System | IP Routing | Default Gateways screen

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation; e.g., 192.168.12.77. This address must *not* be the same as the IP address configured on any VPN 3002 interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

To delete a configured default gateway, enter 0.0.0.0.

The default gateway must be reachable from a VPN 3002 interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. 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 this 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.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen. If you configure a **Default Gateway**, it also appears in the **Static Routes** list on the **Configuration | System | IP Routing | Static Routes** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

Configuration | System | IP Routing | DHCP

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) server parameters that apply to DHCP server functions within the VPN 3002.

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 7-5: Configuration | System | IP Routing | DHCP screen

Configuration | System | IP Routing | DHCP

Configure system-wide DHCP (Dynamic Host Configuration Protocol) parameters.

Enabled Check to enable DHCP.

Lease Timeout minutes

Address Pool Start

Address Pool End

Enabled

Check the box to enable the DHCP server functions on the VPN 3002. The box is checked by default. To use DHCP address assignment, you must enable DHCP functions here.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from the DHCP server. Minimum is 5, default is 120, maximum is 500000 minutes. DHCP servers “lease” IP addresses to clients on the VPN 3002’s private network for this period of time.

Address Pool Start/End

Enter the range of IP addresses that the DHCP server can assign. Use dotted decimal notation. The default is 127 successive addresses, with the first address being the address immediately after that of the private interface. The maximum number of addresses you can configure is 127.

Apply / Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen.

Reminder:

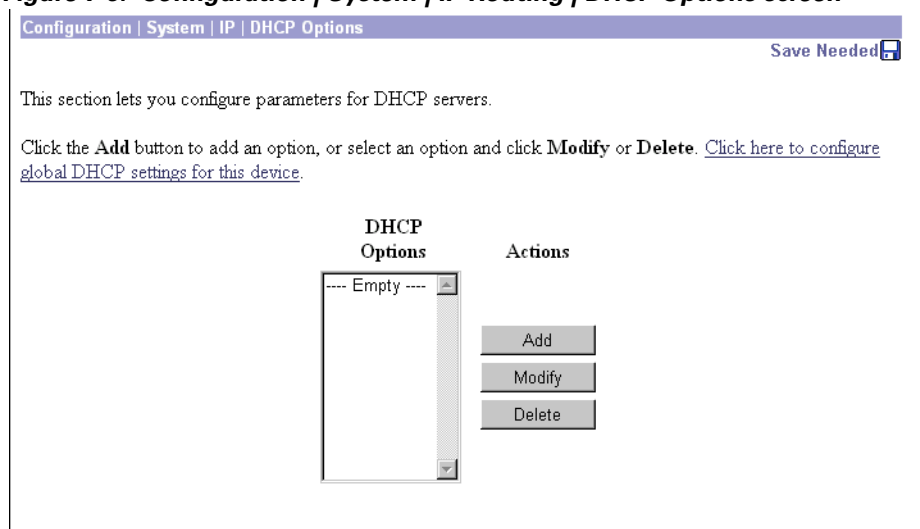
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

Configuration | System | IP Routing | DHCP Options

This section lets you configure DHCP options.

Figure 7-6: Configuration | System | IP Routing | DHCP Options screen



DHCP Option

DHCP Options are facilities that allow the VPN 3002 DHCP server to respond to with configurable parameters for specific kinds of devices such as PCs, IP telephones, print servers, etc, as well as an IP address.

Add / Modify / Delete

To configure and add DHCP options, click **Add**. The Manager opens the **Configuration | System | IP | DHCP Options | Add** screen. To modify a configured DHCP option, select the option from the list and click **Modify**. The Manager opens the **Configuration | System | IP | DHCP Options | Modify** screen.

To remove a configured DHCP option, select the option from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining DHCP options in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | IP Routing | DHCP Options | Add or Modify

These screens let you

Add a new DHCP option to the list of DHCP options this VPN 3002 uses.

Modify a configured DHCP option.

Figure 7-7: Configuration | System | IP Routing | DHCP Options | Add or Modify screen

Configuration | System | IP | DHCP Options | Add

Configure and add a DHCP option.

DHCP Option

Option Value

DHCP Option

Use the pull-down menu to the **DHCP Options** field to select the option you want to add or modify. You can add or modify only one option at a time.

Option Value

Enter the value you want this option to use, for example, the IP address for the TFTP server option, the number of seconds for the ARP Cache Timeout option, 1 or 0 to enable or disable IP forwarding, etc.



Management Protocols

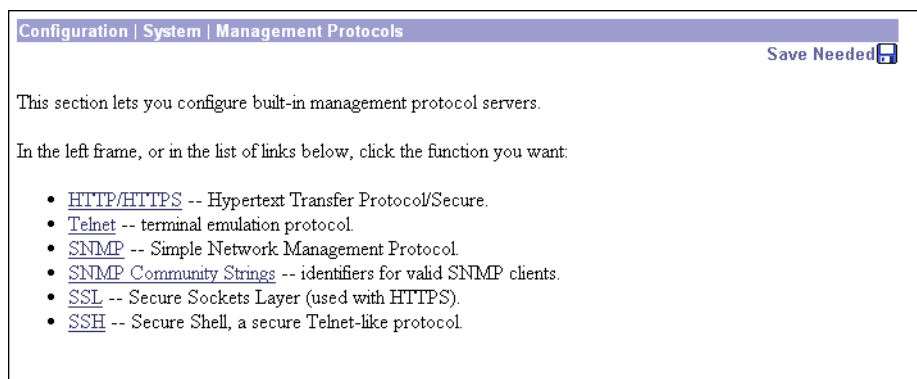
The VPN 3002 Hardware Client includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN 3002 servers that provide management functions using:

- **HTTP/HTTPS:** Hypertext Transfer Protocol, and HTTP over SSL (Secure Sockets Layer) protocol.
- **Telnet:** terminal emulation protocol, and Telnet over SSL.
- **SNMP:** Simple Network Management Protocol.
- **SNMP Community Strings:** identifiers for valid SNMP clients.
- **SSL:** Secure Sockets Layer protocol.
- **SSH:** Secure Shell.

Figure 8-1: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | HTTP/HTTPS

This screen lets you configure and enable the VPN 3002 HTTP/HTTPS server: Hypertext Transfer Protocol and HTTP over SSL (Secure Sockets Layer) protocol. When the server is enabled, you can use a Web browser to communicate with the VPN 3002. HTTPS lets you use a Web browser over a secure, encrypted connection.

Notes: The Manager requires the HTTP/HTTPS server. *If you click **Apply**, even if you have made no changes on this screen, you will break your HTTP/HTTPS connection and you must restart the Manager session from the login screen.*

If you disable *either* HTTP or HTTPS, and that is the protocol you are currently using, you can reconnect with the other protocol if it is enabled and configured.

If you disable *both* HTTP and HTTPS, you cannot use a Web browser to connect to the VPN 3002. Use the Cisco Command Line Interface from the console or a Telnet session.


Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1, *Using the VPN 3002 Hardware Client Manager*.
- To configure SSL parameters, see the **Configuration | System | Management Protocols | SSL** screen.
- To install, generate, view, or delete the SSL certificate on the VPN 3002, see the **Administration | Certificate Management** screens.

Figure 8-2: Configuration | System | Management Protocols | HTTP/HTTPS screen

Configuration | System | Management Protocols | HTTP/HTTPS

Configure the HTTP/HTTPS server.

 If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Enable HTTP	<input checked="" type="checkbox"/>	Disabling will provide additional security.
Enable HTTPS	<input checked="" type="checkbox"/>	HTTPS uses SSL encryption to provide security.
Enable HTTPS on Public	<input type="checkbox"/>	Check to enable HTTPS on the Public interface.
HTTP Port	<input type="text" value="80"/>	The default port is 80. Changing the port will provide additional security.
HTTPS Port	<input type="text" value="443"/>	The default port is 443. Changing the port will provide additional security.
Maximum Sessions	<input type="text" value="4"/>	Enter the maximum number of concurrent HTTP/HTTPS server users.

Enable HTTP

Check the box to enable the HTTP server. The box is checked by default. HTTP must be enabled to install the SSL certificate in the browser initially, so you can thereafter use HTTPS. Disabling the HTTP server provides additional security, but makes system management less convenient. See the notes above.

Enable HTTPS

Check the box to enable the HTTPS server. The box is checked by default. HTTPS—also known as HTTP over SSL—lets you use the Manager over an encrypted connection.

Enable HTTPS on Public

Check the box to enable HTTPS on the Public interface.

HTTP Port

Enter the port number that the HTTP server uses. The default is 80, which is the well-known port.

HTTPS Port

Enter the port number that the HTTPS server uses. The default is 443, which is the well-known port.

Maximum Sessions

Enter the maximum number of concurrent, combined HTTP and HTTPS sessions (users) that the server allows. Minimum is 1, default is 4, maximum is 10.

Apply / Cancel

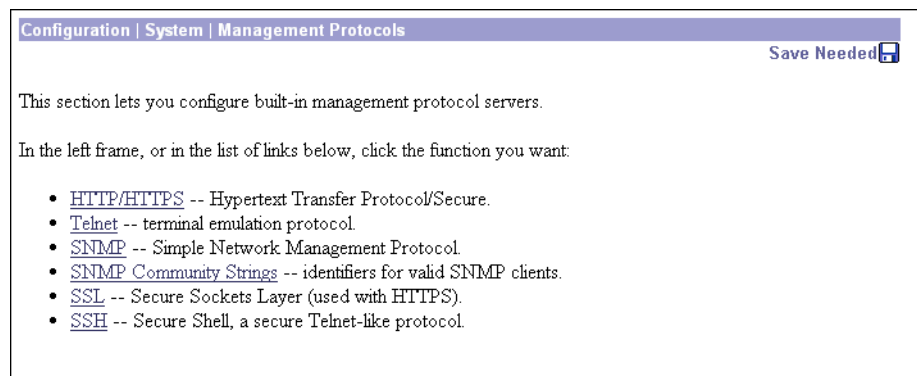
To apply your HTTP/HTTPS server settings, to include your settings in the active configuration, *and to break the current HTTP/HTTPS connection*, click **Apply**. If HTTP or HTTPS is still enabled, the Manager returns to the main login screen. If both HTTP and HTTPS are disabled, you can no longer use the Manager, and you will have to gain access through the console other configured connection.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-3: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | Telnet

This screen lets you configure and enable the VPN 3002 Telnet terminal emulation server, and Telnet over SSL (Secure Sockets Layer protocol). When the server is enabled, you can use a Telnet client to communicate with the VPN 3002. You can fully manage and administer the VPN 3002 using the Cisco Command Line Interface via Telnet.

Telnet server login usernames and passwords are the same as those enabled and configured on the **Administration | Access Rights | Administrators** screens.

Telnet/SSL uses a secure, encrypted connection. This enabled by default for Telnet/SSL clients.

See the **Configuration | System | Management Protocols | SSL** screen to configure SSL parameters. See the **Administration | Certificate Management | Certificates** screen to manage the SSL digital certificate.

Figure 8-4: Configuration | System | Management Protocols | Telnet screen

Enable Telnet

Check the box to enable the Telnet server. The box is checked by default. Disabling the Telnet server provides additional security, but doing so prevents using the Cisco Command Line Interface via Telnet.

Enable Telnet/SSL

Check the box to enable Telnet over SSL. The box is checked by default. Telnet/SSL uses Telnet over a secure, encrypted connection.

Telnet Port

Enter the port number that the Telnet server uses. The default is 23, which is the well-known port number.

Telnet/SSL Port

Enter the port number that Telnet over SSL uses. The default is 992, which is the well-known port number.

Maximum Connections

Enter the maximum number of concurrent, combined Telnet and Telnet/SSL connections that the server allows. Minimum is 1, default is 5, maximum is 10.

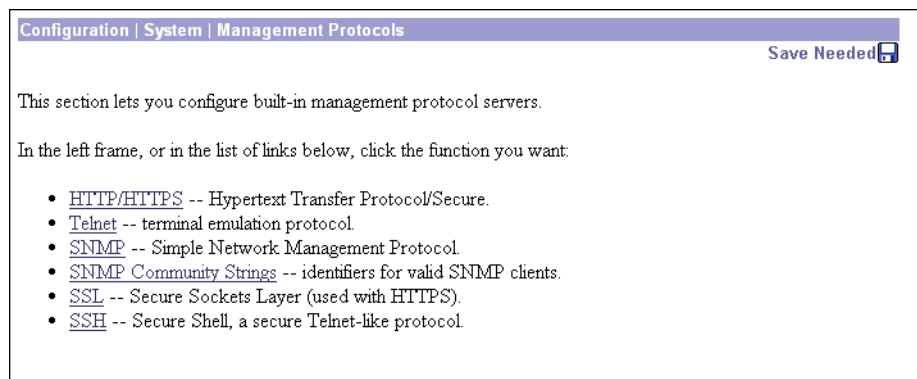
Apply / Cancel

To apply your Telnet settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-5: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | SNMP

This screen lets you configure and enable the SNMP (Simple Network Management Protocol) agent. When enabled, you can use an SNMP manager to collect information from the VPN 3002 but not to configure it.

To use SNMP, you must also configure an SNMP Community on the **Configuration | System | Management Protocols | SNMP Communities** screen.

The settings on this screen have no effect on sending system events to SNMP trap destinations (see **Configuration | System | Events | General** and **Trap Destinations**). For those functions, the VPN 3002 acts as an SNMP client.

Figure 8-6: Configuration | System | Management Protocols | SNMP screen

Configuration | System | Management Protocols | SNMP

Configure the SNMP server.

Enable Disabling will provide additional security. You can use third-party SNMP managers only for viewing statistics, not for configuring this device.

Port The default port is 161. Changing the port will provide additional security.

Maximum Queued Requests Enter the maximum number of outstanding queued requests.

Enable

Check the box to enable SNMP. The box is checked by default. Disabling SNMP provides additional security.

Port

Enter the port number that SNMP uses. The default is 161, which is the well-known port number. Changing the port number provides additional security.

Maximum Queued Requests

Enter the maximum number of outstanding queued requests that the SNMP agent allows. Minimum is 1, default is 4, maximum is 200.

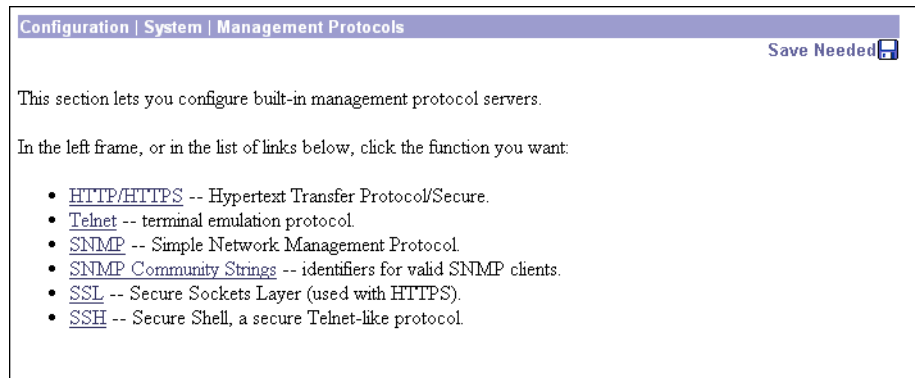
Apply / Cancel

To apply your SNMP settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

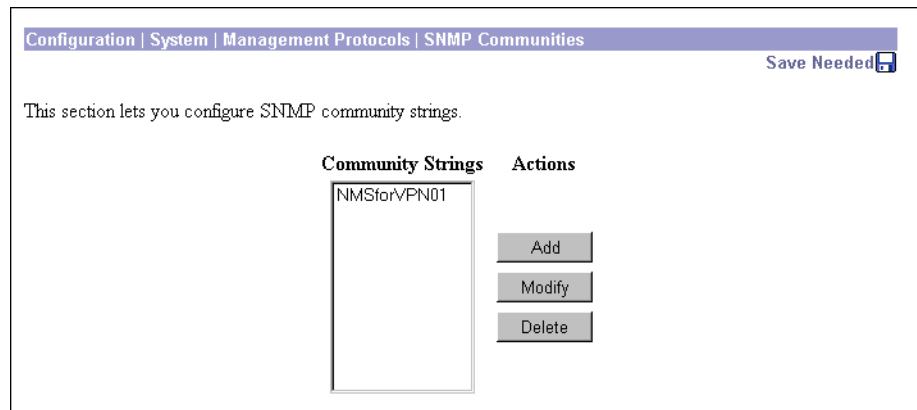
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-7: Configuration | System | Management Protocols screen

Configuration | System | Management Protocols | SNMP Communities

This section of the Manager lets you configure and manage SNMP community strings, which identify valid communities from which the SNMP agent accepts requests. A community string is like a password: it validates messages between an SNMP manager and the agent.

To use the VPN 3002 SNMP agent, you must configure and add at least one community string. You can configure a maximum of 10 community strings. To protect security, the SNMP agent does *not* include the usual default `public` community string, and we recommend that you not configure it.

Figure 8-8: Configuration | System | Management Protocols | SNMP Communities screen

Community Strings

The **Community Strings** list shows SNMP community strings that have been configured. If no strings have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new community string, click **Add**. The Manager opens the **Configuration | System | Management Protocols | SNMP Communities | Add** screen.

To modify a configured community string, select the string from the list and click **Modify**. The Manager opens the **Configuration | System | Management Protocols | SNMP Communities | Modify** screen.

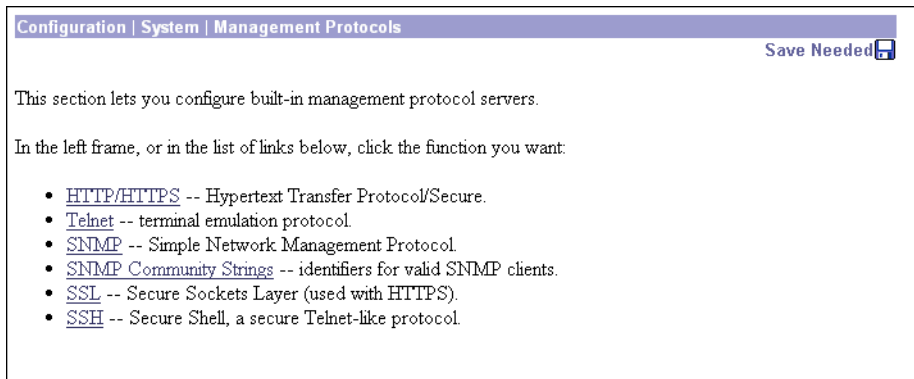
To delete a configured community string, select the string from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-9: Configuration | System | Management Protocols screen



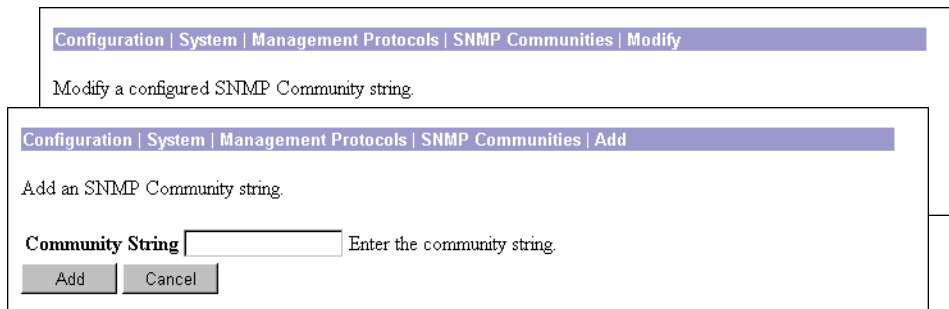
Configuration | System | Management Protocols | SNMP Communities | Add or Modify

These Manager screens let you:

Add: Configure and add a new SNMP community string.

Modify: Modify a configured SNMP community string.

Figure 8-10: Configuration | System | Management Protocols | SNMP Communities | Add or Modify screen



Community String

Enter the SNMP community string. Maximum 31 characters, case-sensitive.

Add or Apply / Cancel

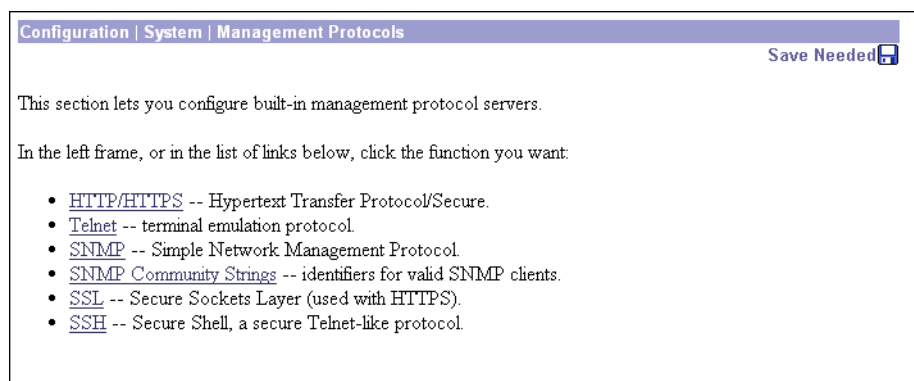
To add this entry to the list of configured community strings, click **Add**. Or to apply your changes to this community string, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Management Protocols | SNMP Communities** screen; a new entry appears at the bottom of the **Community Strings** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry or changes, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols | SNMP Communities** screen, and the **Community Strings** list is unchanged.

Figure 8-11: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | SSL

This screen lets you configure the VPN 3002 SSL (Secure Sockets Layer) protocol server. These settings apply to both HTTPS and Telnet over SSL. HTTPS lets you use a Web browser over a secure, encrypted connection to manage the VPN 3002.

SSL creates a secure session between the client and the VPN 3002 server. The client first authenticates the server, they negotiate session security parameters, and then they encrypt all data passed during the session. If, during negotiation, the server and client cannot agree on security parameters, the session terminates.

SSL uses digital certificates for authentication. The VPN 3002 creates a self-signed SSL server certificate when it boots; or you can install in the VPN 3002 an SSL certificate that has been issued in a PKI context. This certificate must then be installed in the client (for HTTPS; Telnet doesn't usually require it). You need to install the certificate from a given VPN 3002 only once.

The default SSL settings should suit most administration tasks and network security requirements. *We recommend that you not change them unadvisedly.*

Note: To ensure the security of your connection to the Manager, if you click **Apply** on this screen—even if you have made no changes—you will break your connection to the Manager and you must restart the Manager session from the login screen.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1, *Using the VPN 3002 Hardware Client Manager*.
- To configure HTTPS parameters, see the **Configuration | System | Management Protocols | HTTP/HTTPS** screen.
- To configure Telnet/SSL parameters, see the **Configuration | System | Management Protocols | Telnet** screen.
- To manage SSL digital certificates, see the **Administration | Certificate Management** screens.

Figure 8-12: Configuration | System | Management Protocols | SSL screen

Configuration | System | Management Protocols | SSL

Configure SSL.

If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Encryption Protocols

- RC4-128/MD5
- 3DES-168/SHA
- DES-56/SHA
- RC4-40/MD5 Export
- DES-40/SHA Export

Check the encryption algorithms to enable. Unchecking them all disables SSL.

Client Authentication

Check to enable client authentication. Client authentication requires an installed Certificate Authority and a personal certificate installed in your browser.

SSL Version

Select the SSL version to use. Using a SSL V2 Hello provides compatibility with most browsers.

Generated Certificate Key Size

Select the key size used in the generated certificate.

Encryption Protocols

Check the boxes for the encryption algorithms that the VPN 3002 SSL server can negotiate with a client and use for session encryption. All are checked by default. You must check at least one algorithm to enable SSL. *Unchecking all algorithms disables SSL.*

The algorithms are negotiated in the order shown. You cannot change the order, but you can enable or disable selected algorithms.

RC4-128/MD5 = RC4 encryption with a 128-bit key and the MD5 hash function. This option is available in most SSL clients.

3DES-168/SHA = Triple-DES encryption with a 168-bit key and the SHA-1 hash function. This is the strongest (most secure) option.

DES-56/SHA = DES encryption with a 56-bit key and the SHA-1 hash function.

RC4-40/MD5 Export = RC4 encryption with a 128-bit key—40 bits of which are private—and the MD5 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.

DES-40/SHA Export = DES encryption with a 56-bit key—40 bits of which are private—and the SHA-1 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.

Client Authentication

This parameter applies to HTTPS only; it is ignored for Telnet/SSL.

Check the box to enable SSL client authentication. The box is not checked by default. In the most common SSL connection, the client authenticates the server, not vice-versa. Client authentication requires personal certificates installed in the browser, and trusted certificates installed in the server. Specifically, the VPN 3002 must have a root CA certificate installed; and a certificate signed by one of the VPN 3002's trusted CAs must be installed in the Web browser. See **Administration | Certificate Management**.

SSL Version

Click the drop-down menu button and select the SSL version to use. SSL Version 3 has more security options than Version 2, and TLS (Transport Layer Security) Version 1 has more security options than SSL Version 3. Some clients that send an SSL Version 2 “Hello” (initial negotiation), can actually use a more secure version during the session. Telnet/SSL clients usually can use only SSL Version 2.

Choices are:

Negotiate SSL V2/V3 = The server tries to use SSL Version 3 but accepts Version 2 if the client can't use Version 3. This is the default selection. This selection works with most browsers and Telnet/SSL clients.

SSL V3 with SSL V2 Hello = The server insists on SSL Version 3 but accepts an initial Version 2 “Hello.”

SSL V3 Only = The server insists on SSL Version 3 only.

SSL V2 Only = The server insists on SSL Version 2 only. This selection works with most Telnet/SSL clients.

TLS V1 Only = The server insists on TLS Version 1 only. At present, only Microsoft Internet Explorer 5.0 supports this option.

TLS V1 with SSL V2 Hello = The server insists on TLS Version 1 but accepts an initial SSL Version 2 “Hello.” At present, only Microsoft Internet Explorer 5.0 supports this option.

Generated Certificate Key Size

Click the drop-down menu button and select the size of the RSA key that the VPN 3002 uses in its self-signed (generated) SSL server certificate. A larger key size increases security, but it also increases the processing necessary in all transactions over SSL. The increases vary depending on the type of transaction (encryption or decryption).

Choices are:

512-bit RSA Key = This key size provides sufficient security. It is the most common, and requires the least processing.

768-bit RSA Key = This key size provides normal security and is the default selection. It requires approximately 2 to 4 times more processing than the 512-bit key.

1024-bit RSA Key = This key size provides high security. It requires approximately 4 to 8 times more processing than the 512-bit key.

Apply / Cancel

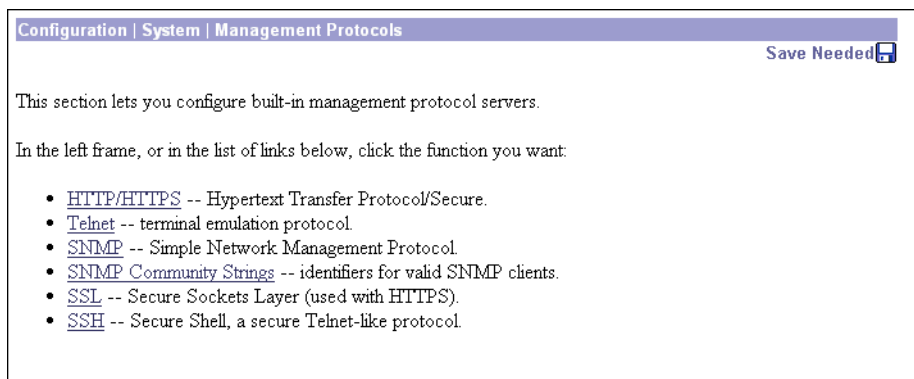
To apply your SSL settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-13: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | SSH

This screen lets you configure the VPN 3002 SSH (Secure Shell) protocol server. SSH is a secure Telnet-like terminal emulator protocol that you can use to manage the VPN 3002, using the Command Line Interface, over a remote connection.

The SSH server supports SSH1 (protocol version 1.5), which uses two RSA keys for security. All communication over the connection is encrypted. To provide additional security, the remote client authenticates the server and the server authenticates the client.

At the start of an SSH session, the VPN 3002 sends both a **host key** and a **server key** to the client, which responds with a **session key** that it generates and encrypts using the host and server keys. The RSA key of the SSL certificate is used as the host key, which uniquely identifies the VPN 3002. See **Configuration | System | Management Protocols | SSL**.

Figure 8-14: Configuration | System | Management Protocols | SSH screen

Configuration | System | Management Protocols | SSH

Configure SSH. Only SSH1 (protocol version 1.5) is supported.

Enable SSH Disabling will provide additional security.

Enable SSH on Public Check to enable SSH on the Public interface.

SSH Port The default port is 22. Changing the port will provide additional security.

Maximum Sessions Enter the maximum number of concurrent SSH users. Maximum is 10, default is 4. *SSH sessions are also limited by the configured number of maximum Telnet sessions.*

Key Regeneration Period Enter the server key regeneration period in minutes. Setting to 0 disables server key regeneration. Maximum is 1 week (10080), default is 1 hour (60).

Encryption Protocols

- 3DES-168
- RC4-128
- DES-56
- No Encryption

Check the encryption algorithms to enable. Unchecking them all effectively disables SSH.

Enable SSH

Check the box to enable the SSH server. The box is checked by default. Disabling the SSH server provides additional security by preventing SSH access.

Enable SSH on Public

Check the box to enable SSH on the Public interface.

SSH Port

Enter the port number that the SSH server uses. The default is 22, which is the well-known port.

Maximum Sessions

Enter the maximum number of concurrent SSH sessions allowed. Minimum is 1, default is 4, and maximum is 10.

Key Regeneration Period

Enter the server key regeneration period in minutes. If the server key has been used for an SSH session, the VPN 3002 regenerates the key at the end of this period. Minimum is 0 (which disables key regeneration, default is 60 minutes, and maximum is 10080 minutes (1 week)). Use 0 (disable key regeneration) only for testing, since it lessens security.

Encryption Protocols

Check the boxes for the encryption algorithms that the VPN 3002 SSH server can negotiate with a client and use for session encryption. All algorithms are checked by default. You must check at least one algorithm to enable a secure session. *Unchecking all algorithms disables SSH.*

3DES-168 = Triple-DES encryption with a 168-bit key. This option is the most secure but requires the greatest processing overhead.

RC4-128 = RC4 encryption with a 128-bit key. This option provides adequate security and performance.

DES-56 = DES encryption with a 56-bit key. This option is least secure but provides the greatest export flexibility.

No Encryption = Connect without encryption. This option provides no security and is for testing purposes only. It is not checked by default.

Apply / Cancel

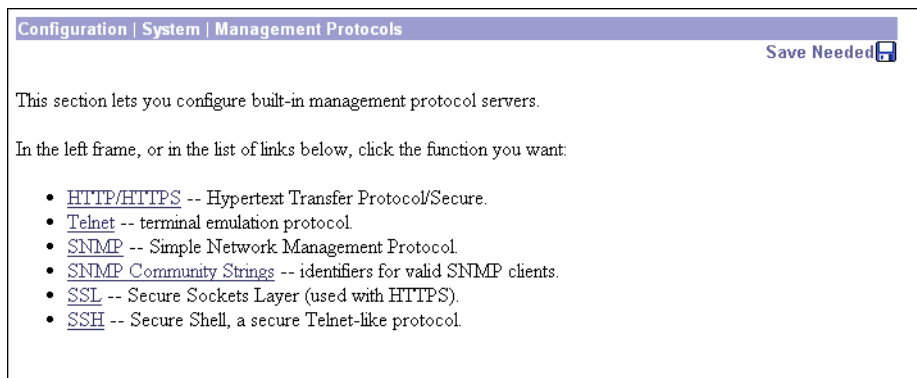
To apply your SSH settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Figure 8-15: Configuration | System | Management Protocols screen





Events

An *event* is any significant occurrence within or affecting the VPN 3002 such as an alarm, trap, error condition, network problem, task completion, threshold breach, or status change. The VPN 3002 records events in an event log, which is stored in nonvolatile memory. You can also specify that certain events trigger a console message, a UNIX syslog record, or an SNMP management system trap.

Event attributes include *class* and *severity level*.

Event class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN 3002. Table 9-1 describes the event classes.

Table 9-1: VPN 3002 event classes

Class name	Class description (event source) (*Cisco-specific event class)
AUTH	Authentication*
AUTHDBG	Authentication debugging*
AUTHDECODE	Authentication protocol decoding*
AUTOUPDATE	Autoupdate subsystem*
BKPLN	WAN backplane driver*
CAPI	Cryptography subsystem*
CERT	Digital certificates subsystem
CONFIG	Configuration subsystem*
DHCP	DHCP subsystem
DHCPDBG	DHCP debugging*
DHCPDECODE	DHCP decoding*
DM	Data Movement subsystem*

Table 9-1: VPN 3002 event classes (continued)

Class name	Class description (event source) (*Cisco-specific event class)
DNS	DNS subsystem
DNSDBG	DNS debugging*
DNSDECODE	DNS decoding*
EVENT	Event subsystem*
EVENTDBG	Event subsystem debugging*
EVENTMIB	Event MIB changes*
EXPANSIONCARD	Expansion card (module) subsystem
FILTER	Filter subsystem
FILTERDBG	Filter debugging*
FSM	Finite State Machine subsystem (for debugging)*
FTPD	FTP daemon subsystem
GENERAL	NTP subsystem and other general events
GRE	GRE subsystem
GREDBG	GRE debugging*
GREDECODE	GRE decoding*
HARDWAREMON	Hardware monitoring (fans, temperature, voltages, etc.)
HDLC	HDLC/SYNC driver for WAN module*
HTTP	HTTP subsystem
HWDIAG	Hardware diagnostics for WAN module*
IKE	ISAKMP/Oakley (IKE) subsystem
IKEDBG	ISAKMP/Oakley (IKE) debugging*
IKEDECODE	ISAKMP/Oakley (IKE) decoding*
IP	IP router subsystem
IPDBG	IP router debugging*
IPDECODE	IP packet decoding*
IPSEC	IP Security subsystem
IPSECDBG	IP Security debugging*
IPSECDECODE	IP Security decoding*
L2TP	L2TP subsystem
L2TPDBG	L2TP debugging*
L2TPDECODE	L2TP decoding*

Table 9-1: VPN 3002 event classes (continued)

Class name	Class description (event source) (*Cisco-specific event class)
LBSSF	Load Balancing/Secure Session Failover subsystem*
MIB2TRAP	MIB-II trap subsystem: SNMP MIB-II traps*
OSPF	OSPF subsystem
PPP	PPP subsystem
PPPDBG	PPP debugging*
PPPDECODE	PPP decoding*
PPTP	PPTP subsystem
PPTPDBG	PPTP debugging*
PPTPDECODE	PPTP decoding*
PSH	Operating system command shell*
PSOS	Embedded real-time operating system*
QUEUE	System queue*
REBOOT	System rebooting
RM	Resource Manager subsystem*
SMTP	SMTP event handling
SNMP	SNMP trap subsystem
SSH	SSH subsystem
SSL	SSL subsystem
SYSTEM	Buffer, heap, and other system utilities*
T1E1	T1/E1 ports on WAN module*
TCP	TCP subsystem
TELNET	Telnet subsystem
TELNETDBG	Telnet debugging*
TELNETDECODE	Telnet decoding*
TIME	System time (clock)
VRRP	VRRP subsystem
WAN	WAN module subsystem*

Note: The Cisco-specific event classes provide information that is meaningful only to Cisco engineering or support personnel. Also, the `DBG` and `DECODE` events require significant system resources and may seriously degrade performance. We recommend that you avoid logging these events unless Cisco requests it.

Event severity level

Severity level indicates how serious or significant the event is; i.e., how likely it is to cause unstable operation of the VPN 3002, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. Table 9-2 describes the severity levels.

Table 9-2: VPN 3002 event severity levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that may require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding
11	Packet Decode	Low-level packet header decoding
12	Packet Decode	Hex dump of header
13	Packet Decode	Hex dump of packet

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the **Information** category, Level 6 provides greater detail than Level 4 but doesn't necessarily include the same information as Level 4.

Logging higher-numbered severity levels degrades performance, since more system resources are used to log and handle these events.

Note: The Debug (7–9) and Packet Decode (10–13) severity levels are intended for use by Cisco engineering and support personnel. We recommend that you avoid logging these events unless Cisco requests it.

The VPN 3002, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the **Configuration | System | Events | General** screen, and you can configure specific events for special handling on the **Configuration | System | Events | Classes** screens.

Event log

The VPN 3002 records events in an event log, which is stored in nonvolatile memory. Thus the event log persists even if the system is powered off. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN 3002 holds 256 events. The log wraps when it is full; that is, newer events overwrite older events when the log is full.

For the event log, you can configure which event classes and severity levels to log.

Note: The VPN 3002 automatically saves the log file 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.

Event log data

Each entry (record) in the event log consists of several fields including:

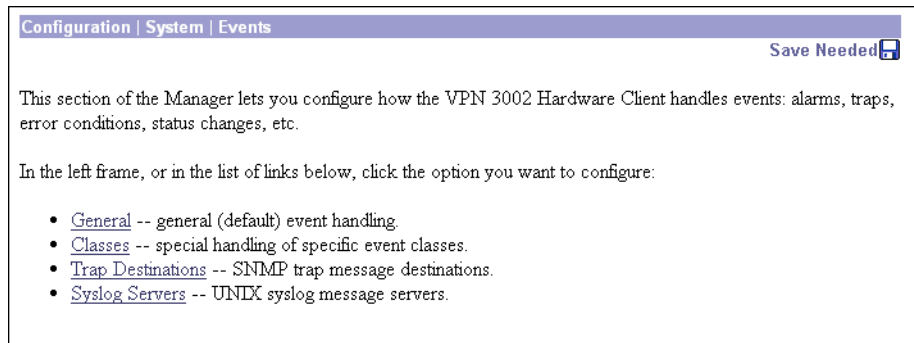
- A sequence number.
- Date and time.
- Event severity level.
- Event class and number.
- Event repetition count.
- Event IP address (only for certain events).
- Description string.

For more information, see the **Monitoring | Filterable Event Log** screen.

Configuration | System | Events

This section of the Manager lets you configure how the VPN 3002 handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

Figure 9-1: Configuration | System | Events screen

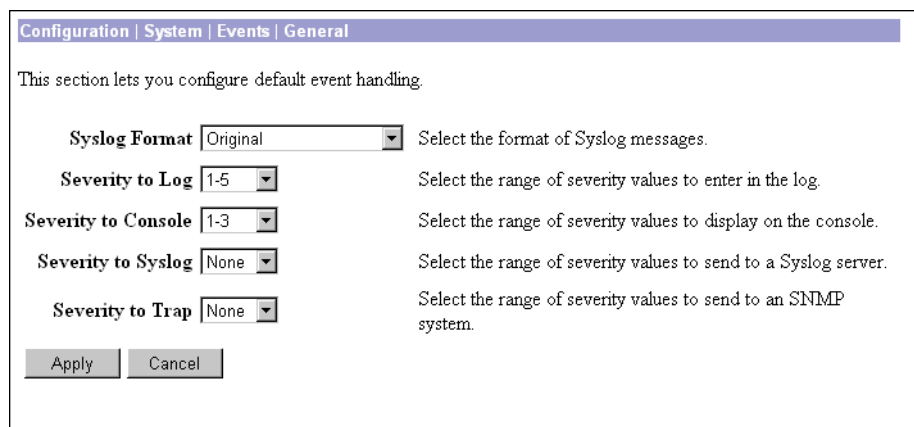


Configuration | System | Events | General

This Manager screen lets you configure the general, or default, handling of all events. These defaults apply to all event classes.

You can override these default settings by configuring specific events for special handling on the **Configuration | System | Events | Classes** screens.

Figure 9-2: Configuration | System | Events | General screen



Syslog Format

Click the drop-down menu button and select the format for all events sent to UNIX syslog servers. Choices are:

Original = Original VPN 3002 event format with information on one line.

Cisco IOS Compatible == Event format that is compatible with Cisco syslog management applications.

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-5**: all events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-3**: all events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-6**. The default is **None**: no events are sent to a syslog server.

If you select any severity levels to send, you must also configure the syslog server(s) on the **Configuration | System | Events | Syslog Servers** screens.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system by default. Event messages sent to SNMP systems are called “traps.” Choices are: **None, 1, 1-2, 1-3**. The default is **None**: no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the **Configuration | System | Events | Trap Destinations** screens.

The VPN 3002 can send the standard, or “well-known,” SNMP traps listed in Table 9-3. To have an SNMP NMS receive them, you must configure the events as in the table, and configure a trap destination.

Table 9-3: Configuring “well-known” SNMP traps

To send this “well-known” SNMP trap	Configure either General event handling or this Event Class	With this Severity to Trap
coldStart	EVENT	1 or higher
linkDown	IP	1-3 or higher
linkUp	IP	1-3 or higher
authFailure (This trap is SNMP authentication failure, not tunnel authentication failure.)	SNMP	1-3 or higher

Apply / Cancel

To include your settings for default event handling in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Events** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

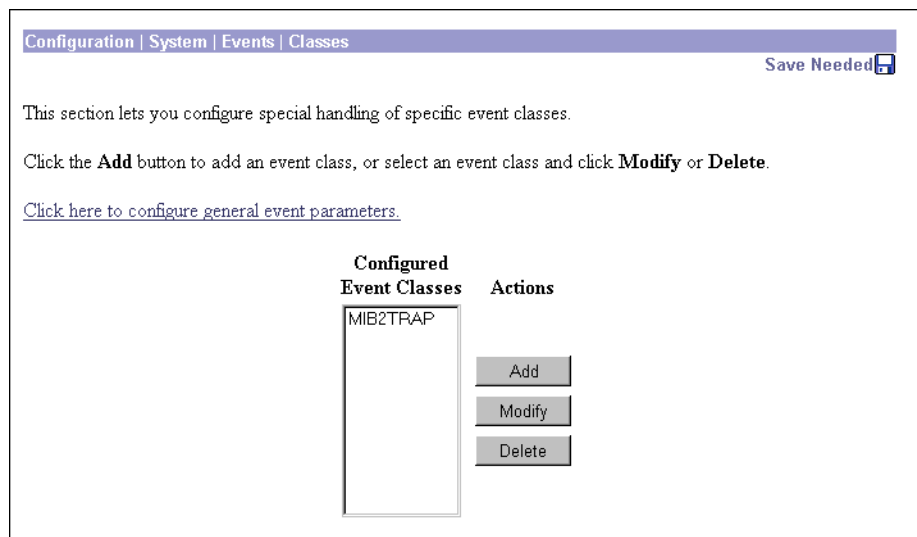
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events** screen.

Configuration | System | Events | Classes

This section of the Manager lets you add, configure, modify, and delete specific event classes for special handling. You can thus override the general, or default, handling of event classes. For example, you might want to send email for **HARDWAREMON** events of severity 1-2, whereas default event handling doesn't send any email.

Event classes denote the source of an event and refer to a specific hardware or software subsystem within the VPN 3002. Table 9-1 describes the event classes.

Figure 9-3: Configuration | System | Events | Classes screen



To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*”

Configured Event Classes

The **Configured Event Classes** list shows the event classes that have been configured for special handling. The initial default entry is **MIB2TRAP**, which are SNMP MIB-II events, or “traps,” that you might want to monitor with an SNMP network management system. Other configured event classes are listed in order by class number and name. If no classes have been configured for special handling, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new event class for special handling, click **Add**. See **Configuration | System | Events | Classes | Add**.

To modify an event class that has been configured for special handling, select the event class from the list and click **Modify**. See **Configuration | System | Events | Classes | Modify**.

To remove an event class that has been configured for special handling, select the event class from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Classes | Add or Modify

These screens let you:

Add and configure the special handling of a specific event class.

Modify the special handling of a specific event class.

Figure 9-4: Configuration | System | Events | Classes | Add or Modify screen

The screenshot shows two overlapping windows. The top window is titled "Configuration | System | Events | Classes | Modify" and contains the text "This screen lets you modify an event class configured for special handling." The bottom window is titled "Configuration | System | Events | Classes | Add" and contains the text "This screen lets you add and configure an event class for special handling." Below the text in the "Add" window are several configuration options:

- Class Name:** A dropdown menu with "Select Class" selected. To its right is the instruction "Select the event class to configure."
- Enable:** A checked checkbox. To its right is the instruction "Check to enable special handling of this class."
- Severity to Log:** A dropdown menu with "1-5" selected. To its right is the instruction "Select the range of severity values to enter in the log."
- Severity to Console:** A dropdown menu with "1-3" selected. To its right is the instruction "Select the range of severity values to display on the console."
- Severity to Syslog:** A dropdown menu with "None" selected. To its right is the instruction "Select the range of severity values to send to a Syslog server."
- Severity to Trap:** A dropdown menu with "None" selected. To its right is the instruction "Select the range of severity values to send to an SNMP system."

At the bottom of the "Add" window are two buttons: "Add" and "Cancel".

Class Name

Add screen:

Click the drop-down menu button and select the event class you want to add and configure for special handling. (Please note that **Select Class** is an instruction reminder, not a class.) Table 9-1 describes the event classes.

Modify screen:

The field shows the configured event class you are modifying. You cannot change this field.

All subsequent parameters on this screen apply to this event class only.

Enable

Check this box to enable the special handling of this event class. (The box is checked by default.)

Clearing this box lets you set up the parameters for the event class but activate it later, or temporarily disable special handling without deleting the entry. The **Configured Event Classes** list on the **Configuration | System | Events | Classes** screen indicates disabled event classes. Disabled event classes are handled according to the default parameters for all event classes.

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-5**: events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-3**: events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **None**: no events are sent to a syslog server.

Note: Sending events to a syslog server generates IP packets, which can generate new events if this setting is above level 9. We strongly recommend that you keep this setting at or below level 6. Avoid setting this parameter above level 9.

If you select any severity levels to send, you must also configure the syslog server(s) on the **Configuration | System | Events | Syslog Servers** screens, and you should configure the **Syslog Format** on the **Configuration | System | Events | General** screen.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system. Event messages sent to SNMP systems are called “traps.” Choices are: **None, 1, 1-2, 1-3, 1-4, 1-5**. The default is **None**: no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the **Configuration | System | Events | Trap Destinations** screens.

To configure “well-known” SNMP traps, see Table 9-3 under **Severity to Trap** for **Configuration | System | Events | General**.

Add or Apply / Cancel

To add this event class to the list of those with special handling, click **Add**. Or to apply your changes to this configured event class, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Classes** screen. Any new event class appears in the **Configured Event Classes** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events | Classes** screen.

Configuration | System | Events | Trap Destinations

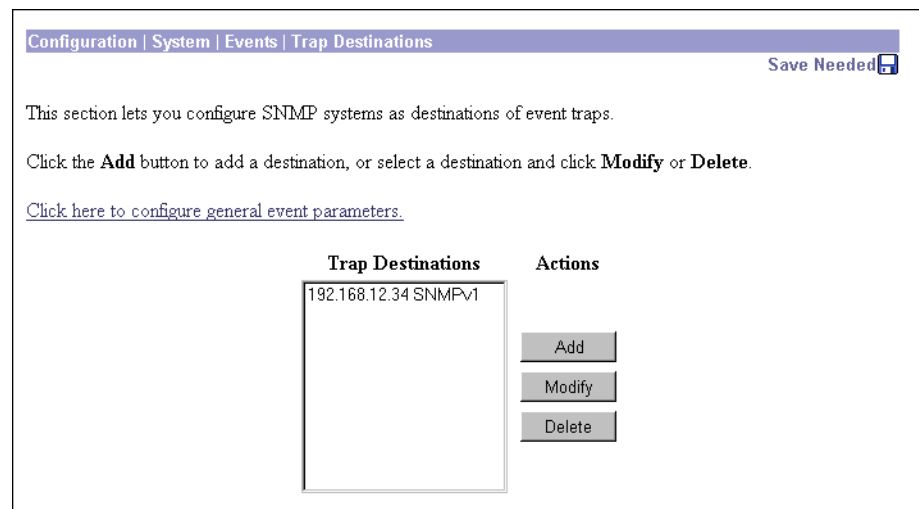
This section of the Manager lets you configure SNMP network management systems as destinations of event traps. Event messages sent to SNMP systems are called “traps.” If you configure any event handling—default or special—with values in **Severity to Trap** fields, you must configure trap destinations in this section.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

To configure “well-known” SNMP traps, see Table 9-3 under **Severity to Trap** for **Configuration | System | Events | General**.

To have an SNMP-based network management system (NMS) receive any events, you must also configure the NMS to “see” the VPN 3002 as a managed device or “agent” in the NMS domain.

Figure 9-5: Configuration | System | Events | Trap Destinations screen



Trap Destinations

The **Trap Destinations** list shows the SNMP network management systems that have been configured as destinations for event trap messages, and the SNMP protocol version associated with each destination. If no trap destinations have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new SNMP trap destination, click **Add**. See **Configuration | System | Events | Trap Destinations | Add**.

To modify an SNMP trap destination that has been configured, select the destination from the list and click **Modify**. See **Configuration | System | Events | Trap Destinations | Modify**.

To remove an SNMP trap destination that has been configured, select the destination from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Trap Destinations | Add or Modify

These screens let you:

Add an SNMP destination system for event trap messages.

Modify a configured SNMP destination system for event trap messages.

Figure 9-6: Configuration | System | Events | Trap Destinations | Add or Modify screen

The screenshot displays two overlapping windows from the configuration interface. The top window, titled 'Configuration | System | Events | Trap Destinations | Modify', contains the text 'Modify a configured trap destination.' The bottom window, titled 'Configuration | System | Events | Trap Destinations | Add', contains the text 'Add a trap destination.' and the following form fields:

- Destination:** A text input field with the instruction 'Enter the IP address or hostname of the trap destination.'
- SNMP Version:** A dropdown menu currently set to 'SNMPv1' with the instruction 'Select the SNMP version of the trap to send to this destination.'
- Community:** A text input field with the instruction 'Enter the community string to use in the trap. Default is "public".'
- Port:** A text input field containing '162' with the instruction 'Enter the destination port for the trap.'

At the bottom of the 'Add' window are two buttons: 'Add' and 'Cancel'.

Destination

Enter the IP address or hostname of the SNMP network management system that is a destination for event trap messages. (If you have configured a DNS server, you can enter a hostname; otherwise enter an IP address.)

SNMP Version

Click the drop-down menu button and select the SNMP protocol version to use when formatting traps to this destination. Choices are **SNMPv1** (version 1; the default) and **SNMPv2** (version 2).

Community

Enter the community string to use in identifying traps from the VPN 3002 to this destination. The community string is like a password: it validates messages between the VPN 3002 and this NMS destination. If you leave this field blank, the default community string is `public`.

Port

Enter the UDP port number by which you access the destination SNMP server. Use a decimal number from 0 to 65535. The default is 162, which is the well-known port number for SNMP traps.

Add or Apply / Cancel

To add this system to the list of SNMP trap destinations, click **Add**. Or to apply your changes to this trap destination, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Trap Destinations** screen. Any new destination system appears in the **Trap Destinations** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

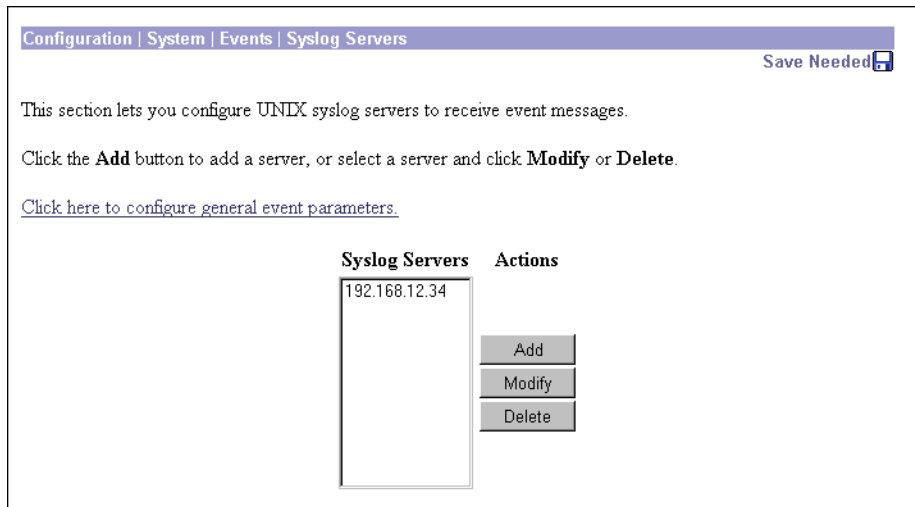
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events | Trap Destinations** screen, and the **Trap Destinations** list is unchanged.

Configuration | System | Events | Syslog Servers

This section of the Manager lets you configure UNIX syslog servers as recipients of event messages. Syslog is a UNIX daemon, or background process, that records events. The VPN 3002 can send event messages in two syslog formats to configured syslog systems. If you configure any event handling—default or special—with values in **Severity to Syslog** fields, you must configure syslog servers in this section.

To configure default event handling and syslog formats, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

Figure 9-7: Configuration | System | Events | Syslog Servers screen



Syslog Servers

The **Syslog Servers** list shows the UNIX syslog servers that have been configured as recipients of event messages. You can configure a maximum of five syslog servers. If no syslog servers have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new syslog server, click **Add**. See **Configuration | System | Events | Syslog Servers | Add**.

To modify a syslog server that has been configured, select the server from the list and click **Modify**. See **Configuration | System | Events | Syslog Servers | Modify**.

To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Syslog Servers | Add or Modify

These screens let you:

Add a UNIX syslog server as a recipient of event messages. You can configure a maximum of five syslog servers.

Modify a configured UNIX syslog server that is a recipient of event messages.

Figure 9-8: Configuration | System | Events | Syslog Servers | Add or Modify screen

Configuration | System | Events | Syslog Servers | Modify

Modify a configured syslog server.

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server Enter the IP address or hostname of the syslog server.

Port Enter the port used by the syslog server.

Facility Select the syslog facility tag for events sent to this server.

Syslog Server

Enter the IP address or hostname of the UNIX syslog server to receive event messages. (If you have configured a DNS server, you can enter a hostname; otherwise, enter an IP address.)

Port

Enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default is 514, which is the well-known port number.

Facility

Click the drop-down menu button and select the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. The choices are:

User = Random user-process messages.

Mail = Mail system.

Daemon = System daemons.

Auth = Security or authorization messages.

Syslog = Internal syslogd-generated messages.

LPR = Line printer subsystem.

News = Network news subsystem.

UUCP = UUCP (UNIX-to-UNIX Copy Program) subsystem.

Reserved (9) through **Reserved (14)** = Outside the **Local** range, with no name or assignment yet, but usable.

CRON = Clock daemon.

Local 0 through **Local 7** (default) = User defined.

Add or Apply / Cancel

To add this server to the list of syslog servers, click **Add**. Or to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Syslog Servers** screen. Any new server appears in the **Syslog Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Events | Syslog Servers** screen, and the **Syslog Servers** list is unchanged.



General

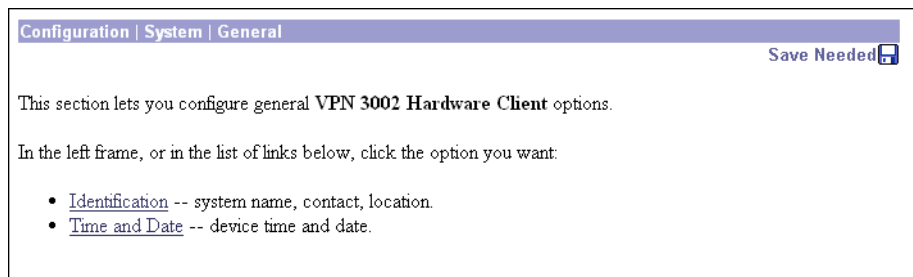
General configuration parameters include VPN 3002 environment items: system identification, time, and date.

Configuration | System | General

This section of the Manager lets you configure general VPN 3002 parameters.

- **Identification:** system name, contact person, system location.
- **Time and Date:** system time and date.

Figure 10-1: Configuration | System | General screen



Configuration | System | General | Identification

This screen lets you configure system identification parameters that are stored in the standard MIB-II system object. Network management systems using SNMP can retrieve this object and identify the system. Configuring this information is optional.

Figure 10-2: Configuration | System | General | Identification screen

Configuration | System | General | Identification

Configure system identification (optional). These entries are stored in the MIB-II system object.

System Name Enter a system name for the device; e.g., vpn01

Contact Enter the name of the contact person

Location Enter the device location; e.g., Computer Lab 3

Apply Cancel

System Name

Enter a system name that uniquely identifies this VPN 3002 on your network; e.g., VPN01. Maximum 255 characters.

Contact

Enter the name of the contact person who is responsible for this VPN 3002. Maximum 255 characters.

Location

Enter the location of this VPN 3002. Maximum 255 characters.

Apply / Cancel

To apply your system identification settings and include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | General** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | General** screen.

Configuration | System | General | Time and Date

This screen lets you set the time and date on the VPN 3002. Setting the correct time is very important so that logging information is accurate.

Figure 10-3: Configuration | System | General | Time and Date screen

Current Time

The screen shows the current date and time on the VPN 3002 at the time the screen displays. You can refresh this by redisplaying the screen.

New Time

The values in the **New Time** fields are the time and date on the *browser PC* at the time the screen displays. Any entries you make apply to the *VPN 3002*, however.

In the appropriate fields, make any changes. The fields are, in order: **Hour : Minute : Second Month / Day / Year Time Zone**. Click the drop-down menu buttons to select **Month**, and **Time Zone**. The time zone selections are offsets in hours relative to GMT (Greenwich Mean Time), which is the basis for Internet time synchronization. Enter the **Year** as a four-digit number.

Enable DST Support

To enable DST support, check the box. During DST (Daylight-Saving Time), 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.*

Apply / Cancel

To apply your time and date settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | General** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | General** screen.



Policy Management

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

Policy management on the VPN 3002 includes deciding whether you want the VPN 3002 to use Client Mode or Network Extension mode. This section lets you enable or disable PAT.

Client mode/PAT

Client mode, also called PAT (Port Address Translation) 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 interface of the VPN 3002 to the network(s) behind the IKE peer, i.e., the central-site Concentrator.
- PAT includes NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 Private interface to the 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.

Thus all traffic from the private network appears on the network behind the IKE peer with a single source IP address, which is the IP address of the VPN 3002 Private interface. This IP address is the one the central-site 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.

Client mode with split tunneling

You assign the VPN 3002 to a Group on the central-site VPN 3002 Concentrator. If you enable split tunneling for that group, IPSec and PAT operate on all traffic that travels through the VPN 3002 to networks within the network list behind the central-site Concentrator, just as described above.

Traffic from the VPN 3002 to any destination other than those within the Concentrator's network list, 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.

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

VPN 3000 Series Concentrator settings required for PAT

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

- 1 The 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 (e.g., DHCP, address pools, per user, or client-specified). If the 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 Concentrator Series User Guide*.
- 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 Concentrator Series User Guide*.
- 4 Configure one or more Users for the group, including **User Names** and **Passwords**.

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 Concentrator. PAT does not apply. Therefore, devices behind the Concentrator have direct access to devices on the VPN 3002 private network via the tunnel, and only over the tunnel, and vice versa. Either side can initiate data exchange.

In this mode, the 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.

Network Extension mode with split tunneling

You assign the VPN 3002 to a Group on the central-site 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 behind the central-site Concentrator, just as described above. PAT does not apply.

Traffic from the VPN 3002 to any other destination than those within the Concentrator's network list 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 via the tunnel, but are protected from the Internet, i.e., they cannot be accessed directly.

VPN 3000 Series Concentrator settings required for Network Extension mode

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

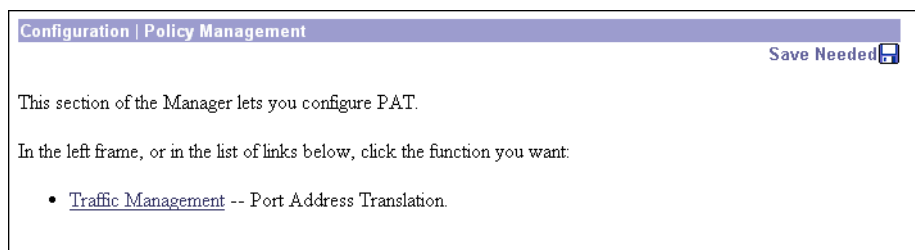
- 1 The Concentrator at the central site must be running Software version 3.x or later.
- 2 Configure a Group to which you assign this VPN 3002. This includes assigning a **Group Name** and **Password**. See Chapter 14, *User Management*, in the *VPN 3000 Concentrator Series User Guide*.
- 3 Configure one or more Users for the group, including **User Names** 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 Concentrator Series User Guide*.

- 5 If you want the VPN 3002 to be able to reach devices on other networks that connect to this Concentrator, review your Network Lists. See Chapter 15, *Policy Management* in the *VPN 3000 Concentrator Series User Guide*.

Configuration | Policy Management

The **Configuration | Policy Management** screen introduces this section of the Manager.

Figure 11-1: Configuration | Policy Management screen



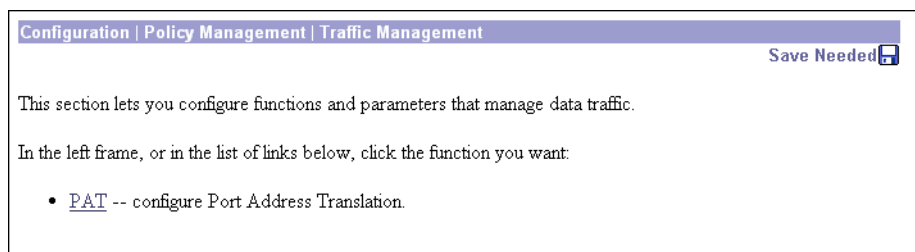
Traffic Management

To enable or disable PAT, click **Traffic Management**.

Configuration | Policy Management | Traffic Management

The Manager displays the **Configuration | Policy Management | Traffic Management** screen.

Figure 11-2: Configuration | Policy Management | Traffic Management screen



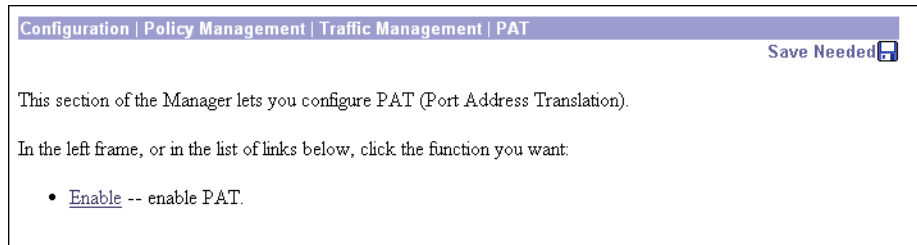
PAT

To configure PAT (Port Address Translation) click **PAT**.

Configuration | Policy Management | Traffic Management | PAT

The **Configuration | Policy Management | Traffic Management | PAT** screen displays.

Figure 11-3: Configuration | Policy Management | Traffic Management | PAT screen



PAT mode provides many-to-one translation; that is, it translates many private network addresses to the single address configured on the public network interface.

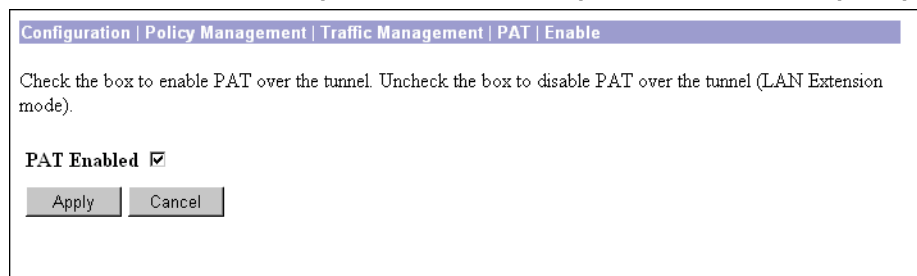
Enable

To enable PAT, click **Enable**.

Configuration | Policy Management | Traffic Management | PAT | Enable

This screen lets you enable or disable PAT, which applies PAT to all configured traffic flowing from the private interface to the public interface.

Figure 11-4: Configuration | Policy Management | Traffic Management | PAT | Enable screen



PAT Enabled

Check the box to enable Client Mode (PAT), or clear it to enable Network Extension Mode.

Note: Remember that to use Network Extension Mode, you must configure an IP address other than the default for the Private interface. If you don't change the IP address of the Private interface, you can't disable PAT.

Apply / Cancel

To enable or disable PAT, and include your setting in the active configuration, click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | PAT** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entry and leave the active configuration unchanged, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | PAT** screen.



Administration

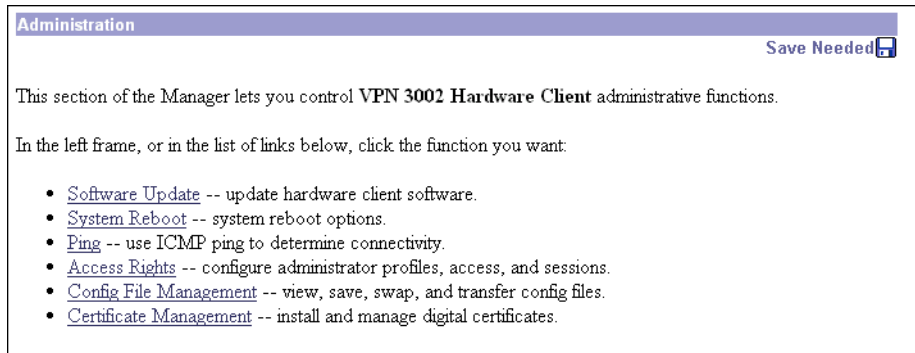
Administering the VPN 3002 involves activities that keep the system operational and secure. Configuring the system sets the parameters that govern its use and functionality as a VPN device, but administration involves higher level activities such as who is allowed to configure the system, and what software runs on it.

Administration

This section of the Manager lets you control administrative functions on the VPN 3002.

- **Software Update:** upload and update the VPN 3002 software image.
- **System Reboot:** set options for VPN 3002 shutdown and reboot.
- **Ping:** use ICMP ping to determine connectivity.
- **Access Rights:** configure administrator profiles, access, and sessions.
 - **Administrators:** configure administrator usernames, passwords, and rights.
 - **Access Settings:** set administrative session idle timeout and limits.
- **Config File Management:** manage configuration files.
 - **View Configuration Files:** view the configuration file currently on the VPN 3002.
 - **Swap Configuration Files:** swap backup and boot configuration files.
 - **Upload Configuration Files:** upload a new configuration file to the VPN 3002.
- **Certificate Management:** install and manage digital certificates.
 - **Enrollment:** create a certificate request to send to a Certificate Authority.
 - **Installation:** install digital certificates.
 - **Certificates:** view, modify, and delete digital certificates.

Figure 12-1: Administration screen



Administration | Software Update

This section of the Manager lets you update the VPN 3002 executable system software. This process uploads the file to the VPN 3002, which then verifies the integrity of the file.

The new image file must be accessible by the workstation you are using to manage the VPN 3002. Software image files ship on the Cisco VPN 3002 CD-ROM. Updated or patched versions are available from the Cisco Website, www.cisco.com, under **Service & Support > Software Center**.

It takes a few minutes to upload and verify the software, and the system displays the progress. Please wait for the operation to finish.

To run the new software image, you must reboot the VPN 3002. The system prompts you to reboot when the update is finished.

We also recommend that you clear your browser's cache after you update the software image: delete all the browser's temporary internet files, history files, and location bar references.

Note: The VPN 3002 has two locations for storing image files: the active location, which stores the image currently running on the system; and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. Updating *twice*, therefore, overwrites the image file in the active location; and the current image file is lost. The Manager displays a warning on this screen if you have already updated the image without rebooting.

Caution: You can *update* the software image while the system is still operating as a VPN device. *Rebooting* the system, however, terminates all active sessions.

While the system is updating the image, do not perform any other operations that affect flash memory (listing, viewing, copying, deleting, or writing files.) Doing so may corrupt memory.

Updating the software image also makes available any new Cisco-supplied configurable selections. When you reboot with the new image, the system updates the active configuration in memory with these new selections, but it does not write them to the CONFIG file until you click the **Save Needed** icon in the Manager window.

Figure 12-2: Administration | Software Update screen

Administration | Software Update

This section lets you update the software on your **VPN 3002 Hardware Client**. VPN 3002 Hardware Client will verify the integrity of the software image that you download. It will take a few minutes for the upload and verification to take place. **Please wait for the operation to finish.**

Current Software Revision:
Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0 (int_66) Jan 22 2001 18:10:43 (DEBUG_MASK 0, NDEBUG off)

Type in the name of the image file below. The current image file is `vpn3002-d-3.0-3des.bin`.

Current Software Revision

The name, version number, and date of the software image currently running on the system.

Browse...

Enter the complete pathname of the new image file, or click **Browse...** to find and select the file from your workstation or network. Cisco-supplied VPN 3002 software image files are named:

The Major and Minor Version numbers are always present; the Sustaining and Patch Version numbers are present only if needed.

Be sure you select the correct file for your VPN 3002; otherwise the update will fail.

Upload / Cancel

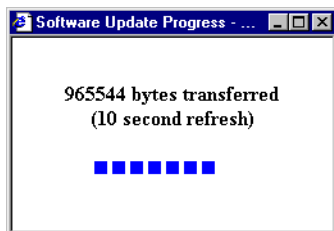
To upload the new image file to the VPN3002, click **Upload**.

To cancel your entries on this screen, *or to stop a file upload that is in progress*, click **Cancel**. The Manager returns to the main **Administration** screen. If you then return to the **Administration | Software Update** screen, you may see a message that a file upload is in progress. Click the highlighted link to stop it and clear the message.

Software Update Progress

This window shows the progress of the software upload. It refreshes the number of bytes transferred at 10-second intervals.

Figure 12-3: Administration | Software Update Progress window



When the upload is finished, or if the upload is cancelled, the progress window closes.

Software Update Success

The Manager displays this screen when it completes the software upload and verifies the integrity of the software. To go to the **Administration | System Reboot** screen, click the highlighted link.

We strongly recommend that you clear your browser's cache after you update the software image: delete all the browser's temporary internet files, history files, and location bar references.

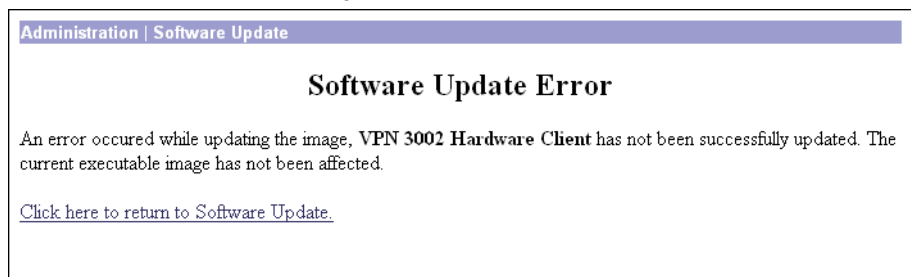
Figure 12-4: Administration | Software Update Success screen



Software Update Error

This screen appears if there was an error in uploading or verifying the image file. You may have selected the wrong file. Click the highlighted link to return to the **Administration | Software Update** screen and try the update again, or contact Cisco support.

Figure 12-5: Administration | Software Update Error screen



Administration | System Reboot

This screen lets you reboot or shutdown (halt) the VPN 3002 with various options.

We strongly recommend that you shut down the VPN 3002 before you turn power off. If you just turn power off without shutting down, you may corrupt flash memory and affect subsequent operation of the system.

If you are logged in the Manager when the system reboots or halts, it automatically logs you out and displays the main login screen. The browser may appear to hang during a reboot; that is, you cannot log in and you must wait for the reboot to finish. You can log back in while the VPN3002 is in a shutdown state, before you turn power off.

If a delayed reboot or shutdown is pending, the Manager also displays a message that describes when the action is scheduled to occur.

Caution: Reboot or shutdown that does not wait for sessions to terminate, terminates all active sessions without warning and prevents new user sessions.

The VPN 3002 automatically saves the current event log file as SAVELOG.TXT when it reboots, and it overwrites any existing file with that name. See **Configuration | System | Events | General, Administration | Config File Management**, and **Monitoring | Filterable Event Log** for more information on the event log file.

Figure 12-6: Administration | System Reboot screen

Administration | System Reboot Save

This section presents reboot options.

If you reboot, the browser may appear to hang as the device is rebooted.

Action

Reboot

Shutdown without automatic reboot

Cancel a scheduled reboot/shutdown

Configuration

Save the active configuration at time of reboot

Reboot without saving the active configuration

Reboot ignoring the configuration file

When to Reboot/Shutdown

Now

Delayed by minutes

At time (24 hour clock)

Wait for sessions to terminate (don't allow new sessions)

Action

Click a radio button to select the desired action. You can select only one action.

Reboot = Reboot the VPN 3002. Rebooting terminates all sessions, resets the hardware, loads and verifies the software image, executes system diagnostics, and initializes the system. A reboot takes about 60-75 seconds. (This is the default selection.)

Shutdown without automatic reboot = Shut down the VPN 3002; that is, bring the system to a halt so you can turn off the power. Shutdown terminates all sessions and prevents new user sessions (but not administrator sessions). While the system is in a shutdown state, the **SYS** LEDs blink on the front panel.

Cancel a scheduled reboot/shutdown = Cancel a reboot or shutdown that is waiting for a certain time or for sessions to terminate. (This is the default selection if a reboot or shutdown is pending.)

Configuration

Click a radio button to select the configuration file handling at reboot. These selections apply to reboot only. You can select only one option.

Save the active configuration at time of reboot = Save the active configuration to the CONFIG file, and reboot using that new file.

Reboot without saving the active configuration = Reboot using the existing CONFIG file and without saving the active configuration. (This is the default selection.)

Reboot ignoring the Configuration file = Reboot using all the factory defaults; i.e., start the system as if it had no CONFIG file. You will need to go through all the Quick Configuration steps described in the *VPN 3002 Getting Started* manual, including setting the system date and time and supplying an IP address for the Ethernet 1 (Private) interface, using the system console. This option *does not* destroy any existing CONFIG file, and it *does not* reset Administrator parameter settings.

When to Reboot/Shutdown

Click a radio button to select when to reboot or shutdown. You can select only one option.

Now = Reboot or shutdown as soon as you click **Apply**. (This is the default selection.)

Delayed by [NN] minutes = Reboot or shutdown NN minutes from when you click **Apply**, based on system time. Enter the desired number in the field; the default is 10 minutes. (FYI: 1440 minutes = 24 hours.)

At time [HH:MM] = Reboot or shutdown at the specified system time, based on a 24-hour clock. Enter the desired time in the field. Use 24-hour notation and enter numbers in all positions. The default is 10 minutes after the current system time.

Wait for sessions to terminate (don't allow new sessions) = Reboot or shutdown as soon as the last session terminates, and don't allow any new sessions in the meantime. If you (the administrator) are the last session, you must log out for the system to reboot or shutdown.

Apply / Cancel

To take action with the selected options, click **Apply**. The Manager returns to the main **Administration** screen if you don't reboot or shutdown now.

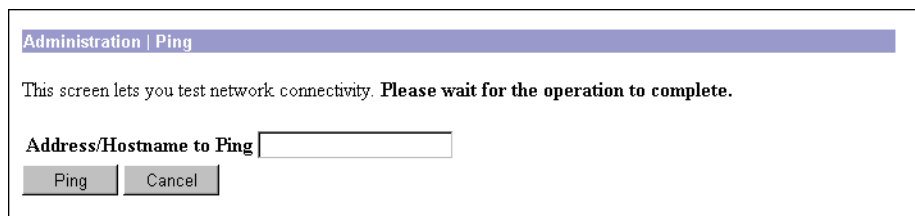
To cancel your settings on this screen, click **Cancel**. The Manager returns to the main **Administration** screen. (Note that this **Cancel** button does not cancel a scheduled reboot or shutdown.)

Administration | Ping

This screen lets you use the ICMP ping (Packet Internet Groper) utility to test network connectivity. Specifically, the VPN3002 sends an ICMP Echo Request message to a designated host. If the host is reachable, it returns an Echo Reply message, and the Manager displays a **Success** screen. If the host is not reachable, the Manager displays an **Error** screen.

You can also **Ping** hosts from the **Administration | Sessions** screen.

Figure 12-7: Administration | Ping screen



Address/Hostname to Ping

Enter the IP address or hostname of the system you want to test. (If you configured a DNS server, you can enter a hostname; otherwise, enter an IP address.) Maximum is 64 characters.

Ping / Cancel

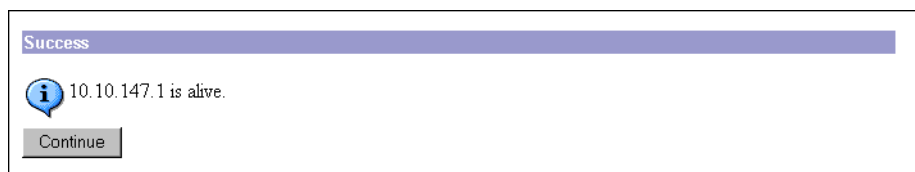
To send the ping message, click **Ping**. The Manager pauses during the test, which may take a few moments; *please wait for the operation to finish*. The Manager then displays either a **Success** or **Error** screen; see below.

To cancel your entry on this screen, click **Cancel**. The Manager returns to the main **Administration** screen.

Success (Ping)

If the system is reachable, the Manager displays a **Success** screen with the name of the tested host.

Figure 12-8: Administration | Ping | Success screen



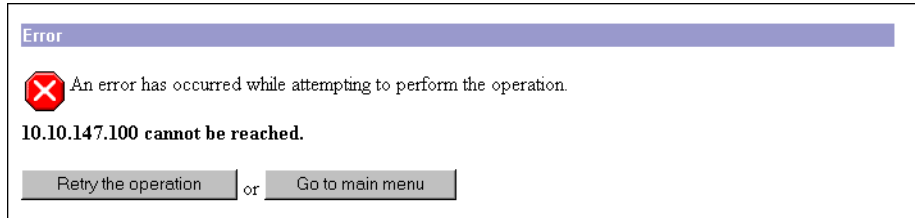
Continue

To return to the **Administration | Ping** screen, click **Continue**.

Error (Ping)

If the system is unreachable for any reason—host down, ICMP not running on host, route not configured, intermediate router down, network down or congested, etc.—the Manager displays an **Error** screen with the name of the tested host. To troubleshoot the connection, try to **Ping** other hosts that you know are working.

Figure 12-9: Administration | Ping | Error screen



To return to the **Administration | Ping** screen, click **Retry the operation**.

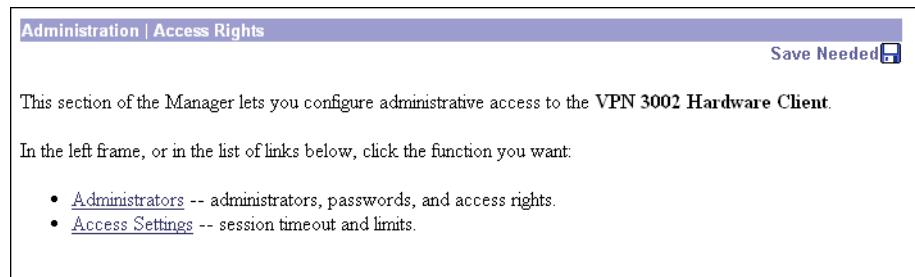
To go to the main Manager screen, click **Go to main menu**.

Administration | Access Rights

This section of the Manager lets you configure and control administrative access to the VPN 3002.

- **Administrators:** configure administrator usernames, passwords, and rights.
- **Access Settings:** set administrative session timeout and limits.

Figure 12-10: Administration | Access Rights screen



Administration | Access Rights | Administrators

Administrators are special users who can access and change the configuration, administration, and monitoring functions on the VPN3002. Only administrators can use the VPN 3002 Hardware Client Manager.

This section of the Manager lets you change administrator properties and rights. Any changes take effect as soon as you click **Apply**.

Figure 12-11: Administration | Access Rights | Administrators screen

Administration | Access Rights | Administrators

This section presents administrator users. Any changes you make take effect immediately.

Administrator <i>admin</i>	Enabled	<input checked="" type="checkbox"/>	Password	<input type="password" value="*****"/>
	Verify			<input type="password" value="*****"/>
Administrator <i>config</i>	Enabled	<input type="checkbox"/>	Password	<input type="password" value="*****"/>
	Verify			<input type="password" value="*****"/>
Administrator <i>monitor</i>	Enabled	<input type="checkbox"/>	Password	<input type="password" value="*****"/>
	Verify			<input type="password" value="*****"/>

Apply Cancel

Administrator

The VPN 3002 has three predefined administrators:

- **admin** = System administrator with access to, and rights to change, all areas. This is the only administrator enabled by default; i.e., this is the only administrator who can log in to, and use, the VPN 3002 Hardware Client Manager as supplied by Cisco.
- **config** = Configuration administrator with access rights to Quick Configuration and monitoring management options only.
- **monitor** = Monitor administrator with rights to monitoring management options only.

Note: The VPN3002 saves Administrator parameter settings from this screen in nonvolatile memory, not in the active configuration (CONFIG) file. Thus, these settings are retained even if the system loses power. These settings are also retained even if you reboot the system with the factory configuration file.

Password

Enter or edit the unique password for this administrator. Maximum is 31 characters. The field displays only asterisks.

Note: *The default password that Cisco supplies is the same as the username. We strongly recommend that you change this password.*

Verify

Re-enter the password to verify it. The field displays only asterisks.

Enabled

Check the box to enable, or clear the box to disable, an administrator. Only enabled administrators can log in to, and use, the VPN 3002 Hardware Client Manager. You must enable at least one administrator, and you can enable all administrators. By default, only **admin** is enabled.

Apply / Cancel

To save this screen's settings in nonvolatile memory, click **Apply**. The settings immediately affect new sessions. The Manager returns to the **Administration | Access Rights** screen.

To discard your settings or changes, click **Cancel**. The Manager returns to the **Administration | Access Rights** screen.

Administration | Access Rights | Access Settings

This screen lets you configure general options for administrator access to the Manager.

Figure 12-12: Administration | Access Rights | Access Settings screen

Administration | Access Rights | Access Settings

This section presents General Access options.

Session Idle Timeout (seconds) Enter the administrative session idle timeout. Limit is 1800 seconds.

Session Limit Enter the maximum number of administrative sessions.

Encrypt Config File Check to enable configuration file encryption.

Session Idle Timeout

Enter the idle timeout period in seconds for administrative sessions. If there is no activity for this period, the Manager session terminates. Minimum is 1, default is 600, and maximum is 1800 seconds (30 minutes).

The Manager resets the inactivity timer only when you click an action button (**Apply**, **Add**, **Cancel**, etc.) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen *does not* reset the timer.

Session Limit

Enter the maximum number of simultaneous administrative sessions allowed. Minimum is 1, default is 10, and maximum is 50 sessions.

Encrypt Config File

To encrypt sensitive entries in the CONFIG file, check the box (default). The CONFIG file is in ASCII text format (.INI format). Check this box to encrypt entries such as passwords, keys, and user information.

To use clear text for all CONFIG file entries, clear the box. For maximum security, we do *not* recommend this option.

Apply / Cancel

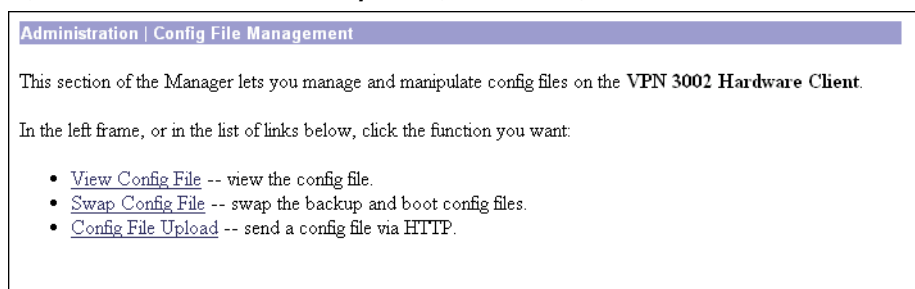
To save your settings in the active configuration, click **Apply**. The Manager returns to the **Administration | Access Rights** screen.

To cancel your settings, click **Cancel**. The Manager returns to the **Administration | Access Rights** screen.

Administration | File Management

This section of the Manager lets you manage config files and view crash dump files in VPN 3002 flash memory. (Flash memory acts like a disk.)

Figure 12-13: Administration | Config File Management screen



View Files

View Files lets you view or delete configuration, crash dump, and saved log files. When you select this option, the **Administration | File Management | View Files** window displays.

Swap Config Files

Swap Config Files lets you swap the boot configuration file with the backup configuration file. When you select this option, the **Administration | File Management | Swap Config Files** window displays.

Config File Upload

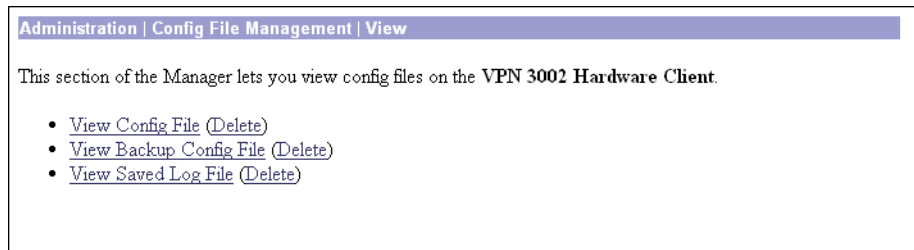
Click Config File Upload to upload a configuration file. When you select this option, the **Administration | File Management | Config File Upload** window displays.

Administration | File Management | View

This window includes these functions:

- **View Config Files:** view, copy, and delete configuration files.
- **View Backup Config Files:** view, copy, and delete backup configuration files.
- **View Crash Dump Files:** view, copy, and delete crash dump files.
- **View Saved Log File:** view, copy, and delete saved log files.

Figure 12-14: Administration | File Management | View screen



View (Save)

To view a file, click **View <Type of File>**. The Manager opens a new browser window to display the file, and the browser address bar shows the filename.

You can also save a copy of the file on the PC that is running the browser. Click the **File** menu on the *new* browser window and select **Save As...** The browser opens a dialog box that lets you save the file. The default filename is the same as on the VPN3002.

Alternatively, you can use the secondary mouse button to click **View** on this Manager screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

Open Link, Open Link in New Window, Open in New Window = Open and view the file in a new browser window, as above.

Save Target As..., **Save Link As...** = Save a copy of the file on your PC. Your system will prompt for a filename and location. The default filename is the same as on the VPN 3002.

When you are finished viewing or saving the file, close the new browser window.

Delete

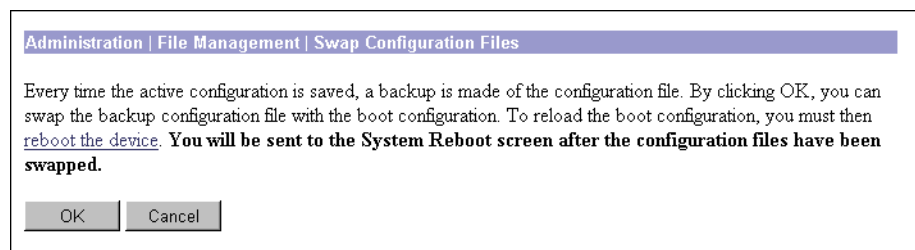
To delete the selected file from flash memory, click **Delete**. The Manager opens a dialog box for you to confirm or cancel. If you confirm, the Manager refreshes the screen and shows the revised list of files.

Administration | File Management | Swap Config Files

This screen lets you swap the boot configuration file with the backup configuration file. Every time you save the active configuration, the system writes it to the CONFIG file, which is the boot configuration file; and it saves the previous CONFIG file as CONFIG.BAK, the backup configuration file.

To reload the boot configuration file and make it the active configuration, you must reboot the system. When you click **OK**, the system automatically goes to the **Administration | System Reboot** screen, where you can reboot the system. You can also click the highlighted link to go to that screen.

Figure 12-15: Administration | Configuration File Management | Swap Config Files screen



OK / Cancel

To swap CONFIG and CONFIG.BAK files, click **OK**. The Manager goes to the **Administration | System Reboot** screen.

To leave the files unchanged, click **Cancel**. The Manager returns to the **Administration | File Management** screen.

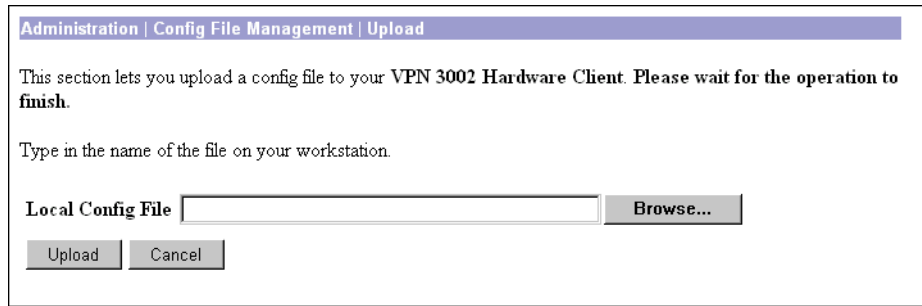
Administration | File Management | Config File Upload

This screen lets you use HTTP (Hypertext Transfer Protocol) to transfer a configuration file from your PC—or a system accessible from your PC—to the VPN 3002 flash memory.

This function provides special handling for configuration (config) files. If the uploaded file has the VPN 3002 filename config, the system deletes any existing config.bak file, renames the existing config file as config.bak, then writes the new config file. However, these actions occur only if the file transfer is successful, so existing files are not corrupted.

To use these functions, you must have **Administrator** or **Configuration Access Rights**. See the **Administration | Access Rights | Administrators** screen.

Figure 12-16: Administration | File Management | Config File Upload screen



Local Config File / Browse...

Enter the name of the file on your PC. In a Windows environment, enter the complete pathname using MS-DOS syntax; e.g., `c:\vpn3002\config0077`. You can also click the **Browse** button to open a file navigation window, find the file, and select it.

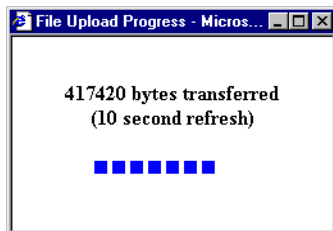
Upload / Cancel

To upload the file to the VPN 3002, click **Upload**. The Manager opens the **File Upload Progress** window. To cancel your entries on this screen, *or to stop a file upload that is in progress*, click **Cancel**. The Manager returns to the **Administration | Config File Management** screen. Stopping an upload may leave a temporary file in VPN 3002 flash memory. Such files are named `TnnnF.nnn` (for example, `T003F.002`). You can delete them on the **Administration | Config File Management | View Config Files** screen.

File Upload Progress

This window shows the progress of the file upload. It refreshes the number of bytes transferred at 10-second intervals.

Figure 12-17: Administration | File Management | File Upload Progress window

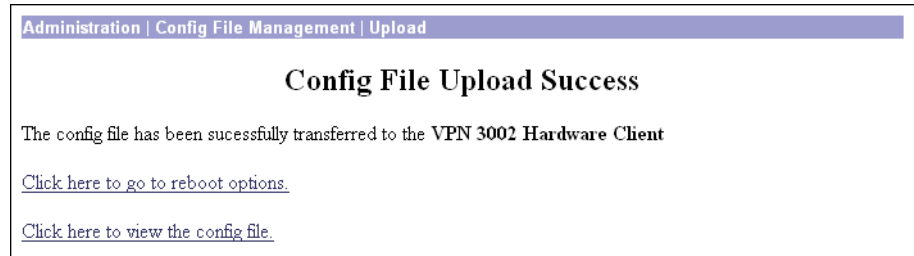


When the upload is finished, or if the upload is cancelled, the progress window closes.

File Upload Success

The Manager displays this screen to confirm that the file upload was successful.

Figure 12-18: Administration | File Management | File Upload Success screen

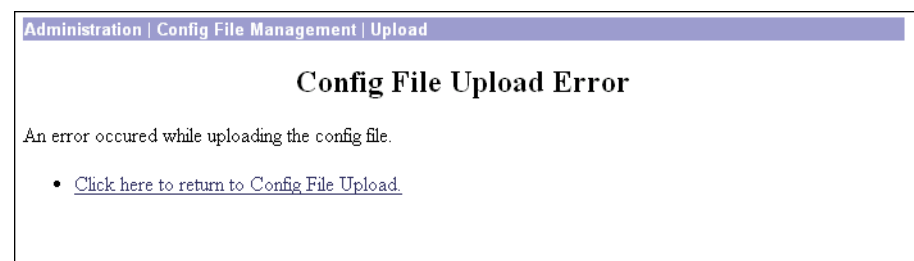


To go to the **Administration | Config File Management | View** screen and examine files in flash memory, click the highlighted link.

File Upload Error

The Manager displays this screen if there was an error during the file upload and the transfer was not successful. Flash memory may be full, or the file transfer may have been interrupted or cancelled.

Figure 12-19: Administration | File Management | File Upload Error screen



Click the link—**Click here to see the list of files**—to go to the **Administration | Config File Management | View** screen and examine space and files in flash memory.

Click the link—**Click here to return to File Upload**—to return to the **Administration | Config File Management | File Upload** screen.

Administration | Certificate Management

This section of the Manager lets you manage digital certificates:

- **Enrollment:** create a certificate request to enroll with a Certificate Authority (CA).
- **Installation:** install certificates on the VPN 3002.
- **Certificates:** view, delete, configure revocation checking, and generate certificates.

Digital certificates are a form of digital identification used for authentication. CAs issue them in the context of a Public Key Infrastructure (PKI), which uses public-key / private-key encryption to ensure security. CAs are trusted authorities who “sign” certificates to verify their authenticity. The systems on each end of the VPN tunnel must have trusted certificates from the same CA, or from different CAs in a hierarchy of trusted relationships; e.g., “A” trusts “B,” and “B” trusts “C,” therefore “A” trusts “C.”

CAs issue **root** certificates (also known as trusted or signing certificates). They may also issue subordinate trusted certificates. Finally, CAs issue **identity** certificates, which are the certificates for specific systems or hosts. There must be at least one identity certificate (and its root certificate) on a given VPN 3002; there may be more than one root certificate.

During IKE (IPSec) Phase 1 authentication, the communicating parties exchange certificate and key information, and they use the public-key / private-key pairs to generate a hash value; if the hash values match, the client is authenticated.

The VPN 3002 supports X.509 digital certificates (International Telecommunications Union Recommendation X.509), including SSL (Secure Sockets Layer) certificates that are self-signed or issued in a PKI context.

On the VPN 3002, digital certificates are stored as encrypted files in a secure area of flash memory. They do not require you to click **Save Needed** to store them, and they are not visible under **Administration | Config File Management**.

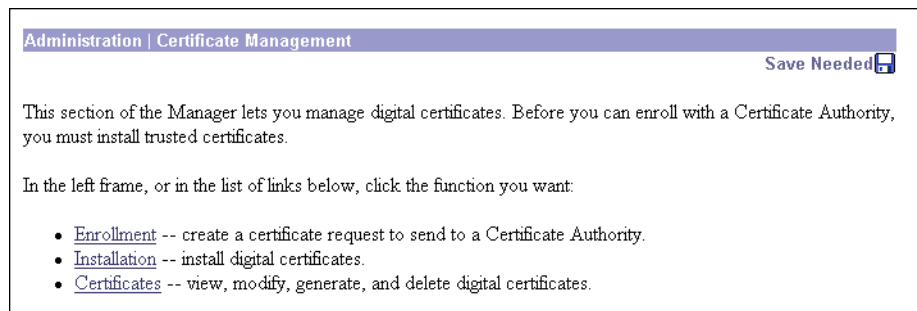
After you install a digital certificate on the VPN 3002, you can use it to negotiate an IPSec tunnel by selecting the check box **Use Certificate** on the **Configuration | System | Tunneling Protocols | IPSec screen**.

The VPN3002 can have only one SSL certificate installed. If you generate a self-signed SSL certificate, it replaces any installed PKI-context SSL certificate; and vice-versa.

For information on using SSL certificates, see *Installing the SSL certificate in your browser* in Chapter 1. See also **Configuration | System | Management Protocols | HTTP/HTTPS** and **Telnet**, and **Configuration | System | Management Protocols | SSL**.

Digital certificates carry a timestamp that determines a time frame for their validity. Therefore, it is essential that the time on the VPN 3002 is correct and synchronized with network time. **Configuration | System | General | Time and Date**.

Figure 12-20: Administration | Certificate Management screen



Installing digital certificates on the VPN 3002

Installing a digital certificate on the VPN 3002 requires these steps:

- 1 Use the **Administration | Certificate Management | Enrollment** screen to generate a certificate request. Save the request as a file, or copy it to the clipboard.
- 2 Process the certificate request to the chosen CA, usually using the CA's Web interface. Most CAs let you submit the request by pasting from the clipboard; otherwise, you can send a file.
- 3 From the CA, receive root (and perhaps subordinate) and identity certificates. *Save them as text files* on your PC or other reachable network host; do not open them or install them in your browser.
- 4 Use the **Administration | Certificate Management | Installation** screen to:

- a Install the root certificate on the VPN 3002 first.
 - b Then install any subordinate certificate(s).
 - c Finally, install the identity certificate.
- 5 Install an SSL certification if the one we generate for you is not good enough?
- 6 Use the **Administration | Certificate Management | Certificates** screen to view the certificates and check them, and perhaps to enable revocation checking.
(You must complete the enrollment and certificate installation process within one week of generating the request.)

See the appropriate **Administration | Certificate Management** screen for more details.

Administration | Certificate Management | Enrollment

This screen lets you generate a certificate request to send to a CA (Certificate Authority), to enroll the VPN 3002 in a PKI.

The entries you make on this screen are governed by PKI standards and practices. The fields conform to ITU-T Recommendation X.520: Selected Attribute Types. You must get from the CA *whether to make an entry* and *what to enter* (format, content, and syntax). You must at least enter the **Common Name (CN)**. All entries may appear in your identity certificate.

When you click **Apply**, the system generates a certificate request; see the **Administration | Certificate Management | Enrollment | Request Generated** screen.

Figure 12-21: Administration | Certificate Management | Enrollment screen

Administration | Certificate Management | Enrollment

This section allows you create a certificate request, so that the VPN 3002 Hardware Client may be enrolled into the PKI. The certificate request may be sent to a CA, which in turn, will send back a certificate. This section may also be used to generate a request for an SSL certificate. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Type in the name of the certificate file below.

Common Name (CN)	<input type="text"/>	Enter the common name for the VPN 3002 Hardware Client to be used in this PKI. For SSL, use the domain name or IP address you will use to connect to this VPN 3002 Hardware Client.
Organizational Unit (OU)	<input type="text"/>	Enter the department.
Organization (O)	<input type="text"/>	Enter the Organization or company.
Locality (L)	<input type="text"/>	Enter the city or town.
State/Province (SP)	<input type="text"/>	Enter the State or Province. Do not abbreviate (i.e. enter <i>Massachusetts</i> , not <i>MA</i>).
Country (C)	<input type="text"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3002 Hardware Client to be used in this PKI.
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA/DSA key pair. Only RSA keys can be used for SSL certificates.

Common Name (CN)

Enter the name for this VPN 3002 that identifies it in the PKI; e.g., Engineering VPN. Spaces are allowed. You must enter a name in this field.

If you are requesting an SSL certificate, enter the IP address or domain name you use to connect to this VPN 3002; e.g., 10.10.147.2.

Organizational Unit (OU)

Enter the name for the department or other organizational unit to which this VPN 3002 belongs; e.g., CPU Design. Spaces are allowed.

Organization (O)

Enter the name for the company or organization to which this VPN 3002 belongs; e.g., Cisco Systems. Spaces are allowed.

Locality (L)

Enter the city or town where this VPN3002 is located; e.g., Franklin. Spaces are allowed.

State/Province (SP)

Enter the state or province where this VPN 3002 is located; e.g., Massachusetts. Spell out completely, do not abbreviate. Spaces are allowed.

Country (C)

Enter the country where this VPN 3002 is located; e.g., US. Use two characters, no spaces, and no periods. This two-character code must conform to ISO 3166 country abbreviations.

Subject Alternative Name (FQDN)

Enter the fully qualified domain name or IP address for this VPN 3002 that identifies it in this PKI; e.g., vpn3030.altiga.com. This field is optional. The alternative name is an additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.

Key Size

Click the drop-down menu button and select the algorithm for generating the public-key / private-key pair, and the key size. If you are requesting an SSL certificate, you must select an RSA choice. Longer key lengths provide stronger security at the expense of increased processing overhead.

RSA 512 bits = Generate 512-bit keys using the RSA (Rivest, Shamir, Adelman) algorithm.

RSA 768 bits = Generate 768-bit keys using the RSA algorithm.

RSA 1024 bits = Generate 1024-bit keys using the RSA algorithm.

DSA 512 bits = Generate 512-bit keys using DSA (Digital Signature Algorithm).

DSA 768 bits = Generate 768-bit keys using the DSA algorithm.

DSA 1024 bits = Generate 1024-bit keys using the DSA algorithm.

OK / Cancel

To generate the certificate request, click **OK**. The Manager displays the **Administration | Certificate Management | Enrollment | Request Generated** screen, which shows the certificate request (see Figure 12-22 below).

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the **Administration | Certificate Management** screen.

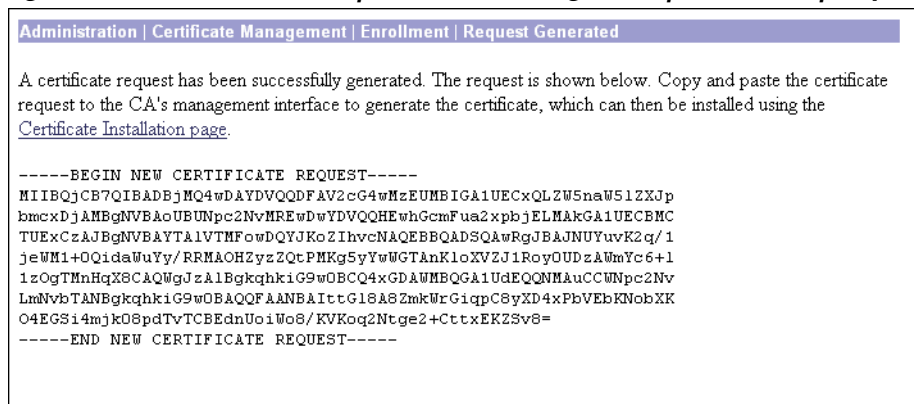
Administration | Certificate Management | Enrollment | Request Generated

The Manager displays this screen when the system has successfully generated a certificate request. The request is a Base-64 encoded file in PKCS-10 format (Public Key Certificate Syntax-10), which most CAs recognize or require. The system automatically saves this file in flash memory with the filename shown in the screen (pkcsNNNN.txt).

In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN 3002, and it is not visible.

You must complete the enrollment and certificate installation process within two weeks of generating the request.

Figure 12-22: Administration | Certificate Management | Enrollment | Request Generated screen



To go to the **Certificate Installation** screen, click the highlighted *Certificate Installation page* link.

Enrolling with a Certificate Authority

To send the certificate request to a CA, enroll, and receive your digital certificates, follow these steps. (These are cut-and-paste steps; your CA may follow different procedures. In any case, you must end up with certificates *saved as text files* on your PC or other reachable network host.)

- 1 Select and copy the certificate request from the browser window to your clipboard.
- 2 Use a browser to connect to the CA's Web site. Navigate to the screen that lets you submit a PKCS-10 request via cut-and-paste.
- 3 Paste the certificate request in the CA screen, and submit the request.
- 4 The CA should respond with a new browser screen that says the certificates were successfully generated. That screen also should include active links that let you "Download the root certificate" and "Download the identity certificate."
- 5 *With the secondary mouse button*, click the root certificate download link and select **Save Link As** or **Save Target As**. You want to *save the file as a text file* on your PC or other reachable network host; *do not open it or install it in the browser*. The browser opens a dialog box that lets you navigate to the desired location and enter a filename. Use a name that clearly identifies this as a root certificate, with a .txt extension.

- 6 Repeat the previous step for any subordinate certificates, and finally for the *identity* certificate. Name the files so that you can distinguish the certificate types.
- 7 Proceed to the **Administration | Certificate Management | Installation** screen below.

Administration | Certificate Management | Installation

This Manager screen lets you install digital certificates on the VPN 3002.

You can install certificates obtained via enrollment with a CA in a PKI (where the private key is generated on—and stays hidden on—the VPN 3002).

Note: You must install the CA root certificate first, then install any other subordinate certificates from the CA. Install the identity certificate last.

You can also install an SSL server identity certificate issued in a PKI context (not a self-signed SSL certificate). If you install such a certificate, it replaces any self-signed SSL certificate. The VPN 3002 can have only one SSL certificate, regardless of type.

Figure 12-23: Administration | Certificate Management | Installation screen

Certificate Type

Click the drop-down menu button and select the type of digital certificate to install.

Issuing or Root Certificate Authority = Root and subordinate certificates obtained from a CA. Select this type and install the root certificate first, then install any subordinate certificates.

SSL Server (via Enrollment) = SSL certificate obtained via enrollment in a PKI.

SSL Server (import with Private Key) = SSL certificate imported along with a private key from some source. *Installing this certificate type is not a completely secure process, and we do not recommend using it.* If you select this type, complete the **Certificate Password** and **Verify** fields below.

Server Identity (via Enrollment) = Identity certificates obtained via enrollment with a CA in a PKI. Select this type and install the identity certificate last.

Certificate Password

Complete this field only if you select an **import with Private Key** certificate type. Enter the password for the private key.

Verify

Complete this field only if you select an **import with Private Key** certificate type. Re-enter the private key password to verify it.

Local File / Browse

Enter the complete path and filename of the certificate you are installing; e.g.,
d:\certs\ca_root.txt. Or click **Browse** to navigate to the file on your PC or other reachable network host.

Certificate Text

You can enter the certificate text in either of two ways. If the certificate text is stored in a file, then enter the file name in the **Local File/Browse** field above. If the text of the certificate is displaying in another open window, you can copy and paste it here. This scrollable input field allows you to enter the certificate text directly, without having to save it to a file first.

OK / Cancel

To install the certificate, click **OK**. The Manager displays the **Administration | Certificate management | Certificates** screen.

To discard your entries and cancel the operation, click **Cancel**. The Manager returns to the **Administration | Certificate Management** screen.

Administration | Certificate Management | Certificates

This screen shows all the certificates installed in the VPN 3002 and lets you view and delete certificates. You can also generate a self-signed SSL server certificate.

The Manager displays this screen each time you install a digital certificate.

Figure 12-24: Administration | Certificate Management | Certificates screen

Administration | Certificate Management | Certificates

This section lets you view certificates on the VPN 3002 Hardware Client.

Certificate Authorities

Subject	Issuer	Expiration	Actions
No Certificate Authorities			

Identity Certificates

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificate [Generate]

Subject	Issuer	Expiration	Actions
192.168.10.1 at Cisco Systems, Inc.	192.168.10.1 at Cisco Systems, Inc.	12/30/2001	[View] [Delete]

Note: The public key in the SSL certificate is also used for the SSH host key.

Certificate Authorities

This table shows installed root and subordinate (trusted) certificates issued by Certificate Authorities (CAs).

Identity Certificates

This table shows installed server identity certificates.

SSL Certificate / [Generate]

This table shows the SSL server certificate installed on the VPN3002. The system can have only one SSL server certificate installed: either a self-signed certificate or one issued in a PKI context.

To generate a self-signed SSL server certificate, click **Generate**. The system uses parameters set on the **Configuration | System | Management Protocols | SSL** screen and generates the certificate. The new certificate replaces any existing SSL certificate.

Subject / Issuer

The Common Name (**CN**) or Organizational Unit (**OU**) (if present), plus the Organization (**O**) in the **Subject** and **Issuer** fields of the certificate. The format is CN at O, OU at O, or just O; e.g., Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See **Administration | Certificate Management | Certificates | View**.

Expiration

The expiration date of the certificate. Format is MM/DD/YYYY.

Actions/View/Delete

To view details of this certificate, click **View**. The Manager opens the **Administration | Certificate Management | Certificates | View** screen; see below.

To delete this certificate from the VPN 3002, click **Delete**. The Manager opens the **Administration | Certificate Management | Certificates | Delete** screen; see below.

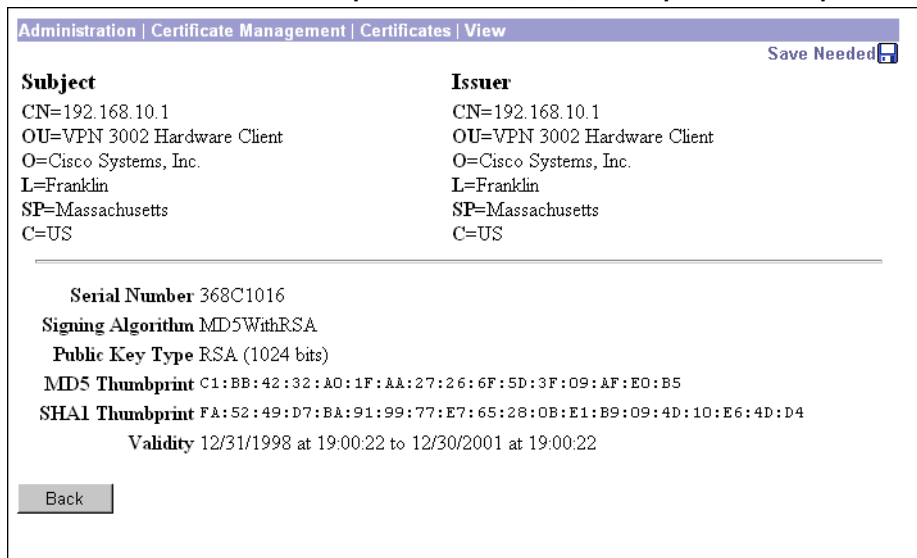
Administration | Certificate Management | Certificates | View

The Manager displays this screen of certificate details when you click **View** for a certificate on the **Administration | Certificate Management | Certificates** screen. The details vary depending on the certificate content.

The content and format for certificate details are governed by ITU (International Telecommunication Union) X.509 standards, specifically RFC 2459. The **Subject** and **Issuer** fields conform to ITU X.520.

This screen is read-only; you cannot change any information here.

Figure 12-25: Administration | Certificate Management | Certificates | View screen



Subject

The person or system that uses the certificate. For a CA root certificate, the **Subject** and **Issuer** are the same.

Issuer

The CA or other entity (jurisdiction) that issued the certificate.

Subject and **Issuer** consist of a specific-to-general identification hierarchy: **CN**, **OU**, **O**, **L**, **SP**, and **C**. These labels and acronyms conform to X.520 terminology, and they echo the fields on the **Administration | Certificate Management | Enrollment** screen.

CN=

Common Name: the name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.

For the VPN 3002 self-signed SSL certificate, the **CN** is the IP address on the Ethernet 1 (Private) interface at the time the certificate is generated. SSL compares this CN with the address you use to connect to the VPN 3002 via HTTPS, as part of its validation.

OU=

Organizational Unit: the subgroup within the organization (**O**).

O=

Organization: the name of the company, institution, agency, association, or other entity.

L=

Locality: the city or town where the organization is located.

SP=

State/Province: the state or province where the organization is located.

C=

Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.

Serial Number

The serial number of the certificate. Each certificate issued by a CA or other entity must have a unique identifies. The serial number serves this purpose.

Signing Algorithm

The cryptographic algorithm that the CA or other issuer used to sign this certificate.

Public Key Type

The algorithm and size of the public key that the CA or other issuer used in generating this certificate.

Certificate Usage

The purpose of the key contained in the certificate; e.g., digital signature, certificate signing, nonrepudiation, key or data encipherment, etc. This field displays only if a key usage extension is present.

MD5 Thumbprint

A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.

SHA1 Thumbprint

A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.

Validity

The time period during which this certificate is valid.

Format is MM/DD/YYYY at HH:MM:SS AM/PM to MM/DD/YYYY at HH:MM:SS AM/PM. Time uses 12-hour AM/PM notation, and is local system time.

Subject Alternative Name (Fully Qualified Domain Name)

The fully qualified domain name for this VPN 3002 that identifies it in this PKI. The alternative name is an optional additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections. This field displays only if the FQDN extension is present.

Back

To return to the **Administration | Certificate Management | Certificates** screen, click **Back**.

Administration | Certificate Management | Certificates | Delete

The Manager displays this confirmation screen when you click **Delete** for a certificate on the **Administration | Certificate Management | Certificates** screen. The screen shows the same certificate details as on the **Administration | Certificate Management | Certificates | View** screen.

Please note:

- You must delete all identity certificates in the certificate chain before you can delete the trusted certificates. Otherwise the Manager displays an error message.
- If the certificate is in use by an SA, the Manager displays an error message.
- If you delete the SSL certificate, the Manager displays `Error getting SSL Certificate: SSLIOERR` in the **SSL Certificate** table. Generate a new SSL certificate to clear this message.

Figure 12-26: Administration | Certificate Management | Certificates | Delete screen

Administration | Certificate Management | Certificates | Delete Save Needed

Subject	Issuer
CN=192.168.10.1	CN=192.168.10.1
OU=VPN 3002 Hardware Client	OU=VPN 3002 Hardware Client
O=Cisco Systems, Inc.	O=Cisco Systems, Inc.
L=Franklin	L=Franklin
SP=Massachusetts	SP=Massachusetts
C=US	C=US

Serial Number 368C1016
Signing Algorithm MD5WithRSA
Public Key Type RSA (1024 bits)
MD5 Thumbprint C1:BB:42:32:A0:1F:AA:27:26:6F:5D:3F:09:AF:EO:B5
SHA1 Thumbprint FA:52:49:D7:BA:91:99:77:E7:65:28:0B:E1:B9:09:4D:10:E6:4D:D4
Validity 12/31/1998 at 19:00:22 to 12/30/2001 at 19:00:22

Are you **sure** you want to delete this certificate?

Yes / No

To delete this certificate, click **Yes**. *There is no undo*. The Manager returns to the **Administration | Certificate Management | Certificates** screen and shows the remaining certificates.

To retain this certificate, click **No**. The Manager returns to the **Administration | Certificate Management | Certificates** screen, and the certificates are unchanged.



Monitoring

The VPN 3002 tracks many statistics and the status of many items essential to system administration and management. This section of the Manager lets you view all those status items and statistics. You can even see the state of LEDs that show the status of hardware subsystems in the device. You can also see statistics that are stored and available in standard MIB-II data objects.

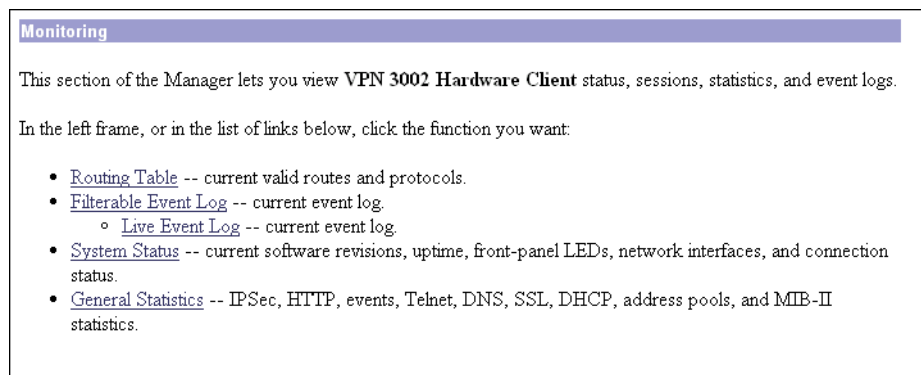
Monitoring

This section of the Manager lets you view VPN 3002 status, sessions, statistics, and event logs.

- **Routing Table:** current valid routes, protocols, and metrics.
- **Filterable Event Log:** current event log in memory, filterable by event class, severity, IP address, etc.
 - **Live Event Log:** current event log, continuously updated.
- **System Status:** current software revisions, uptime, network interfaces, and connection status.
- **General Statistics:** IPSec, HTTP, Telnet, DNS, SSL, DHCP, SSH
 - MIB-II statistics for interfaces, TCP/UDP, IP, ICMP, the ARP table, Ethernet traffic, and SNMP.

These Manager screens are read-only “snapshots” of data or status at the time the screen displays. Most screens have a **Refresh** button that you can click to get a fresh snapshot and update the screen, but you cannot modify the data on the screen.

Figure 13-1: Monitoring screen



Monitoring | Routing Table

This screen shows the VPN3002 routing table at the time the screen displays.

Figure 13-2: Monitoring | Routing Table screen

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	130.0.0.1	Public Interface	Default	0	1
130.0.0.0	255.255.0.0	0.0.0.0	Public Interface	Local	0	1
192.168.10.0	255.255.255.0	0.0.0.0	Private Interface	Local	0	1

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Clear Routes

Clears the dynamic routing entries from the display. Clicking this button does not affect the display of static routing entries.

Valid Routes

The total number of current valid routes that the VPN 3002 knows about. This number includes *all* valid routes, and it may be greater than the number of rows in the routing table, which shows only the best routes with duplicates removed.

Address

The packet destination IP address that this route applies to. This address is combined with the subnet mask to determine the destination route. 0.0.0.0 indicates the default gateway.

Mask

The subnet mask for the destination IP address in the **Address** field. 0.0.0.0 indicates the default gateway.

Next Hop

For remote routes, the IP address of the next system in the path to the destination. 0 . 0 . 0 . 0 indicates a local route; i.e., there is no next hop.

Interface

The VPN 3002 network interface through which traffic moves on this route:

Private interface

Public interface

Protocol

The protocol or source of this routing table entry:

Static = configured static route.

Local = local VPN 3002 interface address.

ICMP = learned from an ICMP (Internet Control Message Protocol) redirect message.

Default = the default gateway.

Age

The number of seconds since this route was last updated or otherwise validated. The age is relative to the screen display time; e.g., 25 means the route was last validated 25 seconds before the screen was displayed. 0 indicates a static, local, or default route.

Metric

The metric, or cost, of this route. 1 is lowest, 16 is highest.

Monitoring | Filterable Event Log

This screen shows the events in the current event log, lets you filter and display events by various criteria, and lets you manage the event log file. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN 3002 records events in nonvolatile memory, thus the event log persists even if the system is powered off. It holds 256 events, and it wraps when it is full; that is, entry 0 or 257 overwrites entry 1, etc. Use the scroll controls (if present) to display more events in the log.

To configure event handling, see the **Configuration | System | Events** screens.

To **Get**, **Save**, or **Clear** the event log file, you must have **Access Rights** to **Read/Write Files**. See the **Administration | Administrators | Modify Properties** screen.

Figure 13-3: Monitoring | Filterable Event Log screen

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE

Severities: ALL, 1, 2, 3

Client IP Address: 0.0.0.0

Events/Page: 100

Direction: Oldest to Newest

Navigation: [Back] [Forward] [Refresh] [Get Log] [Clear Log]

```

33 01/26/2001 11:23:37.030 SEV=4 AUTH/21 RPT=2
User admin connected

34 01/26/2001 11:23:51.700 SEV=5 AUTH/32 RPT=2
User [ ] attempted ADMIN logon.. <ACCESS GRANTED> !

35 01/26/2001 11:23:51.700 SEV=4 AUTH/21 RPT=3
User admin connected

36 01/26/2001 11:23:58.950 SEV=4 IKE/41 RPT=2
IKE Initiator: New Phase 2, Intf 2, IKE Peer 130.0.0.1
local Proxy Address 10.10.99.32, remote Proxy Address 0.0.0.0,
SA (ESP-3DES-MD5)

38 01/26/2001 11:23:58.990 SEV=5 IKE/73 RPT=3 130.0.0.1
Group [130.0.0.1]
Responder forcing change of IPSec rekeying duration from 2147483647 to 28800 seconds

41 01/26/2001 11:23:59.010 SEV=4 IKE/49 RPT=2 130.0.0.1
Group [130.0.0.1]
Security negotiation complete for peer (130.0.0.1)
Initiator, Inbound SPI = 0x26638275, Outbound SPI = 0x6b982583

```

Select Filter Options

You can select any or all of the following options for filtering and displaying the event log. After selecting the option(s), click any one of the four **Page** buttons. The Manager refreshes the screen and displays the event log according to your selections.

Your filter options remain in effect as long as you continue working within and viewing **Monitoring | Filterable Event Log** screens. The Manager resets all options to their defaults if you leave and return, or if you click **Filterable Event Log** in the left frame of the Manager window (the table of contents). You cannot save filter options.

Event Class

To display all the events in a single event class, click the drop-down menu button and select the event class. To select a contiguous range of event classes, select the first class in the range, hold down the keyboard **Shift** key, and select the last class in the range. To select multiple event classes, select the first class, hold down the keyboard **Ctrl** key, and select the other classes. By default, the Manager displays **All Classes** of events. Table 9-1 under **Configuration | System | Events** describes the event classes.

Severities

To display all events of a single severity level, click the drop-down menu button and select the severity level. To select a contiguous range of severity levels, select the first severity level in the range, hold down the keyboard **Shift** key, and select the last severity level in the range. To select multiple severity levels, select the first severity level, hold down the keyboard **Ctrl** key, and select the other severity levels. By default, the Manager displays **All** severity levels. See Table 9-2 under **Configuration | System | Events** for an explanation of severity levels.

Client IP Address

To display all events relating to a single IP address, enter the IP address in the field using dotted decimal notation; e.g., 10.10.1.35. By default, the Manager displays all IP addresses. To restore the default, enter 0.0.0.0.

Events/Page

To display a given number of events per Manager screen (page), click the drop-down menu button and select the number. Choices are **10**, **25**, **50**, **100**, **250**, and **ALL**. By default, the Manager displays **100** events per screen.

Direction

To display events in a different chronological order, click the drop-down menu button and select the order. Choices are:

Oldest to Newest = Display events in actual chronological order, with oldest events at the top of the screen. This is the default selection.

Newest to Oldest = Display events in reverse chronological order, with newest events at the top of the screen.

First Page

To display the first page (screen) of the event log, click this button. By default, the Manager displays the first page of the event log when you first open this screen.

Previous Page

To display the previous page (screen) of the event log, click this button.

Next Page

To display the next page (screen) of the event log, click this button.

Last Page

To display the last page (screen) of the event log, click this button.

All four **Page** buttons are also present at the bottom of the screen.

Get Log

To download the event log from VPN 3002 memory to your PC and view it or save it as a text file, click **Get Log**. The Manager opens a new browser window to display the file. The browser address bar shows the VPN 3002 address and log file default filename; for example, `http://10.10.4.6/LOG/vpn3002log.txt`.

To save a copy of the log file on your PC, click the **File** menu on the *new* browser window and select **Save As...** The browser opens a dialog box that lets you save the file. The default filename is `vpn3002log.txt`.

Alternatively, you can use the *secondary* mouse button to click **Get Log** on this **Monitoring | Filterable Event Log** screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

Open Link, Open Link in New Window, Open in New Window = Open and view the file in a new browser window, as above.

Save Target As..., Save Link As... = Save a copy of the log file on your PC. Your system will prompt for a filename and location. The default filename is `vpn3002log.txt`.

When you are finished viewing or saving the file, close the new browser window.

Clear Log

To clear the current event log from memory, click this button. The Manager then refreshes the screen and shows the empty log.

Caution: The Manager immediately erases the event log from memory without asking for confirmation. *There is no undo.*

Event log format

Each entry (record) in the event log consists of eight or nine fields:

Sequence Date Time Severity Class/Number Repeat (IPAddress)
String

(The `IPAddress` field appears in only certain events.)

For example:

```
3 12/06/1999 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35
New administrator login: admin.
```

Event sequence

The sequential number of the logged entry. Numbering starts or restarts from 1 when the system powers up, when you save the event log, or when you clear the event log. When the log file wraps after 256 entries, numbering continues with event or 257 overwriting event 1.

Although numbering restarts at 1 when the system powers up, it does *not* overwrite existing entries in the event log; it appends them. Assuming the log doesn't wrap, it could contain several sequences of events starting at 1. Thus you can examine events preceding and following reboot or reset cycles.

Event date

The date of the event: MM/DD/YYYY. For example, 12/06/1999 identifies an event that occurred on December 6, 1999.

Event time

The time of the event: hour:minute:second.millisecond. The hour is based on a 24-hour clock. For example, 14:37:06.680 identifies an event that occurred at 2:37:06.680 PM.

Event severity

The severity level of the event; for example: SEV=4 identifies an event of severity level 4. See Table 9-2 under **Configuration | System | Events** for an explanation of severity levels.

Event class / number

The class—or source—of the event, and the internal reference number associated with the specific event within the event class. For example: HTTP/47 identifies that an administrator logged in to the VPN 3002 using HTTP to connect to the Manager. Table 9-1 under **Configuration | System | Events** describes the event classes. The internal reference number assists Cisco support personnel if they need to examine a log file.

Event repeat

The number of times that this specific event has occurred since the VPN 3002 was last booted or reset. For example, RPT=17 indicates that this is the 17th occurrence of this specific event.

Event IP address

The IP address of the client or host associated with this event. Only certain events have this field. For tunnel-related events, this is typically the “outer” or tunnel endpoint address. In the **Event log format** example above, 10.10.1.35 is the IP address of the host PC from which admin logged in using the Manager.

Event string

The string, or message, that describes the specific event. Each event class comprises many possible events, and the string gives a brief description. Event strings usually do not exceed 80 characters. In the **Event log format** example above, “New administrator login: admin” describes the event.

Monitoring | Live Event Log

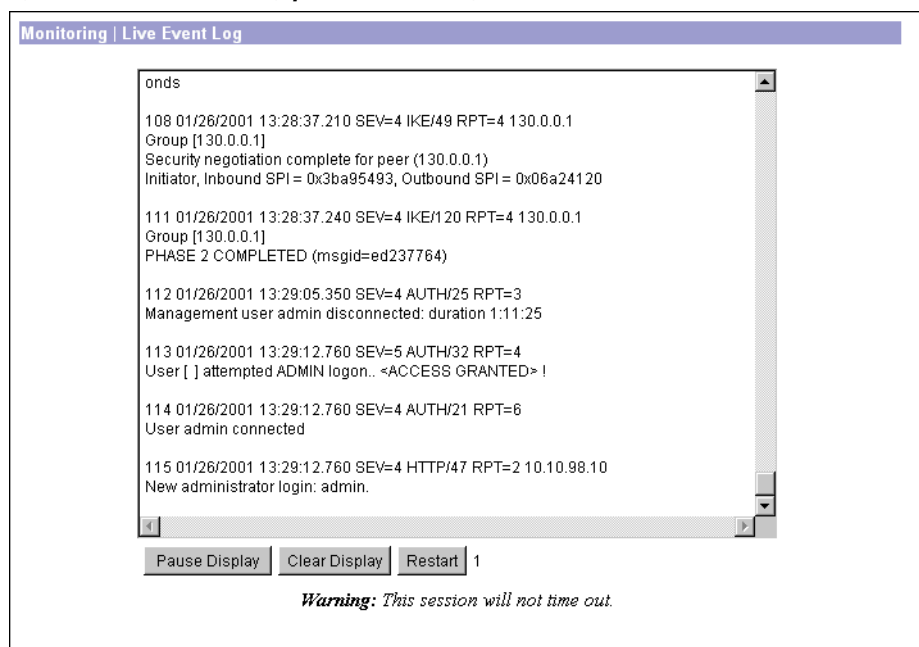
This screen shows events in the current event log and automatically updates the display every 5 seconds. The events may take a few seconds to load when you first open the screen.

Note for Netscape users: The live event log requires Netscape versions 4.5, 4.6, or 4.7. It does not run on other versions of Netscape.

The screen always displays the most recent event at the bottom. Use the scroll bar to view earlier events. To filter and display events by various criteria, see the *Monitoring | Filterable Event Log* section above.

Note: If you keep this Manager screen open, your administrative session does not time out. Each automatic screen update resets the inactivity timer. See **Session Idle Timeout** on the **Administration | Access Rights | Access Settings** screen.

Figure 13-4: Monitoring | Live Event Log screen



Pause Display / Resume Display

To pause the display, click **Pause Display**. While paused, the screen does not display new events, the button changes to **Resume Display**, and the timer counts down to 0 and stops. You can still scroll through the event log. Click the button to resume the display of new events and restart the timer.

Clear Display

To clear the event display, click **Clear Display**. This action *does not* clear the event log, only the display of events on this screen.

Restart

To clear the event display and reload the entire event log in the display, click **Restart**.

Timer

The timer counts 5 – 4 – 3 – 2 – 1 to show where it is in the 5-second refresh cycle. A momentary Rx indicates receipt of new events. A steady 0 indicates the display has been paused.

Monitoring | System Status

This screen shows the status of several software and hardware variables at the time the screen displays. From this screen you can also display the status of the IPSec tunnel SAs, tunnel duration, plus front and rear panel displays of the VPN 3002.

Figure 13-5: Monitoring | System Status screen

Monitoring | System Status
Friday, 26 January 2001 13:39:30

[Refresh](#)


VPN Client Type: 3002-8E
Bootcode Rev: Cisco Systems, Inc./VPN 3000 Concentrator Series Version 2.5.int_63 Jan 19 2001 13:35:58
Software Rev: Cisco Systems, Inc./VPN 3002 Hardware Client Version 3.0 (int_66) Jan 22 2001 18:10:43
 (DEBUG_MASK 0, NDEBUG off)
Up Since: 01/26/2001 12:02:03
RAM Size: 16 MB

Disconnect Now
Connect Now

Tunnel Established to: 130.0.0.1
Duration: 0:11:00
Security Associations:

Type	Encryption	Authentication	Octets In	Octets Out	Packets In	Packets Out	Other
IKE	3DES/MD5	Pre-Shared Key	8248	8365	93	95	Aggressive Mode, DH Group2
IPSec	3DES	HMAC/MD5	0	0	0	0	
IPSec	3DES	HMAC/MD5	126632	434528	674	856	

In the pictures below, select and click a module for status details.



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

VPN Client Type

The type, or model number, of this VPN client.

Bootcode Rev

The version name, number, and date of the VPN 3002 bootcode software file. When you boot or reset the system, the bootcode software runs system diagnostics, and it loads and executes the system software image. The bootcode is installed at the factory, and there is no need to upgrade it. If an engineering change requires a bootcode upgrade, only Cisco support personnel can do so.

Software Rev

The version name, number, and date of the VPN 3002 Hardware Client system software image file. You can update this image file from the **Administration | Software Update** screen.

Up Since

The date and time that the VPN 3002 was last booted or reset.

RAM Size

The total amount of SDRAM memory installed in the VPN 3002.

Disconnect Now

Disconnects the tunnel.

Connect Now

Connects the tunnel.

Assigned IP Address

The IP address assigned to the VPN 3002 by the central-site Concentrator when PAT mode is enabled. This field is not displayed when the VPN 3002 is running in Network Extension mode, because the central-site Concentrator does not assign an IP address to the VPN 3002 in Network Extension mode.

Tunnel Established to:

The IP address of the VPN 3000 Concentrator to which this VPN 3002 connects.

Duration:

The length of time that this tunnel has been up.

Security Associations:

This table describes the following attributes of the SAs for this VPN 3002.

Type

The type of tunnel for this SA, either IPSec or IKE (the control tunnel).

Encryption

The encryption method this SA uses.

Authentication

The authentication method this SA uses.

Octets In

The number of octets (bytes) this SA has received since the tunnel has been up.

Octets Out

The number of octets (bytes) this SA has sent since the tunnel has been up.

Packets In

The number of packets this SA has received since the tunnel has been up.

Packets Out

The number of packets this SA has sent since the tunnel has been up.

Other

Additional information about this SA, including mode.

Front Panel

The front panel image is an inactive link.

Back Panel

The back panel image includes active links for the VPN 3002 Private and Public interfaces. Use the mouse pointer to select either the private or public module on the back-panel image and click anywhere in the highlighted area. The Manager displays the appropriate **Monitoring | System Status | Interface** screen.

Monitoring | System Status | Private/Public Interface

This screen displays status and statistics for a VPN 3002 Ethernet interface. To configure an interface, see **Configuration | Interfaces**.

Figure 13-6: Monitoring | System Status | Ethernet Interface screen

Interface	Public Interface
IP Address	130.0.0.2
Status	UP
Rx Unicast	3031
Tx Unicast	3397
Rx Multicast	0
Tx Multicast	0
Rx Broadcast	0
Tx Broadcast	8

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the **Monitoring | System Status** screen, click **Back**.

Interface

The VPN 3002 Ethernet interface number:

Private interface

Public interface

IP Address

The IP address configured on this interface.

Status

The operational status of this interface:

`UP` = configured and enabled, ready to pass data traffic.

`DOWN` = configured but disabled.

`Testing` = in test mode; no regular data traffic can pass.

`Dormant` = configured and enabled but waiting for an external action, such as an incoming connection.

`Not Present` = missing hardware components.

`Lower Layer Down` = not operational because a lower-layer interface is down.

`Unknown` = not configured.

Rx Unicast

The number of unicast packets that were received by this interface since the VPN 3002 was last booted or reset. Unicast packets are those addressed to a single host.

Tx Unicast

The number of unicast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Rx Multicast

The number of multicast packets that were received by this interface since the VPN 3002 was last booted or reset. Multicast packets are those addressed to a specific group of hosts.

Tx Multicast

The number of multicast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Rx Broadcast

The number of broadcast packets that were received by this interface since the VPN 3002 was last booted or reset. Broadcast packets are those addressed to all hosts on a network.

Tx Broadcast

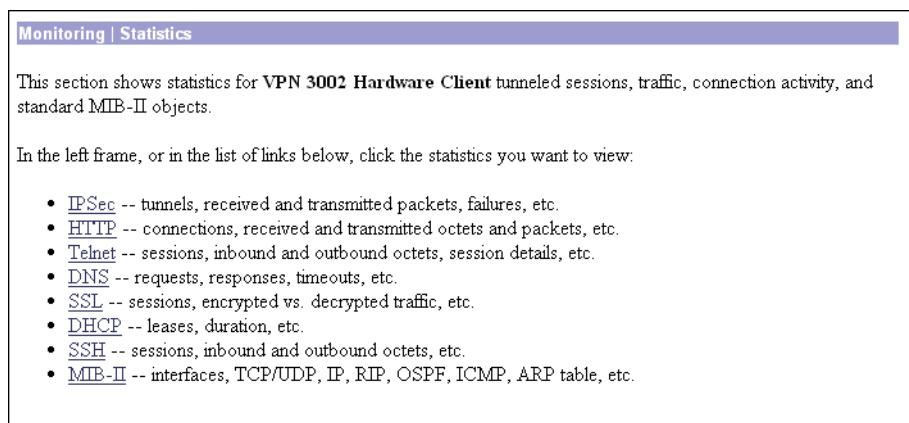
The number of broadcast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitoring | Statistics

This section of the Manager shows statistics for traffic and activity on the VPN3002 since it was last booted or reset, and for current tunneled sessions, plus statistics in standard MIB-II objects for interfaces, TCP/UDP, IP, ICMP, the ARP table, and SNMP.

- **IPSec**: total Phase 1 and Phase 2 tunnels, received and transmitted packets, failures, drops, etc.
- **HTTP**: total data traffic and connection statistics.
- **Telnet**: total sessions, and current session inbound and outbound traffic.
- **DNS**: total requests, responses, timeouts, etc.
- **SSL**: total sessions, encrypted vs. unencrypted traffic, etc.
- **DHCP**: leased addresses, duration, etc.
- **SSH**: total and active sessions, bytes and packets sent and received, etc.
- **MIB-II Stats**: interfaces, TCP/UDP, IP, ICMP, the ARP table, Ethernet, and SNMP.

Figure 13-7: Monitoring | Statistics screen



Monitoring | Statistics | IPSec

This screen shows statistics for IPSec activity—including the current IPSec tunnel—on the VPN 3002 since it was last booted or reset. These statistics conform to the IETF draft for the IPSec Flow Monitoring MIB.

Figure 13-8: Monitoring | Statistics | IPSec screen

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	1
Total Tunnels	1	Total Tunnels	1
Received Bytes	2468	Received Bytes	2544
Sent Bytes		Sent Bytes	
Received Packets	30	Received Packets	23
Sent Packets	5	Sent Packets	0
Received Packets Dropped	25	Received Packets Dropped	1
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	0	Sent Packets Dropped	0
Sent Notifies	2	Inbound Authentications	22
Received Phase-2 Exchanges		Failed Inbound Authentications	0
Sent Phase-2 Exchanges		Outbound Authentications	0
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	22
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	0
Phase-2 SA Delete Requests Received	0	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	0	System Capability Failures	
Initiated Tunnels	0	No-SA Failures	
Failed Initiated Tunnels	0	Protocol Use Failures	
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	0		

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IKE (Phase 1) Statistics

This table provides IPSec Phase 1 (IKE: Internet Key Exchange) global statistics. During IPSec Phase 1 (IKE), the two peers establish control tunnels through which they negotiate Security Associations.

Active Tunnels

The number of currently active IKE control tunnels.

Total Tunnels

The cumulative total of all currently and previously active IKE control tunnels.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IKE tunnels.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IKE tunnels.

Received Packets

The cumulative total of packets received by all currently and previously active IKE tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IKE tunnels.

Received Packets Dropped

The cumulative total of packets that were dropped during receive processing by all currently and previously active IKE tunnels. If there is a problem with the content of a packet—such as hash failure, parsing error, or encryption failure—received in Phase 1 or the negotiation of Phase 2, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Sent Packets Dropped

The cumulative total of packets that were dropped during send processing by all currently and previously active IKE tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Received Notices

The cumulative total of notify packets received by all currently and previously active IKE tunnels. A notify packet is an informational packet that is sent in response to a bad packet or to indicate status; e.g., error packets, keepalive packets, etc.

Sent Notices

The cumulative total of notify packets sent by all currently and previously active IKE tunnels. See comments for **Received Notices** above.

Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges received by all currently and previously active IKE tunnels; i.e., the total of Phase-2 negotiations received that were initiated by a remote peer. A complete exchange consists of three packets.

Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were sent by all currently and previously active and IKE tunnels; i.e., the total of Phase-2 negotiations initiated by this VPN 3002.

Invalid Phase-2 Exchanges Received

The cumulative total of IPSec Phase-2 exchanges that were received, found to be invalid because of protocol errors, and dropped, by all currently and previously active IKE tunnels. In other words, the total of Phase-2 negotiations that were initiated by a remote peer but that this VPN 3002 dropped because of protocol errors.

Invalid Phase-2 Exchanges Sent

The cumulative total of IPSec Phase-2 exchanges that were sent and were found to be invalid, by all currently and previously active IKE tunnels.

Rejected Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by a remote peer, received, and rejected by all currently and previously active IKE tunnels. Rejected exchanges indicate policy-related failures, such as configuration problems.

Rejected Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by this VPN 3002, sent, and rejected, by all currently and previously active IKE tunnels. See comment above.

Phase-2 SA Delete Requests Received

The cumulative total of requests to delete IPSec Phase-2 Security Associations received by all currently and previously active IKE tunnels.

Phase-2 SA Delete Requests Sent

The cumulative total of requests to delete IPSec Phase-2 Security Associations sent by all currently and previously active IKE tunnels.

Initiated Tunnels

The cumulative total of IKE tunnels that this VPN 3002 initiated.

Failed Initiated Tunnels

The cumulative total of IKE tunnels that this VPN 3002 initiated and that failed to activate.

Failed Remote Tunnels

The cumulative total of IKE tunnels that remote peers initiated and that failed to activate.

Authentication Failures

The cumulative total of authentication attempts that failed, by all currently and previously active IKE tunnels. Authentication failures indicate problems with preshared keys, digital certificates, or user-level authentication.

Decryption Failures

The cumulative total of decryptions that failed, by all currently and previously active IKE tunnels.

Hash Validation Failures

The cumulative total of hash validations that failed, by all currently and previously active IKE tunnels. Hash validation failures usually indicate misconfiguration or mismatched preshared keys or digital certificates.

System Capability Failures

The cumulative total of system capacity failures that occurred during processing of all currently and previously active IKE tunnels. These failures indicate that the system has run out of memory, or that the tunnel count exceeds the system maximum.

No-SA Failures

The cumulative total of nonexistent-Security Association failures that occurred during processing of all currently and previously active IKE tunnels. These failures occur when the system receives a packet for which it has no Security Association, and may indicate synchronization problems.

IPSec (Phase 2) Statistics

This table provides IPSec Phase 2 global statistics. During IPSec Phase 2, the two peers negotiate Security Associations that govern traffic within the tunnel.

Active Tunnels

The number of currently active IPSec Phase-2 tunnels.

Total Tunnels

The cumulative total of all currently and previously active IPSec Phase-2 tunnels.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IPSec Phase-2 tunnels, before decompression. In other words, total bytes of IPSec-only data received by the IPSec subsystem, before decompressing the IPSec payload.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IPSec Phase-2 tunnels, after compression. In other words, total bytes of IPSec-only data sent by the IPSec subsystem, after compressing the IPSec payload.

Received Packets

The cumulative total of packets received by all currently and previously active IPSec Phase-2 tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IPSec Phase-2 tunnels.

Received Packets Dropped

The cumulative total of packets dropped during receive processing by all currently and previously active IPSec Phase-2 tunnels, excluding packets dropped due to anti-replay processing. If there is a problem with the content of a packet, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Received Packets Dropped (Anti-Replay)

The cumulative total of packets dropped during receive processing due to anti-replay errors, by all currently and previously active IPSec Phase-2 tunnels. If the sequence number of a packet is a duplicate or out of bounds, there may be a faulty network or a security breach, and the system drops the packet.

Sent Packets Dropped

The cumulative total of packets dropped during send processing by all currently and previously active IPSec Phase-2 tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Inbound Authentications

The cumulative total number of inbound individual packet authentications performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Inbound Authentications

The cumulative total of inbound packet authentications that failed, by all currently and previously active IPSec Phase-2 tunnels. Failed authentications could indicate corrupted packets or a potential security attack (“man in the middle”).

Outbound Authentications

The cumulative total of outbound individual packet authentications performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Outbound Authentications

The cumulative total of outbound packet authentications that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPsec subsystem problem.

Decryptions

The cumulative total of inbound decryptions performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Decryptions

The cumulative total of inbound decryptions that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check for misconfiguration.

Encryptions

The cumulative total of outbound encryptions performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Encryptions

The cumulative total of outbound encryptions that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPsec subsystem problem.

System Capability Failures

The total number of system capacity failures that occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures indicate that the system has run out of memory or some other critical resource; check the event log.

No-SA Failures

The cumulative total of nonexistent-Security Association failures which occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures occur when the system receives an IPsec packet for which it has no Security Association, and may indicate synchronization problems.

Protocol Use Failures

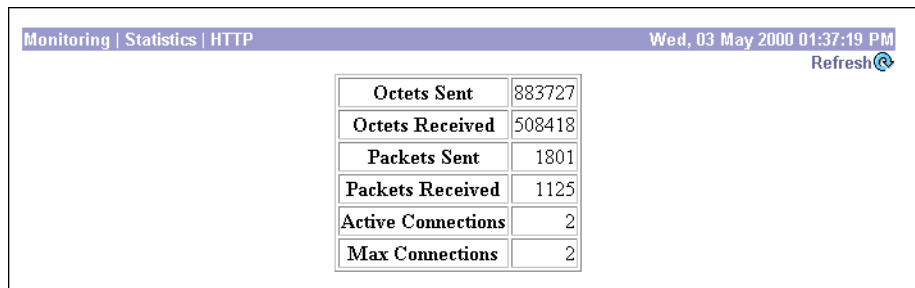
The cumulative total of protocol use failures that occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures indicate errors parsing IPsec packets.

Monitoring | Statistics | HTTP

This screen shows statistics for HTTP activity on the VPN 3002 since it was last booted or reset.

To configure system-wide HTTP server parameters, see the **Configuration | System | Management | Protocols | HTTP** screen.

Figure 13-9: Monitoring | Statistics | HTTP screen



The screenshot shows a web interface with a purple header bar containing the text "Monitoring | Statistics | HTTP" on the left and "Wed, 03 May 2000 01:37:19 PM" and a "Refresh" button on the right. Below the header is a table with the following data:

Octets Sent	883727
Octets Received	508418
Packets Sent	1801
Packets Received	1125
Active Connections	2
Max Connections	2

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Octets Sent

The total number of HTTP octets (bytes) sent since the VPN 3002 was last booted or reset.

Octets Received

The total number of HTTP octets (bytes) received since the VPN 3002 was last booted or reset.

Packets Sent

The total number of HTTP packets sent since the VPN 3002 was last booted or reset.

Packets Received

The total number of HTTP packets received since the VPN 3002 was last booted or reset.

Active Connections

The number of currently active HTTP connections.

Max Connections

The maximum number of HTTP connections that have been simultaneously active on the VPN 3002 since it was last booted or reset.

Monitoring | Statistics | Telnet

This screen shows statistics for Telnet activity on the VPN 3002 since it was last booted or reset, and for current Telnet sessions.

To configure the VPN 3002's Telnet server, see the **Configuration | System | Management Protocols | Telnet** screen.

Figure 13-10: Monitoring | Statistics | Telnet screen

The screenshot shows a web interface with a header bar containing 'Monitoring | Statistics | Telnet' on the left, 'Wed, 03 May 2000 01:39:00 PM' on the right, and a 'Refresh' button with a circular arrow icon. Below the header, there are three summary statistics:

Active Sessions	1
Attempted Sessions	1
Successful Sessions	1

Below these statistics is a table titled 'Telnet Sessions' with the following structure:

Client IP Address:Port	Inbound Octets			Outbound Octets	
	Total	Command	Discarded	Total	Dropped
100.200.147.1:1324	29	6	0	1218	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of active Telnet sessions. The **Telnet Sessions** table shows statistics for these sessions.

Attempted Sessions

The total number of attempts to establish Telnet sessions on the VPN 3002 since it was last booted or reset.

Successful Sessions

The total number of Telnet sessions successfully established on the VPN 3002 since it was last booted or reset.

Telnet Sessions

This table shows statistics for active Telnet sessions on the VPN 3002. Each active session is a row.

Client IP Address:Port

The IP address and TCP source port number of this session's remote Telnet client.

Inbound Octets Total

The total number of Telnet octets (bytes) received by this session.

Inbound Octets Command

The number of octets (bytes) containing Telnet commands or options, received by this session.

Inbound Octets Discarded

The number of Telnet octets (bytes) received and dropped during input processing by this session.

Outbound Octets Total

The total number of Telnet octets (bytes) transmitted by this session.

Outbound Octets Dropped


The number of outbound Telnet octets dropped during output processing by this session.

Monitoring | Statistics | DNS

This screen shows statistics for DNS (Domain Name System) activity on the VPN 3002 since it was last booted or reset.

To configure the VPN 3002 to communicate with DNS servers, see the **Configuration | System | Servers | DNS** screen.

Figure 13-11: Monitoring | Statistics | DNS screen

Monitoring Statistics DNS		Mon, 19 Jun 2000 01:39:17 PM
		Refresh 
Requests	18	
Responses	18	
Timeouts	0	
Server Unreachable	0	
Other Failures	0	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests

The total number of DNS queries the VPN 3002 made since it was last booted or reset. This number equals the sum of the numbers in the four cells below.

Responses

The number of DNS queries that were successfully resolved.

Timeouts

The number of DNS queries that failed because there was no response from the server.

Server Unreachable

The number of DNS queries that failed because the address of the server is not reachable according to the VPN 3002's routing table.

Other Failures

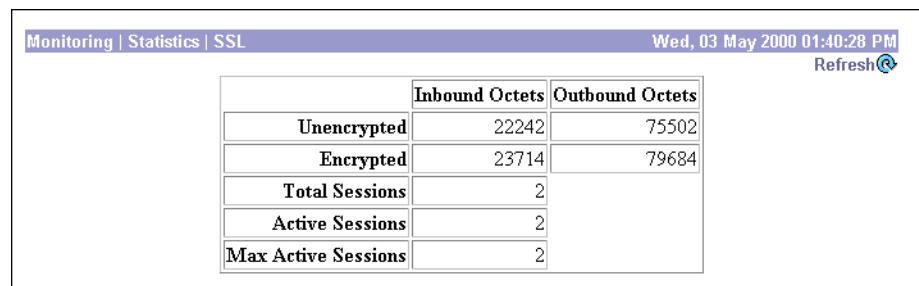
The number of DNS queries that failed for an unspecified reason.

Monitoring | Statistics | SSL

This screen shows statistics for SSL (Secure Sockets Layer) protocol traffic on the VPN 3002 since it was last booted or reset.

To configure SSL, see **Configuration | System | Management Protocols | SSL**.

Figure 13-12: Monitoring | Statistics | SSL screen



The screenshot shows a web interface for monitoring SSL statistics. At the top, there is a header bar with the text "Monitoring | Statistics | SSL" on the left and "Wed, 03 May 2000 01:40:28 PM" on the right. Below the header bar is a table with the following data:

	Inbound Octets	Outbound Octets
Unencrypted	22242	75502
Encrypted	23714	79684
Total Sessions	2	
Active Sessions	2	
Max Active Sessions	2	

On the right side of the table, there is a "Refresh" button with a circular arrow icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Unencrypted Inbound Octets

The number of octets (bytes) of inbound traffic output by the decryption engine.

Encrypted Inbound Octets

The number of octets (bytes) of encrypted inbound traffic sent to the decryption engine. This number includes negotiation traffic.

Unencrypted Outbound Octets

The number of unencrypted outbound octets (bytes) sent to the encryption engine.

Encrypted Outbound Octets

The number of octets (bytes) of outbound traffic output by the encryption engine. This number includes negotiation traffic.

Total Sessions

The total number of SSL sessions.

Active Sessions

The number of currently active SSL sessions.

Max Active Sessions


The maximum number of SSL sessions simultaneously active at any one time.

Monitoring | Statistics | DHCP

This screen shows statistics for DHCP (Dynamic Host Configuration Protocol) server activity on the VPN 3002 since it was last booted or reset. Each row of the table shows data for each IP address handed out to a DHCP client (PC) on the VPN 3002 private network.

To configure the DHCP server, see [Configuration | System | IP Routing | DHCP](#).

Figure 13-13: Monitoring | Statistics | DHCP screen

Monitoring Statistics DHCP					Thu, 15 Jun 2000 05:26:02 PM
					Refresh 
Leased IP Address	Lease Duration	Time Used	Time Left	DHCP Server Address	
100.175.0.2	2:00:00	0:05:21	1:54:39	100.199.7.7	
100.175.0.3	2:00:00	0:05:05	1:54:55	100.199.7.7	
100.175.0.6	2:00:00	0:04:58	1:55:02	100.199.7.7	
100.175.0.7	2:00:00	0:04:46	1:55:14	100.199.7.7	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Leased IP Address

The IP address leased from the DHCP server by the remote client.

Lease Duration

The length of the current IP lease period, shown as HH:MM:SS.

Time Used

The time used on the current IP address lease, shown as HH:MM:SS.

Time Left

The time remaining until the current IP address lease expires, shown as HH:MM:SS.

DHCP Server Address

The IP address of the DHCP server that supplied the leased IP address to the remote client.

Monitoring | Statistics | SSH

This screen shows statistics for SSH (Secure Shell) protocol traffic on the VPN 3002 since it was last booted or reset.

To configure SSH, see [Configuration | System | Management Protocols | SSH](#).

Figure 13-14: Monitoring | Statistics | SSH screen

The screenshot shows a web interface with a purple header bar containing the text 'Monitoring | Statistics | SSH' on the left and 'Wednesday, 02 August 2000 15:34:57' on the right. Below the header is a table with the following data:

Octets Sent	12092
Octets Received	1540
Packets Sent	307
Packets Received	53
Total Sessions	4
Active Sessions	0
Max Sessions	1

To the right of the table is a 'Refresh' button with a circular arrow icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Octets Sent / Received

The total number of SSH octets (bytes) sent / received since the VPN 3002 was last booted or reset.

Packets Sent / Received

The total number of SSH packets sent / received since the VPN 3002 was last booted or reset.

Total Sessions

The total number of SSH sessions since the VPN 3002 was last booted or reset.

Active Sessions

The number of currently active SSH sessions.

Max Sessions

The maximum number of simultaneously active SSH sessions on the VPN 3002.

Monitoring | Statistics | MIB-II

This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN 3002. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN 3002 to gather the data.

Each subsequent screen displays the data for a standard MIB-II group of objects:

- **Interfaces:** packets sent and received on network interfaces and VPN tunnels.
- **TCP/UDP:** Transmission Control Protocol and User Datagram Protocol segments and datagrams sent and received, etc.
- **IP:** Internet Protocol packets sent and received, fragmentation and reassembly data, etc.
- **ICMP:** Internet Control Message Protocol ping, timestamp, and address mask requests and replies, etc.
- **ARP Table:** Address Resolution Protocol physical (MAC) addresses, IP addresses, and mapping types.
- **Ethernet:** errors and collisions, MAC errors, etc.
- **SNMP:** Simple Network Management Protocol requests, bad community strings, parsing errors, etc.

To configure and enable the VPN 3002's SNMP server, see the **Configuration | System | Management Protocols | SNMP** screen.

Figure 13-15: Monitoring | Statistics | MIB-II screen

Monitoring | Statistics | MIB-II

This section shows statistics recorded in standard MIB-II objects.

In the left frame, or in the list of links below, click the MIB-II statistics you want to view:

- [Interfaces](#) -- packets in and out on Ethernet interfaces, and VPN tunnels.
- [TCP/UDP](#) -- segments and datagrams received and transmitted, timeouts, resets, etc.
- [IP](#) -- packets received and transmitted, fragmentation data, etc.
- [ICMP](#) -- received and transmitted PINGs, timestamps, mask requests, etc.
- [ARP Table](#) -- physical addresses, IP addresses, and mapping type.
- [Ethernet](#) -- transmit errors, collisions, etc.
- [SNMP](#) -- in packets, bad community strings, parse errors, etc.

Monitoring | Statistics | MIB-II | Interfaces

This screen shows statistics in MIB-II objects for VPN 3002 interfaces since the system was last booted or reset.

Figure 13-16: Monitoring | Statistics | MIB-II | Interfaces screen

Monitoring | Statistics | MIB-II | Interfaces Friday, 26 January 2001 13:57:13
Refresh

Interface	Status	Unicast		Multicast		Broadcast	
		In	Out	In	Out	In	Out
Private Interface	UP	0	0	0	0	0	1
Public Interface	UP	3267	3652	0	0	0	8

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN 3002 interface:

```
Private
Public
```

Status

The operational status of this interface:

UP = configured and enabled, ready to pass data traffic.

DOWN = configured but disabled.

Testing = in test mode; no regular data traffic can pass.

Dormant = configured and enabled but waiting for an external action, such as an incoming connection.

Not Present = missing hardware components.

Lower Layer Down = not operational because a lower-layer interface is down.

Unknown = not configured.

Unicast In

The number of unicast packets that were received by this interface. Unicast packets are those addressed to a single host.

Unicast Out

The number of unicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Multicast In

The number of multicast packets that were received by this interface. Multicast packets are those addressed to a specific group of hosts.

Multicast Out

The number of multicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Broadcast In

The number of broadcast packets that were received by this interface. Broadcast packets are those addressed to all hosts on a network.

Broadcast Out

The number of broadcast packets that were routed to this interface for transmission, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitoring | Statistics | MIB-II | TCP/UDP

This screen shows statistics in MIB-II objects for TCP and UDP traffic on the VPN 3002 since it was last booted or reset. RFC 2012 defines TCP MIB objects, and RFC 2013 defines UDP MIB objects.

Figure 13-17: Monitoring | Statistics | MIB-II | TCP/UDP screen

The screenshot shows a web interface with a title bar containing 'Monitoring | Statistics | MIB-II | TCP/UDP', the date and time 'Wed, 03 May 2000 01:41:10 PM', and a 'Refresh' button. Below the title bar is a table with two main sections: TCP and UDP. The TCP section includes Segments Received (3023), Segments Transmitted (3101), Segments Retransmitted (1), Timeout Min (1000 msec), Timeout Max (32000 msec), Connection Limit (-1), Active Opens (0), Passive Opens (26), Attempt Failures (0), Established Resets (21), and Current Established (2). The UDP section includes Datagrams Received (5424), Datagrams Transmitted (0), Errored Datagrams (0), and No Port (2466).

TCP		UDP	
Segments Received	3023	Datagrams Received	5424
Segments Transmitted	3101	Datagrams Transmitted	0
Segments Retransmitted	1	Errored Datagrams	0
Timeout Min	1000 msec	No Port	2466
Timeout Max	32000 msec		
Connection Limit	-1		
Active Opens	0		
Passive Opens	26		
Attempt Failures	0		
Established Resets	21		
Current Established	2		

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

TCP Segments Received

The total number of segments received, including those received in error and those received on currently established connections. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Transmitted

The total number of segments sent, including those on currently established connections but excluding those containing only retransmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Retransmitted

The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Timeout Min

The minimum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Timeout Max

The maximum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Connection Limit

The limit on the total number of TCP connections that the system can support. A value of -1 means there is no limit.

TCP Active Opens

The number of TCP connections that went directly from an unconnected state to a connection-synchronizing state, bypassing the listening state. These connections are allowed, but they are usually in the minority.

TCP Passive Opens

The number of TCP connections that went from a listening state to a connection-synchronizing state. These connections are usually in the majority.

TCP Attempt Failures

The number of TCP connection attempts that failed. Technically this is the number of TCP connections that went to an unconnected state, plus the number that went to a listening state, from a connection-synchronizing state.

TCP Established Resets

The number of established TCP connections that abruptly closed, bypassing graceful termination.

TCP Current Established

The number of TCP connections that are currently established or are gracefully terminating.

UDP Datagrams Received

The total number of UDP datagrams received. Datagram is the official UDP name for what is casually called a data packet.

UDP Datagrams Transmitted

The total number of UDP datagrams sent. Datagram is the official UDP name for what is casually called a data packet.

UDP Errored Datagrams

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port (**UDP No Port**). Datagram is the official UDP name for what is casually called a data packet.

UDP No Port

The total number of received UDP datagrams that could not be delivered because there was no application at the destination port. Datagram is the official UDP name for what is casually called a data packet.

Monitoring | Statistics | MIB-II | IP

This screen shows statistics in MIB-II objects for IP traffic on the VPN 3002 since it was last booted or reset. RFC 2011 defines IP MIB objects.

Figure 13-18: Monitoring | Statistics | MIB-II | IP screen

The screenshot shows a web interface with a header bar containing the navigation path "Monitoring | Statistics | MIB-II | IP" on the left, the date and time "Thu, 15 Jun 2000 04:19:38 PM" on the right, and a "Refresh" button with a circular arrow icon. Below the header is a table with 17 rows of statistics. Each row has a label in the first column and a numerical value in the second column.

Packets Received (Total)	2703
Packets Received (Header Errors)	0
Packets Received (Address Errors)	0
Packets Received (Unknown Protocols)	0
Packets Received (Discarded)	0
Packets Received (Delivered)	2414
Packets Forwarded	225
Outbound Packets Discarded	0
Outbound Packets with No Route	0
Packets Transmitted (Requests)	1988
Fragments Needing Reassembly	0
Reassembly Successes	0
Reassembly Failures	0
Fragmentation Successes	0
Fragmentation Failures	0
Fragments Created	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets Received (Total)

The total number of IP data packets received by the VPN 3002, including those received with errors.

Packets Received (Header Errors)

The number of IP data packets received and discarded due to errors in IP headers, including bad checksums, version number mismatches, other format errors, etc.

Packets Received (Address Errors)

The number of IP data packets received and discarded because the IP address in the destination field was not a valid address for the VPN 3002. This count includes invalid addresses (e.g., 0 . 0 . 0 . 0) and addresses of unsupported classes (e.g., Class E).

Packets Received (Unknown Protocols)

The number of IP data packets received and discarded because of an unknown or unsupported protocol.

Packets Received (Discarded)

The number of IP data packets received that had no problems preventing continued processing, but that were discarded (e.g., for lack of buffer space). This number does not include any packets discarded while awaiting reassembly.

Packets Received (Delivered)

The number of IP data packets received and successfully delivered to IP user protocols (including ICMP) on the VPN 3002; i.e., the VPN 3002 was the final destination.

Packets Forwarded

The number of IP data packets received and forwarded to destinations other than the VPN 3002.

Outbound Packets Discarded

The number of outbound IP data packets that had no problems preventing their transmission to a destination, but that were discarded (e.g., for lack of buffer space).

Outbound Packets with No Route

The number of outbound IP data packets discarded because no route could be found to transmit them to their destination. This number includes any packets that the VPN 3002 could not route because all of its default routers are down.

Packets Transmitted (Requests)

The number of IP data packets that local IP user protocols (including ICMP) supplied to transmission requests. This number does not include any packets counted in **Packets Forwarded**.

Fragments Needing Reassembly

The number of IP fragments received by the VPN 3002 that needed to be reassembled.

Reassembly Successes

The number of IP data packets successfully reassembled.

Reassembly Failures

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). This number is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

Fragmentation Successes

The number of IP data packets that have been successfully fragmented by the VPN 3002.

Fragmentation Failures

The number of IP data packets that have been discarded because they needed to be fragmented but could not be (e.g., because the Don't Fragment flag was set).


Fragments Created

The number of IP data packet fragments that have been generated by the VPN 3002.

Monitoring | Statistics | MIB-II | ICMP

This screen shows statistics in MIB-II objects for ICMP traffic on the VPN 3002 since it was last booted or reset. RFC 2011 defines ICMP MIB objects.

Figure 13-19: Monitoring | Statistics | MIB-II | ICMP screen

Monitoring Statistics MIB-II ICMP			Thu, 15 Jun 2000 04:20:43 PM	
	Received	Transmitted	Refresh 	
Total	59	13		
Errors	0	0		
Destination Unreachable	46	0		
Time Exceeded	0	0		
Parameter Problems	0	0		
Source Quench	0	0		
Redirects	0	0		
Echo Requests (PINGs)	13	0		
Echo Replies (PINGs)	0	13		
Timestamp Requests	0	0		
Timestamp Replies	0	0		
Address Mask Requests	0	0		
Address Mask Replies	0	0		

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Received / Transmitted

The total number of ICMP messages that the VPN 3002 received / sent. This number includes messages counted as **Errors Received / Transmitted**. ICMP messages solicit and provide information about the network environment.

Errors Received / Transmitted

The number of ICMP messages that the VPN 3002 received but determined to have ICMP-specific errors (bad ICMP checksums, bad length, etc.).

The number of ICMP messages that the VPN 3002 did not send due to problems within ICMP such as a lack of buffers.

Destination Unreachable Received / Transmitted

The number of ICMP Destination Unreachable messages received / sent. Destination Unreachable messages apply to many network situations, including inability to determine a route, an unusable source route specified, and the Don't Fragment flag set for a packet that must be fragmented.

Time Exceeded Received / Transmitted

The number of ICMP Time Exceeded messages received / sent. Time Exceeded messages indicate that the lifetime of the packet has expired, or that a router cannot reassemble a packet within a time limit.

Parameter Problems Received / Transmitted

The number of ICMP Parameter Problem messages received / sent. Parameter Problem messages indicate a syntactic or semantic error in an IP header.

Source Quench Received / Transmitted

The number of ICMP Source Quench messages received / sent. Source Quench messages provide rudimentary flow control; they request a reduction in the rate of sending traffic on the network.

Redirects Received / Transmitted

The number of ICMP Redirect messages received / sent. Redirect messages advise that there is a better route to a particular destination.

Echo Requests (PINGs) Received / Transmitted

The number of ICMP Echo (request) messages received / sent. Echo messages are probably the most visible ICMP messages. They test the communication path between network entities by asking for Echo Reply response messages.

Echo Replies (PINGs) Received / Transmitted

The number of ICMP Echo Reply messages received / sent. Echo Reply messages are sent in response to Echo messages, to test the communication path between network entities.

Timestamp Requests Received / Transmitted

The number of ICMP Timestamp (request) messages received / sent. Timestamp messages measure the propagation delay between network entities by including the originating time in the message, and asking for the receipt time in a Timestamp Reply message.

Timestamp Replies Received / Transmitted

The number of ICMP Timestamp Reply messages received / sent. Timestamp Reply messages are sent in response to Timestamp messages, to measure propagation delay in the network.

Address Mask Requests Received / Transmitted

The number of ICMP Address Mask Request messages received / sent. Address Mask Request messages ask for the address (subnet) mask for the LAN to which a router connects.

Address Mask Replies Received / Transmitted

The number of ICMP Address Mask Reply messages received / sent. Address Mask Reply messages respond to Address Mask Request messages by supplying the address (subnet) mask for the LAN to which a router connects.

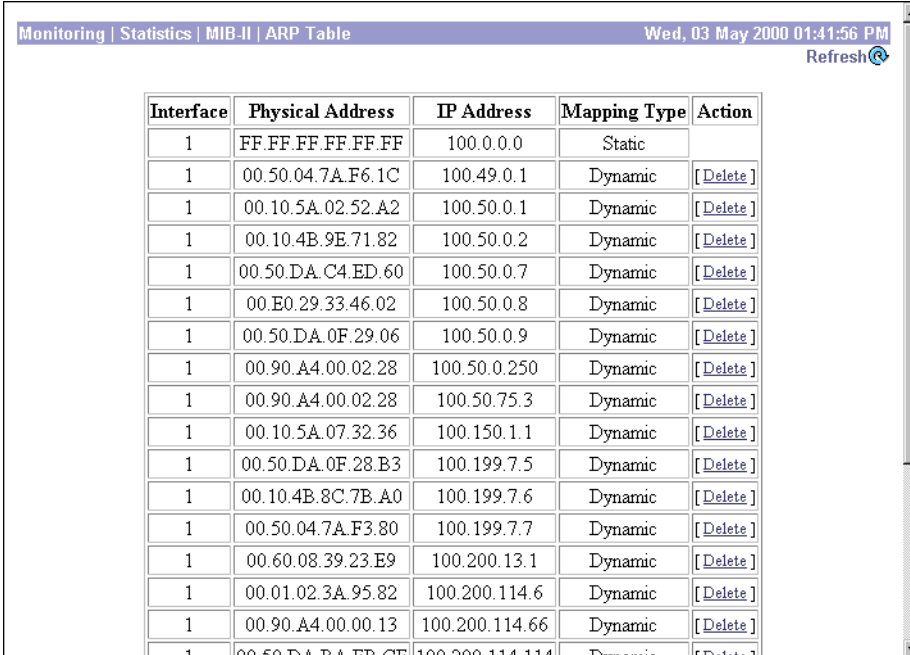
Monitoring | Statistics | MIB-II | ARP Table

This screen shows entries in the Address Resolution Protocol mapping table since the VPN 3002 was last booted or reset. ARP matches IP addresses with physical MAC addresses, so the system can forward traffic to computers on its network. RFC 2011 defines MIB entries in the ARP table.

The entries are sorted first by **Interface**, then by **IP Address**. To speed display, the Manager may construct multiple 64-row tables. Use the scroll controls (if present) to view the entire series of tables.

You can also delete dynamic, or learned, entries in the mapping table.

Figure 13-20: Monitoring | Statistics | MIB-II | ARP Table screen



The screenshot shows a web browser window with the title "Monitoring | Statistics | MIB-II | ARP Table" and a timestamp "Wed, 03 May 2000 01:41:56 PM". A "Refresh" button is visible in the top right corner. The main content is a table with the following columns: Interface, Physical Address, IP Address, Mapping Type, and Action. The table contains 16 rows of data, with the first row having a blank Action column and the others having a "[Delete]" link.

Interface	Physical Address	IP Address	Mapping Type	Action
1	FF.FF.FF.FF.FF.FF	100.0.0.0	Static	
1	00.50.04.7A.F6.1C	100.49.0.1	Dynamic	[Delete]
1	00.10.5A.02.52.A2	100.50.0.1	Dynamic	[Delete]
1	00.10.4B.9E.71.82	100.50.0.2	Dynamic	[Delete]
1	00.50.DA.C4.ED.60	100.50.0.7	Dynamic	[Delete]
1	00.E0.29.33.46.02	100.50.0.8	Dynamic	[Delete]
1	00.50.DA.0F.29.06	100.50.0.9	Dynamic	[Delete]
1	00.90.A4.00.02.28	100.50.0.250	Dynamic	[Delete]
1	00.90.A4.00.02.28	100.50.75.3	Dynamic	[Delete]
1	00.10.5A.07.32.36	100.150.1.1	Dynamic	[Delete]
1	00.50.DA.0F.28.B3	100.199.7.5	Dynamic	[Delete]
1	00.10.4B.8C.7B.A0	100.199.7.6	Dynamic	[Delete]
1	00.50.04.7A.F3.80	100.199.7.7	Dynamic	[Delete]
1	00.60.08.39.23.E9	100.200.13.1	Dynamic	[Delete]
1	00.01.02.3A.95.82	100.200.114.6	Dynamic	[Delete]
1	00.90.A4.00.00.13	100.200.114.66	Dynamic	[Delete]
1	00.50.DA.BA.FB.CF	100.200.114.114	Dynamic	[Delete]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN 3002 network interface on which this mapping applies:

Private Interface.

Public Interface.

Physical Address

The hardwired MAC (Medium Access Control) address of a physical network interface card, in 6-byte hexadecimal notation, that maps to the **IP Address**. Exceptions are:

00 = a virtual address for a tunnel.

FF.FF.FF.FF.FF.FF = a network broadcast address.

IP Address

The IP address that maps to the **Physical Address**.

Mapping Type

The type of mapping:

Other = none of the following.

Invalid = an invalid mapping.

Dynamic = a learned mapping.

Static = a static mapping on the VPN 3002.

Action / Delete

To remove a dynamic, or learned, mapping from the table, click **Delete**. *There is no confirmation or undo.* The Manager deletes the entry and refreshes the screen.

To delete an entry, you must have the administrator privilege to **Modify Config** under **General Access Rights**. See **Administration | Access Rights | Administrators**.


You cannot delete static mappings.

Monitoring | Statistics | MIB-II | Ethernet

This screen shows statistics in MIB-II objects for Ethernet interface traffic on the VPN 3002 since it was last booted or reset. IEEE standard 802.3 describes Ethernet networks, and RFC 1650 defines Ethernet interface MIB objects.

To configure Ethernet interfaces, see [Configuration | Interfaces](#).

Figure 13-21: Monitoring | Statistics | MIB-II | Ethernet screen

Monitoring Statistics MIB-II Ethernet														Mon, 22 May 2000 04:34:48 PM	
														Refresh 	
Interface	Errors					Deferred Transmits	Collisions				MAC Errors		Speed (Mbps)	Duplex	
	Alignment	FCS	Carrier Sense	SQE Test	Frame Too Long		Single	Multiple	Late	Excessive	Transmit	Receive			
Ethernet 1 (Private)	0	0	0	0	0	0	0	0	0	0	0	0	100	Half	
Ethernet 2 (Public)	0	0	0	0	0	0	0	0	0	0	0	0	0	Half	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The Private or Public interface to which the data in this row applies.

Alignment Errors

The number of frames received on this interface that are not an integral number of bytes long and do not pass the FCS (Frame Check Sequence; used for error detection) check.

FCS Errors

The number of frames received on this interface that are an integral number of bytes long but do not pass the FCS (Frame Check Sequence) check.

Carrier Sense Errors

The number of times that the carrier sense signal was lost or missing when trying to transmit a frame on this interface.

SQE Test Errors

The number of times that the SQE (Signal Quality Error) Test Error message was generated for this interface. The SQE message tests the collision circuits on an interface.

Frame Too Long Errors

The number of frames received on this interface that exceed the maximum permitted frame size.

Deferred Transmits

The number of frames for which the first transmission attempt on this interface is delayed because the medium is busy. This number does not include frames involved in collisions.

Single Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by exactly one collision. This number is not included in the **Multiple Collisions** number.

Multiple Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by more than one collision. This number does not include the **Single Collisions** number.

Late Collisions

The number of times that a collision is detected on this interface later than 512 bit-times into the transmission of a packet. 512 bit-times = 51.2 microseconds on a 10-Mbps system.

Excessive Collisions

The number of frames for which transmission on this interface failed due to excessive collisions.

MAC Errors: Transmit

The number of frames for which transmission on this interface failed due to an internal MAC sublayer transmit error. This number does not include **Carrier Sense Errors**, **Late Collisions**, or **Excessive Collisions**.

MAC Errors: Receive

The number of frames for which reception on this interface failed due to an internal MAC sublayer receive error. This number does not include **Alignment Errors**, **FCS Errors**, or **Frame Too Long Errors**.

Speed (Mbps)

This interface's nominal bandwidth in megabits per second.

Duplex

The current LAN duplex transmission mode for this interface:

`Full` = Full-Duplex: transmission in both directions at the same time.

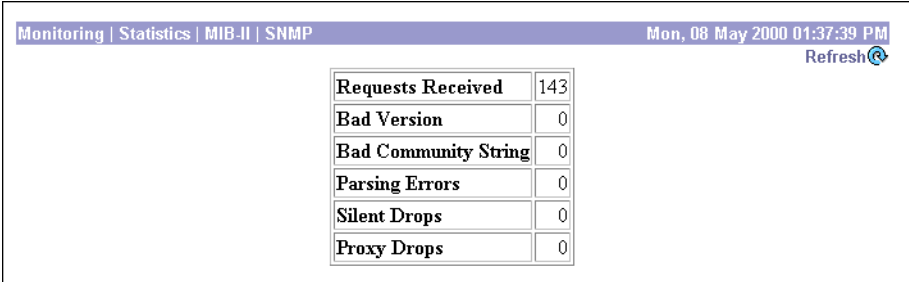
`Half` = Half-Duplex: transmission in only one direction at a time.

Monitoring | Statistics | MIB-II | SNMP

This screen shows statistics in MIB-II objects for SNMP traffic on the VPN 3002 since it was last booted or reset. RFC 1907 defines SNMP version 2 MIB objects.

To configure the VPN 3002 SNMP server, see [Configuration | System | Management Protocols | SNMP](#).

Figure 13-22: Monitoring | Statistics | MIB-II | SNMP screen



The screenshot shows a web interface with a purple header bar containing the navigation path "Monitoring | Statistics | MIB-II | SNMP" on the left, the date and time "Mon, 08 May 2000 01:37:39 PM" on the right, and a "Refresh" button with a circular arrow icon. Below the header is a table with the following data:

Requests Received	143
Bad Version	0
Bad Community String	0
Parsing Errors	0
Silent Drops	0
Proxy Drops	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests Received

The total number of SNMP messages received by the VPN 3002.

Bad Version

The total number of SNMP messages received that were for an unsupported SNMP version. The VPN 3002 supports SNMP version 2.

Bad Community String

The total number of SNMP messages received that used an SNMP community string the VPN 3002 did not recognize. See **Configuration | System | Management Protocols | SNMP Communities** to configure permitted community strings. To protect security, the VPN 3002 *does not* include the usual default `public` community string.

Parsing Errors

The total number of syntax or transmission errors encountered by the VPN 3002 when decoding received SNMP messages.

Silent Drops

The total number of SNMP request messages that were silently dropped because the reply exceeded the maximum allowable message size.

Proxy Drops

The total number of SNMP request messages that were silently dropped because the transmission of the reply message to a proxy target failed for some reason (other than a timeout).

C



Using the Command Line Interface

The VPN 3002 Hardware Client Command Line Interface (CLI) is a menu- and command-line-based configuration, administration, and monitoring system built into the VPN 3002. You use it via the system console or a Telnet (or Telnet over SSL) session.

You can use the CLI to completely manage the system. You can access and configure the same parameters as the HTML-based VPN 3002 Hardware Client Manager.

This chapter describes general features of the CLI and how to access and use it. It *does not* describe the individual menu items and parameter entries. For information on specific parameters and options, see the corresponding section of the Manager in this manual. For example, to understand Ethernet interface configuration parameters and choices, see **Configuration | Interfaces | Private/Public** in Chapter 3, *Interfaces*.

Accessing the CLI

You can access the CLI in two ways: via the system console or a Telnet (or Telnet over SSL) client.

Console access

To access the CLI via console:

- 1 Connect a PC to the VPN 3002 via an RJ-45 serial cable (which Cisco supplies with the system) between the **Console** port on the VPN 3002 and the COM1 or serial port on the PC. For more information, see the *VPN 3002 Hardware Client Getting Started* manual.
- 2 Start a terminal emulator (e.g., HyperTerminal) on the PC. Configure a connection to COM1 with port settings of:
 - 9600 bits per second.
 - 8 data bits.
 - No parity.
 - 1 stop bit.Set the emulator for VT100 emulation, or let it auto-detect the emulation type.
- 3 Press **Enter** on the PC keyboard until you see the login prompt. (You may see a password prompt and error messages as you press **Enter**; ignore them and stop at the login prompt.)

Login: _

Telnet or Telnet/SSL access

To access the CLI via a Telnet or Telnet/SSL client:

- 1 Enable the Telnet or Telnet/SSL server on the VPN 3002. (They are both enabled by default on the private network.) See the **Configuration | System | Management Protocols | Telnet** screen on the Manager.
- 2 Start the Telnet or Telnet/SSL client, and connect to the VPN 3002 using these parameters:

Host Name or **Session Name** = The IP address on the VPN 3002 Private interface; e.g., 10.10.147.2

Port = Telnet (default Telnet port is 23, Telnet/SSL port is 992)

Terminal Type = VT100 or ANSI

Telnet/SSL only: If the client offers it, enable *both* **SSL** and **SSL Only**.

- 3 The VPN 3002 displays a login prompt.

Login: _

Starting the CLI

You start the CLI by logging in.

CLI login usernames and passwords for both console and Telnet access are the same as those configured and enabled for administrators. See the **Administration | Access Rights | Administrators** screen. By default, only admin is enabled.

This example uses the factory-supplied default admin login and password. If you have changed them, use your entries.

At the prompts, enter the administrator login name and password. Entries are case-sensitive.

Login: admin

Password: admin (The CLI does not show your entry.)

The CLI displays the opening welcome message, the main menu, and the Main -> prompt.

```
                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 -> \_

## Using the CLI

This section explains how to:

- Choose menu items.
- Enter values for parameters and options.
- Specify configured items by number or name.
- Navigate quickly—using shortcuts—through the menus.
- Display a brief help message.
- Save entries to the system configuration file.
- Stop the CLI.
- Understand CLI administrator access rights.

The CLI displays menus or prompts at every level to guide you in choosing configurable options and setting parameters. The prompt always shows the menu context.

### Choosing menu items

To use the CLI, enter a number at the prompt that corresponds to the desired menu item, and press **Enter**.

For example, this is the **Configuration > System > General > System Identification** menu:

- 1) Set System Name
- 2) Set Contact
- 3) Set Location
- 4) Back

```
General -> _
```

Enter 1 to set the system name.

### Entering values

The CLI shows any current or default value for a parameter in brackets [ ]. To change the value, enter a new value at the prompt. To leave the value unchanged, just press **Enter**.

Continuing the example above, this is the prompt to enter a value for the system name:

```
> Host Name
```

```
General -> [Lab VPN] _
```

You can enter a new name at the prompt, or just press **Enter** to keep the current name.

## Navigating quickly through the CLI

There are two ways to move quickly through the CLI: shortcut numbers, and the Back/Home options. Both ways work only when you are at a menu, not when you are at a value entry.

### Using shortcut numbers

When you become familiar with the structure of the CLI—which parallels the HTML-based VPN 3002 Hardware Client Manager—you can quickly access any level by entering a series of numbers separated by periods. For example, suppose you want to change the Access Rights for Administrators. The series of menus that gets to that level from the main menu is:

```
Main -> _
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
Main -> 2 (Administration)
```

```
) Software Update
2) System Reboot
3) Ping
4) Access Rights
5) File Management
6) Certificate Management
7) Back
```

```
Config -> 4 (Access Rights)
```

```
1) Administrators
2) Access Settings
3) Back
```

```
Admin -> 1
```

```
Administrative Users

Username Enabled

admin Yes
config No
isp No

```

```
1) Modify Administrator
2) Back
```

```
Admin -> 1
```

---

```
> Which Administrator to Modify
```

```
Admin ->
```

As a shortcut, you can just enter 2.4.1.1 at the Main-> prompt, and move directly to the Modify Administrators menu:

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

```
Main -> 2.4.1.1
```

```
> Which Administrator to Modify
```

```
Admin ->
```

---

**Note:** At this last prompt, you cannot use a number shortcut. At this prompt, you must type in the name of the administrator you want to modify, for example, `config`.

```
Admin -> config
```

The prompt always shows the current context in the menu structure.

## Using Back and Home

Most menus include a numbered Back choice. Instead of entering a number, you can just enter `b` or `B` to move back to the previous menu.

Also, at any menu level, you can just enter `h` or `H` to move home to the main menu.

### Getting Help Information

To display a brief help message, enter 5 at the main menu prompt. The CLI explains how to navigate through menus and enter values. This help message is available only at the main menu.

```
Cisco Systems. Help information for the Command Line Interface
```

```
From any menu except the Main menu.
```

```
-- 'B' or 'b' for Back to previous menu.
```

```
-- 'H' or 'h' for Home back to the main menu.
```

```
For Data entry
```

```
-- Current values are in '[']'s. Just hit 'Enter' to accept value.
```

```
1) View Help Again
```

```
2) Back
```

```
Help -> _
```

To return to the main menu from this help menu, enter h (for home), or 2 or b (for back) at the prompt.

### Saving the configuration file

Configuration and administration entries take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN 3002 without *saving* the active configuration, you lose any changes.

To save changes to the system configuration (CONFIG) file, navigate to the main menu. At the prompt, enter 4 for Save changes to Config file.

```
1) Configuration
```

```
2) Administration
```

```
3) Monitoring
```

```
4) Save changes to Config file
```

```
5) Help Information
```

```
6) Exit
```

```
Main -> 4
```

The system writes the active configuration to the CONFIG file and redisplay the main menu.



## Stopping the CLI

To stop the CLI, navigate to the main menu and enter 6 for Exit at the prompt:

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

```
Main -> 6
```

```
Done
```

Make sure you save any configuration changes before you exit from the CLI.

## Understanding CLI access rights

What you see and can configure with the CLI depends on administrator access rights. If you don't have permission to configure an option, you see -), rather than a number, in menus.

For example, here is the main menu for the default Monitor administrator:

- ) Configuration
- ) Administration
- 3) Monitoring
- ) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> _
```

The default Monitor administrator can only monitor the VPN 3002, not configure system parameters or administer the system.

See **Administration | Access Rights | Administrators** in Chapter 12, *Administration*, for more information.

## CLI menu reference

This section shows all the menus in the first three levels below the CLI main menu. (There are many additional menus below the third level; and within the first three levels, there are some non-menu parameter settings. To keep this chapter at a reasonable size, we show only the *menus* here.)

The numbers in each heading are the keyboard shortcut to reach that menu from the main menu. For example, entering 1.3.1 at the main menu prompt takes you to the **Configuration > System Management > IP Routing** menu.

---

**Notes:** The CLI menus and options—and thus the keyboard shortcuts—may change with new software versions. Please check familiar shortcuts carefully when using a new release.

---

### Main menu

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

Main -> \_

### 1 Configuration

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

Config -> \_

#### 1.1 Configuration > Quick Configuration

See the *VPN 3002 Hardware Client Getting Started* guide for complete information about Quick Config.

#### 1.2 Configuration > Interface Configuration

This table shows current IP addresses.

.  
.

- 1) Configure the Private Interface
- 2) Configure the Public Interface
- 3) Back

Interfaces -> \_

#### 1.2.1 or 1.2.2 Configuration > Interface Configuration > Configure the Private/Public Interface

- 1) Enable/Disable
- 2) Set IP Address
- 3) Set Subnet Mask
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Back

Private/Public Interface -> \_

## 1.2 Configuration > System Management

- 1) Servers (DNS)
- 2) Tunneling Protocols (IPSec)
- 3) IP Routing (static routes, etc.)
- 4) Management Protocols (Telnet, HTTP, etc.)
- 5) Event Configuration
- 6) General Config (system name, time, etc.)
- 7) Back

System -> \_

### 1.2.1 Configuration > System Management > Servers

- 1) DNS Servers
- 2) Back

Servers -> \_

### 1.2.2 Configuration > System Management > Tunneling Protocols

- 1) DNS Servers
- 2) Back

Tunnel -> \_

### 1.2.3 Configuration > System Management > IP Routing

- 1) Static Routes
- 2) Default Gateway
- 3) DHCP
- 4) DHCP Options
- 5) Back

Routing -> \_

### 1.2.4 Configuration > System Management > Management Protocols

- 1) Configure HTTP/HTTPS
- 2) Configure Telnet
- 3) Configure SNMP
- 4) Configure SNMP Community Strings
- 5) Configure SSL
- 6) Configure SSH
- 7) Back

Network -> \_

### 1.2.5 Configuration > System Management > Event Configuration

- 1) General
- 2) Classes
- 3) Trap Destinations
- 4) Syslog Servers
- 5) Back

Event -> \_

### 1.2.6 Configuration > System Management > General Config

- 1) System Identification
- 2) System Time and Date
- 3) Back

General -> \_

### 1.4 Configuration > Policy Management

- 1) Traffic Management
- 2) Back

Policy -> \_

### 1.4.2 Configuration > Policy Management > Traffic Management

- 1) Port Address Translation (PAT)
- 2) Back

Traffic ->

## 2 Administration

- 1) Software Update
- 2) System Reboot
- 3) Ping
- 4) Access Rights
- 5) File Management
- 6) Certificate Management
- 7) Back

Admin -> \_

### 2.1 Administration > Software Update

Name of the file for main code upgrade? [phoenix3002dc.bin]  
IP address of the host where the file resides? [10.10.66.10]

(M)odify any of the above (C)ontinue or (E)xit? [M]

## 2.2 Administration > System Reboot

- 1) Cancel Scheduled Reboot/Shutdown
- 2) Schedule Reboot
- 3) Schedule Shutdown
- 4) Back

Admin -> \_

### 2.2.2 Administration > System Reboot > Schedule Reboot

- 1) Save active Configuration and use it at Reboot
- 2) Reboot without saving active Configuration file
- 3) Reboot ignoring the Configuration file
- 4) Back

Admin -> \_

### 2.2.3 Administration > System Reboot > Schedule Shutdown

- 1) Save active configuration and use it at next reboot
- 2) Shutdown without saving active Configuration file
- 3) Shutdown, ignoring the Configuration file at next reboot
- 4) Back

Admin -> \_

## 2.3 Ping

> Ping host

Admin ->

## 2.4 Administration > Access Rights

- 1) Administrators
- 2) Access Settings
- 3) Back

Admin -> \_

### 2.4.1 Administration > Access Rights > Administrators

Admin -> 1

```
Administrative Users

Username Enabled

admin Yes
config No
isp No

```

- 1) Modify Administrator
- 2) Back

Admin ->

### 2.4.2 Administration > Access Rights > Access Settings

- 1) Set Session Timeout
- 2) Set Session Limit
- 3) Enable/Disable Encrypt Config File
- 4) Back

Admin -> \_

### 2.5 Administration > File Management

```
List of Files

CONFIG CONFIG.BAK
```

- 1) View Config File
- 2) Delete Config File
- 3) View Backup Config File
- 4) Delete Backup Config File
- 5) Swap Config Files
- 6) Upload Config File
- 7) Back

File -> \_

## 2.5.5 Administration > File Management > Swap Configuration File

```
Every time the active configuration is saved,...
.
.
.

1) Swap
2) Back

Admin -> _
```

## 2.6 Administration > Certificate Management

```
1) Enrollment
2) Installation
3) Certificate Authorities
4) Identity Certificates
5) SSL Certificate
6) Back

Certificates -> _
```

### 2.6.2 Administration > Certificate Management > Installation

```
1) Install Certificate Authority
2) Install SSL Certificate (from Enrollment)
3) Install SSL Certificate (with private key)
4) Install Identity Certificate (from Enrollment)
5) Back

Certificates -> _
```

### 2.6.3 Administration > Certificate Management > Certificate Authorities

```
Certificate Authorities
.
.
.

1) View Certificate
2) Delete Certificate
4) Back

Certificates -> _
```

### 2.6.4 Administration > Certificate Management > Identity Certificates

```
Identity Certificates
.
.
.
1) View Certificate
2) Delete Certificate
3) Back

Certificates -> _
```

### 2.6.5 Administration > Certificate Management > SSL Certificate

```
Subject
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
Issuer
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
Serial Number
.
.

1) Delete Certificate
2) Generate Certificate
3) Back

Certificates -> _
```

## 3 Monitoring

```
1) Routing Table
2) Event Log
3) System Status
4) General Statistics
5) Back

Monitor -> _
```



### 3.1 Monitoring > Routing Table

```
Routing Table
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
.
1) Refresh Routing Table
2) Clear Routing Table
3) Back

Routing -> _
```

### 3.2 Monitoring > Event Log

```
1) Configure Log viewing parameters
2) View Event Log
3) Clear Log
4) Back

Log -> _
```

#### 3.2.2 Monitoring > Event Log > View Event Log

```
[Event Log entries]
.
.
.
1) First Page
2) Previous Page
3) Next Page
4) Last Page
5) Back

Log -> _
```

### 3.3 Monitoring > System Status

```
System Status
.
.
.
1) Refresh System Status
2) Connect Now
3) Disconnect Now
4) Back

Status -> _

Card Status -> _
```

### 3.4 Monitoring > General Statistics

- 1) Protocol Statistics
- 2) Server Statistics
- 3) MIB II Statistics
- 4) Back

General -> \_

#### 3.4.1 Monitoring > General Statistics > Protocol Statistics

- 1) IPSec Statistics
- 2) HTTP Statistics
- 3) Telnet Statistics
- 4) DNS Statistics
- 5) More
- 6) Back

General -> \_

#### 3.4.2 Monitoring > General Statistics > Server Statistics

- 1) DHCP Statistics
- 2) Back

General -> \_

#### 3.4.3 Monitoring > General Statistics > MIB II Statistics

- 1) Interface-based
- 2) System-level
- 3) Back

MIB2 -> \_



## Errors and troubleshooting

---

This appendix describes files for troubleshooting the VPN 3002, LED indicators on the system, and common errors that may occur while configuring and using the system, and how to correct them.

### 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.
- 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, timers, etc., which help Cisco support engineers diagnose the problem. In case of a crash, we ask that you send this file when you contact Cisco 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 may 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 may indicate an error condition.

Contact Cisco support if any LED indicates an error condition.

### VPN 3002 LEDs (front)

The LEDs on the front of the VPN 3002 are:

| LEDs on front of unit |                |                                 |
|-----------------------|----------------|---------------------------------|
| LED                   | State          | 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.    |
|                       | green          | Unit is operational.            |
| VPN                   | off            | No VPN tunnel exists.           |
|                       | amber          | Tunnel has failed.              |
|                       | green          | Tunnel is established.          |

### VPN 3002 LEDs (rear)

The LEDs on the rear of the VPN 3002 indicate the status of the Private and Public Interfaces.

| LED Indicator (Rear) | Explanation                                |
|----------------------|--------------------------------------------|
| Green                | Interface is connected to the network.     |
| OFF                  | Interface is not connected to the network. |
| Flashing amber       | Traffic is traveling across the interface. |

## Errors on the system

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

| Problem/symptom                                                                                                                | Possible solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel is not up/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:<br>PWR = green<br>SYS LED = green<br>VPN LED = off.                                                  | <ol style="list-style-type: none"> <li>1 Verify that the VPN 3000 Series Concentrator to which this VPN 3002 connects is running version 3.0 software.</li> <li>2 Navigate to <b>Monitoring &gt; System Status</b>. Click <b>Connect Now</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Connect Now</b> didn't bring up the tunnel, and the Public interface LED (back of unit) is off.                             | <ol style="list-style-type: none"> <li>1 Check that a LAN cable is properly attached to the Public interface of the VPN 3002.</li> <li>2 Make sure the IP address for the Public interface is properly configured.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Public interface LED is on, but attempting to ping the default gateway ( <b>Administration &gt; Ping</b> ) yields no response. | <ol style="list-style-type: none"> <li>1 Make sure the default gateway is properly configured.</li> <li>2 Contact your ISP.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| VPN LED is solid amber (tunnel failed to establish to central-site Concentrator).                                              | <ol style="list-style-type: none"> <li>1 Make sure the IPsec parameters are properly configured. Verify: <ul style="list-style-type: none"> <li>– <b>Public IP Address</b> of the IKE peer (central-site Concentrator) is correct.</li> <li>– <b>Group</b> name and password are correct.</li> <li>– <b>User</b> name and password are correct.</li> </ul> </li> <li>2 Make sure the <b>Group</b> and <b>User</b> names and passwords match those set for this VPN 3002 on the central-site Concentrator.</li> <li>3 After you make any changes, navigate to <b>Monitoring &gt; System Status</b> and click <b>Connect Now</b>.</li> <li>4 Study the event log files. To capture more events, and to interpret events, see Chapter 9, <i>Events</i>, in the <i>VPN 3002 Hardware Client User Guide</i>.</li> </ol> |
| My PC can't communicate with the remote network.                                                                               | <ol style="list-style-type: none"> <li>1 Verify that the VPN 3000 Series Concentrator to which this VPN 3002 connects is running version 3.0 software.</li> <li>2 Navigate to <b>Monitoring &gt; System Status</b> and click <b>Connect Now</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| <b>Problem/symptom</b>                                                                         | <b>Possible solution</b>                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Connect Now</b> worked.                                                                     |                                                                                                                                                                                                                                                                 |
| LED(s) for the Private interface/<br>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/<br>switch port are on.                                       | <ol style="list-style-type: none"><li>1 Is this PC configured as a DHCP client? If so, verify that the DHCP server on the VPN 3002 is enabled.</li><li>2 With any method of address assignment, verify that the PC got an IP address and subnet mask.</li></ol> |
| Attempting to ping the default gateway ( <b>Administration &gt; Ping</b> ) yields no response. | <ol style="list-style-type: none"><li>1 Make sure your PC has an appropriate IP address, reachable on this network.</li><li>2 Contact your network administrator.</li></ol>                                                                                     |

## Settings on the VPN 3000 Series Concentrator

If your VPN 3002 experiences connectivity problems, check the configuration of the VPN 3000 Series Concentrator.

- 1 Configure the connection as a Client, **NOT** LAN-to-LAN.
- 2 Assign this VPN 3002 to a group. Configure **Group** and **User** names and passwords. These must match the **Group** and **User** names and passwords that you set on the VPN 3002. See Chapter 14, *User Management*, in the *VPN 3000 Concentrator Series User Guide*.
- 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. See Chapter 6, *Address Management* in the *VPN 3000 Concentrator Series User Guide*.
- 4 If you are using Network Extension mode, configure a default gateway or a static route to the Private network of the VPN 3002. See Chapter 8, *IP Routing*, in the *VPN 3000 Concentrator Series User Guide*.
- 5 Check the Event log. See Chapter 10, *Events*, in the *VPN 3000 Concentrator Series User Guide*.

## VPN 3002 Hardware Client Manager errors

These errors may occur while using the HTML-based VPN 3002 Hardware Client Manager with a browser.

### Browser Refresh / Reload button logs out the Manager

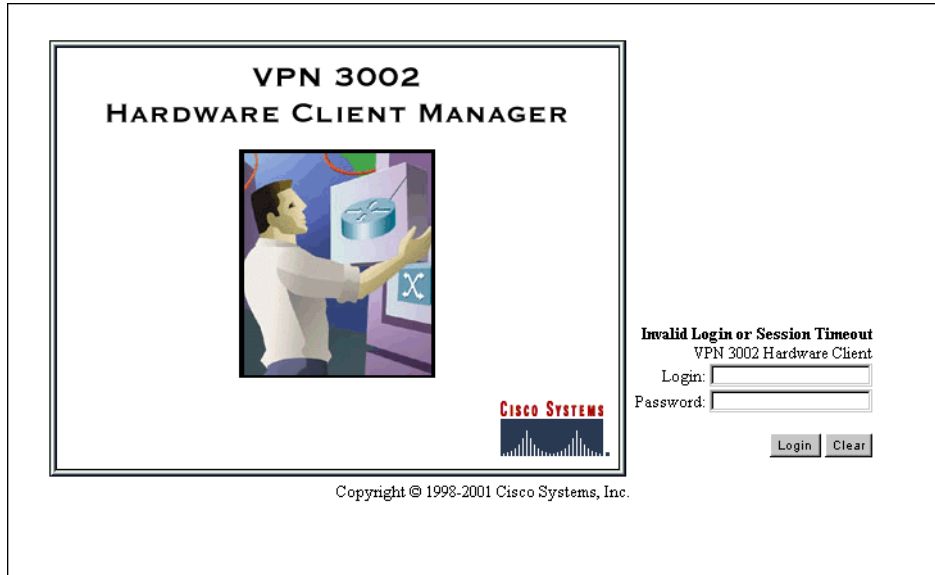
| Problem                                                                                                                                                       | Possible cause                                                                                                                    | Solution                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked the <b>Refresh</b> or <b>Reload</b> button on the <i>browser's</i> navigation toolbar, and the Manager logged out. The main login screen appears. | To protect access security, clicking <b>Refresh / Reload</b> on the browser's toolbar automatically logs out the Manager session. | Do not use the browser's navigation toolbar buttons with the VPN 3002 Hardware Client Manager.<br><br>Use only the Manager's <b>Refresh</b> button where it appears on a screen.<br><br>We recommend that you hide the browser's navigation toolbar to prevent mistakes. |

### Browser Back or Forward button displays an incorrect screen or incorrect data

| Problem                                                                                                                                                        | Possible cause                                                                                                                                                         | Solution                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked the <b>Back</b> or <b>Forward</b> button on the <i>browser's</i> navigation toolbar, and the Manager displayed the wrong screen or incorrect data. | To protect security and the integrity of data entries, clicking <b>Back</b> or <b>Forward</b> on the browser's toolbar deletes pointers and values within the Manager. | Do not use the browser's navigation toolbar buttons with the VPN 3002 Hardware Client Manager.<br><br>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.<br><br>We recommend that you hide the browser's navigation toolbar to prevent mistakes. |

## Invalid Login or Session Timeout

The Manager displays the **Invalid Login or Session Timeout** screen

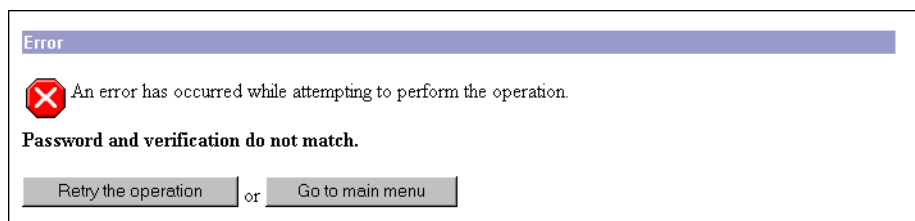


| Problem                                                                        | Possible cause                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Solution                                                                                                                                                     |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You entered an invalid administrator login name/password combination.          | <ul style="list-style-type: none"> <li>• Typing error.</li> <li>• Invalid (unrecognized) login name or password.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                               | Re-enter the login name and password, and click <b>Login</b> . Use a valid login name and password. Verify your typing before clicking <b>Login</b> .        |
| The Manager session has been idle longer than the configured timeout interval. | <ul style="list-style-type: none"> <li>• No activity for (interval) seconds. The Manager resets the inactivity timer only when you click an action button (<b>Apply</b>, <b>Add</b>, <b>Cancel</b>, etc.) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen <i>does not</i> reset the timer.</li> <li>• Default timeout interval is 600 seconds (10 minutes).</li> <li>• Timeout interval set too low for normal use.</li> </ul> | On the <b>Administration   Access Rights   Access Settings</b> screen, change the <b>Session Timeout</b> interval to a larger value and click <b>Apply</b> . |



## Error / An error has occurred while attempting to perform...

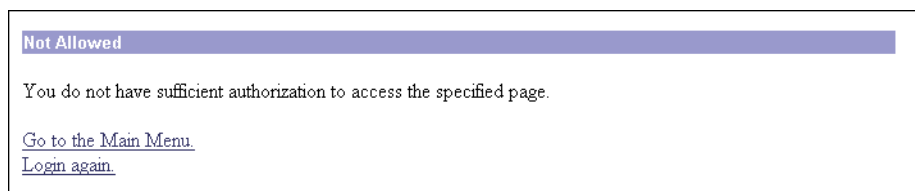
The Manager displays a screen with the message: **Error / An error has occurred while attempting to perform the operation**. An additional error message describes the erroneous operation.



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

## Not Allowed / You do not have sufficient authorization...

The Manager displays a screen with the message: **Not Allowed / You do not have sufficient authorization to access the specified page**.




| Problem                                                                                  | Possible cause                                                                                                                                                                                            | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You tried to access an area of the Manager that you do not have authorization to access. | <ul style="list-style-type: none"><li>You logged in using an administrator login name that has limited privileges.</li><li>You logged in from a workstation that has limited access privileges.</li></ul> | <p>Log in using the system administrator login name and password. (Defaults are admin / admin.)</p> <p>Log in from a workstation with greater access privileges.</p> <p>Have the system administrator change your privileges on the <b>Administration   Access Rights   Administrators</b> screen.</p> <p>Have the system administrator change the privileges of your workstation on the <b>Administration   Access Rights   Access Control List</b> screen.</p> |

## Not Found/An error has occurred while attempting to access...

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.

### Not Found



An error has occurred while attempting to access the specified page. The feature hasn't been implemented yet, or the page does not exist. If you have recently upgraded or downgraded the VPN 3000 Concentrator Series, clearing the browser's cache may solve the problem.

**Error:** HTTP 404 - Not Found  
**Request:** GET http://10.10.147.2/foobar.html  
**Referring Page:** Unknown  
**Browser:** Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)  
**JavaScript:** JavaScript 1.2  
**Software Version:** Cisco Systems, Inc./VPN 3000 Concentrator Series Version 2.5 (6898) built by tshort on Apr 14 2000 13:55:31 (DEBUG\_MASK 0, NDEBUG off)  
**Feature Set:**

[Go to the login page.](#)

| Problem                              | Possible cause                                                                                                                                                       | Solution                                                                                                                                                                                                                                       |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Manager could not find a screen. | <ul style="list-style-type: none"> <li>You updated the software image and did not clear the browser's cache.</li> <li>There is an internal Manager error.</li> </ul> | <p>Clear the browser's cache: delete its temporary internet files, history files, and location bar references. Then try again.</p> <p>Please note the system information on the screen and contact Cisco support personnel for assistance.</p> |

## 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**.

| Problem                                                                                                                                                                                                  | Possible cause                                         | Solution                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| While using a Manager function that opens another browser window (such as <b>Save Needed, Help, Software Update</b> , etc.), Internet Explorer cannot open the window and displays the error dialog box. | A bug in the Internet Explorer JavaScript interpreter. | <ol style="list-style-type: none"> <li>Click <b>No</b> on the error dialog box.</li> <li>Log out of the Manager.</li> <li>Close Internet Explorer.</li> <li>Reinstall Internet Explorer.</li> </ol> |

## Command Line Interface errors

These errors may occur while using the menu-based Command Line Interface from a console or Telnet session.

### ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID.

| Problem                                                                                       | Possible cause                                                                                                                                                                                                                                                                 | Solution                                                      |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| The system expected a valid 4-byte dotted decimal entry, and the entry wasn't in that format. | <ul style="list-style-type: none"><li>You entered something other than a 4-byte dotted decimal number. You may have omitted a byte position, or entered a number greater than 255 in a byte position.</li><li>You entered 0.0.0.0 instead of an appropriate address.</li></ul> | At the prompt, re-enter a valid 4-byte dotted decimal number. |

### ERROR:-- Out of Range value entered. Try again.

| Problem                                                                                    | Possible cause                                                                                                                                                 | Solution                                                   |
|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| The system expected a number within a certain range, and the entry was outside that range. | <ul style="list-style-type: none"><li>You entered a letter instead of a number.</li><li>You entered a number greater than the possible menu numbers.</li></ul> | At the prompt, re-enter a number in the appropriate range. |

### ERROR:-- The Passwords do not match. Please try again.

| Problem                                                                     | Possible cause                                                                                                                                   | Solution                                                                                                                                                                                |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The entry for a password and the entry to verify the password do not match. | <ul style="list-style-type: none"><li>You mistyped an entry.</li><li>You entered either a password or verify entry, but not the other.</li></ul> | At the <code>Verify</code> prompt, re-enter the password. If the original password is incorrect, press <b>Enter</b> and re-enter both the password and the verification at the prompts. |

## Copyrights, licenses, and notices

---

### Software License Agreement of Cisco Systems, Inc.

CISCO SYSTEMS, INC. IS WILLING TO LICENSE TO YOU THE SOFTWARE CONTAINED IN THE ACCOMPANYING CISCO PRODUCT ONLY IF YOU ACCEPT ALL OF THE TERMS AND CONDITIONS IN THIS LICENSE AGREEMENT. PLEASE READ THIS AGREEMENT CAREFULLY BEFORE YOU OPEN THE PACKAGE BECAUSE, BY OPENING THE SEALED PACKAGE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CISCO SYSTEMS WILL NOT LICENSE THIS SOFTWARE TO YOU. IN THAT CASE YOU SHOULD RETURN THE PRODUCT PROMPTLY, INCLUDING THE PACKAGING, THE UNOPENED PACKAGE, ALL ACCOMPANYING HARDWARE, AND ALL WRITTEN MATERIALS, TO THE PLACE OF PURCHASE FOR A FULL REFUND.

#### Ownership of the Software

1. The software contained in the accompanying Cisco product (“the Software”) and any accompanying written materials are owned or licensed by Cisco Systems and are protected by United States copyright laws, laws of other nations, and/or international treaties.

#### Grant of License

2. Cisco Systems hereby grants to you the right to use the Software with the Cisco VPN 3000 Concentrator product. To this end, the Software contains both operator software for use by the network administrator and client software for use by clients at remote network nodes. You may transfer the client software, or portions thereof, only to prospective nodes on the network, and to no one else. You may not transfer the operator software.

#### Restrictions on Use and Transfer

3. You may not otherwise copy the Software, except that you may make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single disk provided you keep the disk solely for backup or archival purposes. You may not copy the written materials and you may not use the backup or archival copy of the Software except in conjunction with the accompanying Cisco product.

4. You may permanently transfer the Software and accompanying written materials (including the most recent update and all prior versions) only in conjunction with a transfer of the entire Cisco product, and only if you retain no copies and the transferee agrees to be bound by the terms of this Agreement. Any transfer terminates your license. You may not rent or lease the Software or otherwise transfer or assign the right to use the Software, except as stated in this paragraph.
5. You may not export the Software, even as part of the Cisco product, to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software, even as part of the Cisco product, in violation of any export control laws of the United States or any other country.
6. You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or accompanying documentation or any copy thereof, in whole or in part.
7. The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy, or return to Cisco Systems, the Software and accompanying documentation and all copies thereof. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.
8. You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 and 3 hereof.
9. You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.
10. Any notice, demand, or request with respect to this Agreement shall be in writing and shall be effective only if it is delivered by hand or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to Cisco Systems, whose address is set forth below. Such communications shall be effective when they are received by Cisco Systems.

## Limited Warranty

11. Cisco Systems warrants that the Software will perform substantially in accordance with the accompanying written materials for a period of 90 days from the date of your receipt of the Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.
12. CISCO SYSTEMS DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING WRITTEN MATERIALS, AND THE ACCOMPANYING HARDWARE. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.
13. CISCO SYSTEMS' ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY SHALL BE, AT CISCO SYSTEMS' CHOICE, EITHER (A) RETURN OF THE PRICE PAID OR (B) REPLACEMENT OF THE SOFTWARE THAT DOES NOT MEET CISCO SYSTEMS' LIMITED WARRANTY AND WHICH IS RETURNED TO CISCO SYSTEMS TOGETHER WITH A COPY OF YOUR RECEIPT. Any replacement Software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. These remedies are not available outside the United States of America.
14. This Limited Warranty is void if failure of the Software has resulted from modification, accident, abuse, or misapplication.
15. IN NO EVENT WILL CISCO SYSTEMS BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY LOSS OF PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE SOFTWARE. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

16. This Agreement is governed by the laws of the State of Massachusetts.

17. If you have any questions concerning this Agreement or wish to contact Cisco Systems for any reason, please call (508) 541-7300, or write to

**Cisco Systems, Inc.  
124 Grove Street, Suite 205  
Franklin, Massachusetts 02038.**

18. U.S. Government Restricted Rights. The Software and accompanying documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c)(1) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1)(ii) and (2) of Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Supplier is Cisco Systems, Inc., 124 Grove Street, Suite 205, Franklin, Massachusetts 02038.

19. This Agreement constitutes the entire agreement between Cisco Systems and the licensee. There are no understandings, agreements, representations, or warranties, expressed or implied, not specified herein regarding this Agreement or the Software licensed hereunder. Only the terms and conditions contained in this Agreement shall govern the transaction contemplated hereunder, notwithstanding any additional, different, or conflicting terms which may be contained in any purchase order or other documents pertaining to the subject transaction.

## Other licenses

The VPN 3000 Concentrator Series contains and uses software from other firms, under license. Relevant copyright and license notices follow.

## BSD software

Copyright © 1990, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# DHCP client

Copyright © 1995, 1996, 1997 The Internet Software Consortium.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of The Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# DNS Resolver (client)

DNS Resolver / BSD / DEC / Internet Software Consortium

Copyright © 1988, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



Portions Copyright © 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission.

To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product.

THE SOFTWARE IS PROVIDED "AS IS", AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

## IPSec

COPYRIGHT 1.1a (NRL) 17 August 1995

### COPYRIGHT NOTICE

All of the documentation and software included in this software distribution from the US Naval Research Laboratory (NRL) are copyrighted by their respective developers.

This software and documentation were developed at NRL by various people. Those developers have each copyrighted the portions that they developed at NRL and have assigned All Rights for those portions to NRL. Outside the USA, NRL also has copyright on the software developed at NRL. The affected files all contain specific copyright notices and those notices must be retained in any derived work.

NRL LICENSE

NRL grants permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation created at NRL provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed at the Information Technology Division, US Naval Research Laboratory.

4. Neither the name of the NRL nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THE SOFTWARE PROVIDED BY NRL IS PROVIDED BY NRL AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NRL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the US Naval Research Laboratory (NRL).

## **LDAP**

Copyright © 1992-1996 Regents of the University of Michigan.  
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

## **LZS221-C v6**

Copyright © 1988-1999 by Hi/fn, Inc. Includes one or more U.S. Patent numbers: 4701745, 5016009, 5126739, 5146221, 5414425, 5463390, and 5506580. Other Patents Pending.

## **MPPC-C v4**

Copyright © 1996-1998 by Hi/fn, Inc. Includes one or more U.S. Patent numbers: 4701745, 5016009, 5126739, 5146221, 5414425, and 5463390. Other Patents Pending.

# Outline style table of contents in JavaScript

OUTLINE STYLE TABLE OF CONTENTS in JAVASCRIPT, Version 3.0  
by Danny Goodman (dannyg@dannyg.com)  
Analyzed and described at length in "JavaScript Bible", by Danny Goodman  
(IDG Books ISBN 0-7645-3022-4)

This program is Copyright 1996, 1997, 1998 by Danny Goodman. You may adapt this outline for your Web pages, provided these opening credit lines (down to the lower dividing line) are in your outline HTML document. You may not reprint or redistribute this code without permission from the author.

## RSA software



Copyright © 1995-1998 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

BSAFE is a trademark of RSA Data Security, Inc.

## SecureID

SecureID is a product of RSA Security Inc., Bedford, MA. (formerly Security Dynamics Technologies, Inc.)

Use of SDTI's Trade Name and Trademarks

- (a) Any advertising or promotional literature or announcement to the press by the Partner regarding its relationship with SDTI, or otherwise utilizing SDTI's name or trademarks must be approved by SDTI in writing in advance, which approval will not be unreasonably withheld or delayed.
- (b) The Partner shall include and shall not alter, obscure or remove any SDTI name or any other trademark or trade name used by SDTI or any markings, colors or other insignia which are contained on or in or fixed to the Software (collectively, "Proprietary Marks"). Partner agrees to include SDTI's copyright notice in its help screen as it pertains to the SDTI Translation.

## Server SNMP

Copyright 1998 by Carnegie Mellon University  
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Client SNMP

Copyright © 1996, 1997 by Westhawk Ltd.

(www.westhawk.co.uk)

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

author tpanton@ibm.net (Tim Panton)

## SSH

Copyright © 1993, 1995-2000 by DataFellows, Inc. All rights reserved.

## SSL Plus

Certicom, the Certicom logo, SSL Plus, and Security Builder are trademarks of Certicom Corp. Copyright © 1997-1999 Certicom Corp. Portions are Copyright © 1997-1998, Consensus Development Corporation, a wholly owned subsidiary of Certicom Corp. All rights reserved.

Contains an implementation of NR signatures, licensed under U.S. patent 5,600,725. Protected by U.S. patents 5,787,028; 4,745,568; 5,761,305. Patents pending.

## TCP compression / uncompression

Routines to compress and uncompress TCP packets (for transmission over low speed serial lines).

Copyright © 1989 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

**THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.**

Van Jacobson (van@helios.ee.lbl.gov), Dec 31, 1989:

- Initial distribution.

Modified for KA9Q Internet Software Package by Katie Stevens (dkstevens@ucdavis.edu)

University of California, Davis

Computing Services

|            |               |                                               |
|------------|---------------|-----------------------------------------------|
| - 01-31-90 |               | initial adaptation (from 1.19)                |
| PPP.05     | 02-15-90 [ks] |                                               |
| PPP.08     | 05-02-90 [ks] | use PPP protocol field to signal compression  |
| PPP.15     | 09-90 [ks]    | improve mbuf handling                         |
| PPP.16     | 11-02 [karn]  | substantially rewritten to use NOS facilities |

- Feb 1991 Bill\_Simpson@um.cc.umich.edu  
variable number of conversation slots  
allow zero or one slots  
separate routines  
status display

## Telnet server

Copyright phase2 networks 1996  
All rights reserved

SID: 1.1

Revision History:

1.1 97/06/23 21:17:43 root

## Regulatory Standards Compliance

The VPN 3002 Hardware Client complies with these regulatory standards.

| Item                  | Description                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulatory Compliance | Products bear CE Marking indicating compliance with the 89/366/EEC, and 73/23/EEC directives, which includes the following safety and EMC standards.                                |
| Safety                | UL 60950<br>CAN/CSA-No. 60950-00<br>EN60950<br>IEC 60950<br>AS/NZS 3260                                                                                                             |
| EMC                   | FCC Part 15 (CFR 47) Class B<br>ICES-003 Class B<br>EN55022 Class B<br>CISPR22 Class B<br>AS/NZS 3548 Class B<br>VCCI Class B<br>EN55024<br>EN50082-1<br>EN61000-3-2<br>EN61000-3-3 |





## A

- about this manual xi
- access rights section, administration 12-8
- access settings, general, for administrators 12-10
- accessing the CLI 14-1
- add
  - event class 9-9
  - SNMP community 8-8
  - SNMP event destination 9-12
  - static route for IP routing 7-3
  - syslog server to receive events 9-15
- administering the VPN Concentrator 12-1
- administration section of Manager 12-1
- Administration (tab on Manager screen) 1-21
- administrators
  - access rights 12-8
  - access settings, general 12-10
  - configuring 12-9
  - parameters in nonvolatile memory 12-9
  - predefined 12-9
  - session idle timeout 12-11
- ARP table 13-37

## B

- back panel display (monitoring) 13-12
- Bad IP Address (error) A-10
- bibliography xv
- bootcode
  - filename 13-10
  - version 13-10
- browser
  - Back or Forward button displays incorrect screen or incorrect data A-5
  - clear cache after software update 12-4
  - installing SSL certificate 1-3
  - navigation toolbar, don't use with Manager 1-2
  - Refresh / Reload button logs out the Manager A-5
  - requirements 1-1
- built-in servers, configuring
  - See* management protocols 8-1

## C

- Certificate Authority

- See* digital certificates
- certificate management 12-15
- Cisco Connection Online Web page 1-20
- Cisco Systems (logo) 1-22
- clear event log 13-6
- CLI
  - access rights 14-7
  - accessing 14-1
    - via console 14-1
    - via Telnet 14-2
  - entering values 14-3
  - errors A-10
  - help command 14-6
  - main menu 14-2
  - menu reference 14-7
  - menus, navigating 14-4
  - saving configuration file 14-6
  - starting 14-2
  - stopping 14-7
  - using 14-1, 14-3
  - using Back and Home 14-5
  - using shortcut numbers to navigate 14-4
- Client (PAT) mode 11-1
- closed or collapsed (icon) 1-22
- Command Line Interface
  - See* CLI
- Concentrator settings
  - required for Network Extension mode 11-2
  - required for PAT 11-2
- configuration files
  - automatic backup with file upload 12-13
  - changes with software update 12-2
  - handling at reboot or shutdown 12-6
  - handling during file upload 12-13
  - saving 1-21
    - CLI 14-6
  - swap 12-13
  - useful for troubleshooting A-2
- configuration section of Manager 2-1
- Configuration (tab on Manager screen) 1-21
- configuring VPN Concentrator with CLI 14-1
- connecting to VPN Concentrator
  - using HTTP 1-3
  - using HTTPS 1-16
- console, accessing CLI via 14-1

## conventions

- documentation xvi
- typographic xvi

## cookies, requirements 1-2

## copyrights and licenses B-1

## crash, system, saves log file 9-5, A-1

## CRSHDUMP.TXT file A-1

**D**

## data

- formats xvi

## date and time, configuring 10-3

## Daylight-Saving Time, enabling 10-3

## default

- event handling, configuring 9-6
- gateways, configuring for IP routing 7-4

## delete

- digital certificate 12-27

## DHCP

- functions within the VPN Concentrator, configuring 7-5
- statistics 13-26

## digital certificates

- deleting 12-23, 12-27
- display all 12-23
- enrolling with a Certificate Authority 12-20
- enrollment request 12-17
- generating SSL 12-23
- identity 12-16
- in IPSec LAN-to-LAN 6-3
- installing 12-16, 12-21
- managing 12-15
- PKCS-10 request 12-20
- root 12-16
- SSL 12-16
- viewing details 12-24
- X.509 12-16

## display settings 1-3

## DNS

- servers, configuring 5-1
- statistics 13-23

## documentation

- additional xii
- Cisco Web page 1-20
- conventions xvi

**E**

## enrolling with a Certificate Authority 12-20

## entering values with CLI 14-3

## error

- an error has occurred ... A-7
- bad IP address A-10
- insufficient authorization A-7
- invalid login A-6

## no such interface supported (IE) A-9

## not allowed A-7

## not found A-8

## out of range value A-10

## passwords do not match A-10

## session timeout A-6

## errors

- and troubleshooting A-1
- CLI A-10
- VPN 3002 Hardware Client Manager A-5

## Ethernet MIB-II statistics 13-39

## event classes

- configuring for special handling 9-8
  - add 9-9
  - modify 9-9
- table 9-1

## event log 9-5

- clear (erase) 13-6
- download to PC 13-6
- filterable 13-3
- format of 13-6
- get 13-6
- live 13-8
- monitoring 13-3, 13-8
- save 13-6
- save on VPN Concentrator 13-6
- saved at system reboot 9-5, A-1
- saved if system crashes 9-5, A-1
- stored in nonvolatile memory 13-3
- view 13-3, 13-6, 13-8

## event severity levels, table 9-4

## event trap destinations, configuring 9-11

## events

- configuring default handling 9-6
- configuring handling 9-6
- configuring special handling 9-8
- section of Manager 9-1

## exiting

- from CLI 14-7
- the Manager (logout) 1-21

**F**

## file management on VPN Concentrator 12-11

file upload to VPN Concentrator 12-2, 12-13

- stopping 12-3, 12-14

## filter

- configuring on interface
  - Ethernet 3-6

## flash memory

- corrupting 12-2, 12-5
- managing files in 12-11
- temporary files in 12-14

## formats



- data xvi
- hostnames xvi
- IP addresses xvi
- MAC addresses xvi
- port numbers xvii
- subnet masks xvi
- text strings xvi
- wildcard masks xvi

front panel display (monitoring) 13-12

## G

- gateways, default 7-4
- general parameters, configuring 10-1
- generating SSL server certificate 12-23
- get event log 13-6

## H

- halt system 12-5
- help, CLI 14-6
- Help (tab on Manager screen) 1-20
- hostnames, format xvi
- HTTP
  - configuring internal server 8-2
  - statistics 13-21
  - using with Manager 1-3

## HTTPS

- configuring internal server 8-2
- connecting using 1-16
- login screen 1-17

## I

- ICMP MIB-II statistics 13-35
- icon
  - Cisco Systems logo 1-22
  - closed or collapsed 1-22
  - open or expanded 1-22
  - Refresh 1-22
  - Save 1-21
  - Save Needed 1-21
- identity certificates 12-16
- idle timeout for administrator sessions 12-11
- image, software
  - filenames 12-3
  - update 12-2
- indicators, LED A-2, A-10
- Install SSL Certificate (screen) 1-4
- installing digital certificates 12-16, 12-21
- installing SSL certificate
  - with Internet Explorer 1-4
  - with Netscape 1-9
- interfaces
  - configuring 3-1

- Ethernet, configuring
  - speed 3-6
  - transmission mode 3-4, 3-6
- filter
  - Ethernet 3-6
- MIB-II statistics 13-28
- public 3-6
- status 3-2

- Internet Explorer, requirements 1-1
- Invalid Login or Session Timeout (error) A-6
- IP addresses, format xvi
- IP MIB-II statistics 13-32
- IP routing
  - configuring 7-1
  - section of Manager 7-1
- IPSec
  - configuring 6-2
  - discussion 6-2
  - statistics 13-15

## J

- JavaScript, requirements 1-1

## L

- LED indicators
  - table A-2, A-10
- left frame (table of contents) in Manager window 1-22
- licenses and copyrights B-1
- log files
  - See event log
- logging in the VPN Concentrator Manager 1-17
- login
  - name
    - current (Manager) 1-21
    - factory default (Manager) 1-17
  - password, factory default (Manager) 1-17
  - screen 1-3
    - HTTPS 1-17
      - Internet Explorer 1-8
      - Netscape 1-14
- Logout (tab on Manager screen) 1-21

## M

- MAC addresses, format xvi
- main frame (Manager screen) in Manager window 1-22
- main menu, CLI 14-2
- Main (tab on Manager screen) 1-20
- management protocols, configuring 8-1
- Manager table of contents 1-23
- Manager toolbar, in Manager window 1-20
- Manager window
  - Cisco Systems logo 1-22

- left frame (table of contents) 1-22
- main frame 1-22
- mouse pointer and tips 1-20
- status bar 1-19
- title bar 1-19
- top frame (Manager toolbar) 1-20
- managing VPN Concentrator with CLI 14-1
- memory, SDRAM 13-10
- menus, CLI, navigating 14-4
- MIB-II
  - statistics 13-28
  - system object 10-2
- model number, system 13-10
- modify
  - event class 9-9
  - SNMP community 8-8
  - SNMP event trap destination 9-12
  - static route, for IP routing 7-3
  - syslog server to receive events 9-15
- monitor / display settings 1-3
- monitoring
  - section of Manager 13-1
- Monitoring (tab on Manager screen) 1-21
- mouse pointer and tips in Manager window 1-20

## **N**

- NAT
  - enable 11-4
  - many-to-one translation 11-4
- navigating
  - CLI menus 14-4
  - the VPN Concentrator Manager 1-23
- Netscape Navigator, requirements 1-1
- Network Extension mode 11-2
- No such interface supported (error) A-9
- nonvolatile memory 12-9
  - event log stored in 13-3
- Not Allowed (error) A-7
- Not Found (error) A-8
- notices, regulatory agency B-9

## **O**

- open or expanded (icon) 1-22
- organization of the VPN Concentrator Manager 1-22
- Out of Range value (error) A-10

## **P**

- password
  - factory default (Manager) 1-17
- Passwords do not match (error) A-10
- ping a host 12-7
- PKCS-10 enrollment request 12-20

- policy management
  - section of Manager 11-1
- port numbers, format xvii
- power, turning off 12-5
- prerequisites, system administrator xi

## **Q**

- quitting the Manager (logout) 1-21

## **R**

- reboot system 12-5
  - saves log file 9-5, 12-5, A-1
- references (bibliography) xv
- Refresh (icon) 1-22
- refreshing screen content 1-22
- regulatory agency notices B-9
- requirements
  - browser 1-1
  - cookies 1-2
  - Internet Explorer 1-1
  - JavaScript 1-1
  - Netscape Navigator 1-1
- root certificates 12-16
- routing table (monitoring) 13-2

## **S**

- save event log 13-6
- Save (icon) 1-21
- Save Needed (icon) 1-21
- SAVELOG.TXT file 9-5, 12-5, A-1
- saving configuration file with CLI 14-6
- screen
  - login 1-3
  - login, using HTTPS 1-17
- SDRAM memory 13-10
- servers, configuring system access to 5-1
- Session Timeout (error) A-6
- shutdown system 12-5
- SNMP
  - configuring internal server 8-5
  - event trap destinations, configuring 9-11
    - add 9-12
    - modify 9-12
  - MIB-II statistics 13-41
  - traps, configuring "well-known" 9-7
- SNMP communities, configuring 8-7
  - add 8-8
  - modify 8-8
- software image
  - filenames 12-3, 13-10
  - update on VPN Concentrator 12-2
    - stopping 12-3

- version info 12-3, 13-10
  - speed, configuring Ethernet interface 3-6
  - SSH
    - configuring internal server 8-12
    - host key 8-12
    - server key 8-12
    - server key regeneration 8-13
    - session key 8-12
    - statistics 13-27
  - SSL
    - client authentication 8-11
    - configuring internal server 8-9
    - statistics 13-24
  - SSL certificate 8-9, 12-16
    - generating 12-23
    - installing in browser 1-3
    - installing with Internet Explorer 1-4
    - installing with Netscape 1-9
    - viewing with Internet Explorer 1-8
    - viewing with Netscape 1-14
    - VPN Concentrator 1-4
  - starting the CLI 14-2
  - static routes, configuring for IP routing 7-2
    - add 7-3
    - modify 7-3
  - statistics 13-14
    - DHCP 13-26
    - DNS 13-23
    - HTTP 13-21
    - IPSec 13-15
    - MIB-II 13-28
      - ARP table 13-37
      - Ethernet 13-39
      - ICMP 13-35
      - interfaces 13-28
      - IP traffic 13-32
      - SNMP 13-41
      - TCP/UDP 13-30
    - SSH 13-27
    - SSL 13-24
    - Telnet 13-22
  - status bar in Manager window 1-19
  - stopping
    - CLI 14-7
    - file upload to VPN Concentrator 12-3, 12-14
    - the Manager (logout) 1-21
    - the VPN Concentrator 12-5
  - strings, text, format xvi
  - subnet masks, format xvi
  - superuser *See* administrators
  - support, Cisco 1-20
  - Support (tab on Manager screen) 1-20
  - swap configuration files 12-13
  - syslog servers, configuring for events 9-13
    - add 9-15
    - modify 9-15
  - system configuration section of Manager 4-1
  - system identification, configuring 10-2
  - system reboot 12-5
  - system shutdown 12-5
  - system status (monitoring) 13-9
- ## T
- tab
    - Administration 1-21
    - Configuration 1-21
    - Help 1-20
    - Logout 1-21
    - Main 1-20
    - Monitoring 1-21
    - Support 1-20
  - table of contents, Manager 1-23
  - TCP/UDP MIB-II statistics 13-30
  - Technical Assistance Center (TAC), contacting 1-21
  - Telnet
    - accessing CLI 14-2
    - configuring internal server 8-4
    - statistics 13-22
  - Telnet over SSL
    - configuring internal server 8-4
  - text strings, format xvi
  - time and date, configuring 10-3
  - time zone, configuring 10-3
  - timeout, administrator 12-11
    - live event log overrides 13-8
  - title bar in Manager window 1-19
  - top frame (Manager toolbar) in Manager window 1-20
  - transmission mode, configuring Ethernet interface 3-4, 3-6
  - traps, configuring
    - "well-known" 9-7
    - destination systems 9-11, 9-12
    - general events 9-7
    - specific events 9-10
  - troubleshooting A-1
    - consult event log 9-5, 13-3
    - files created for A-1
  - tunneling protocols
    - configuring 6-2
    - section of Manager 6-1
  - type (model number), system 13-10
  - typographic conventions xvi
- ## U
- understanding the VPN Concentrator Manager window 1-19
  - update software on VPN Concentrator 12-2
  - upload files to VPN Concentrator 12-13
  - using the CLI 14-3

using the VPN Concentrator Manager 1-1

**V**

viewing SSL certificates

    with Internet Explorer 1-8

    with Netscape 1-14

VPN 3002 Hardware Client Manager

    errors A-5

VPN Concentrator Manager

    logging in 1-17

    logging out 1-21

    navigating 1-23

    organization of 1-22

    understanding the window 1-19

    using 1-1

**W**

wildcard masks, format xvi

window, Manager, understanding 1-19

**X**

X.509 digital certificates 12-16