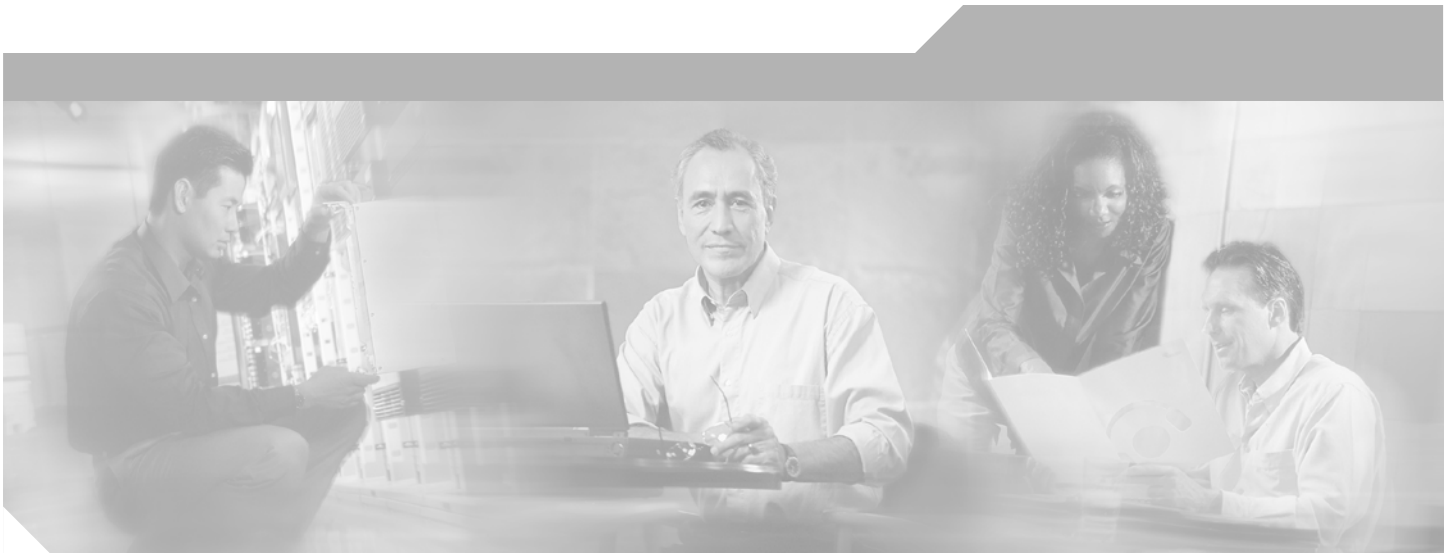


VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring

Release 4.0
April 2003

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: DOC-7815415=
Text Part Number: 78-15415-01

VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring

Preface

The VPN Concentrator provides an HTML-based graphic interface, called the *VPN Concentrator Manager*, that allows you to configure, administer, and monitor your device easily. The VPN Concentrator Manager has three sets of screens that correspond to these tasks: Configuration screens, Administration screens, and Monitoring screens.

VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring is the second in the two volume *VPN 3000 Series Concentrator Reference*. Together, both volumes document all the screens of the VPN Concentrator Manager.

- *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

This manual contains only administration and monitoring information. It does not contain any information about configuring the VPN Concentrator. For configuration information, refer to *VPN 3000 Series Concentrator Reference Volume I: Configuration.*

This manual also contains no information about installing the VPN Concentrator and initially configuring it. For information about set-up and initial configuration, refer to V*PN 3000 Series Concentrator Getting Started*.

Audience

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

Prerequisites

We assume you have read the *VPN 3000 Series Concentrator Getting Started* manual, set up your VPN Concentrator, and followed the minimal configuration steps in quick configuration.

Organization

Note This guide is the second volume of the complete VPN Concentrator Manager reference. It documents only administration and monitoring tasks. For information on configuring your VPN Concentrator, refer to *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

The chapters and sections of this guide correspond to the Administration and Monitoring parts of the VPN Concentrator Manager table of contents (the left frame of the Manager browser window) and are in the same order they appear there.

This guide has two parts:

- Part 1, "Administration," explains and defines all functions available in the Administration screens of the VPN Concentrator Manager.
- Part 2, "Monitoring," explains and defines all functions available in the Monitoring screens of the VPN Concentrator Manager.

This guide is organized as follows:

Chapter	Title	Explains How To...
Part One	**Administration**	
Chapter 1	Administration	Access the Administration screens.
Chapter 2	Administer Sessions	View statistics for all active sessions, to test if particular sessions are active, and to terminate sessions.
Chapter 3	Software Update	Update both the VPN Concentrator system software and the VPN Client software.
Chapter 4	System Reboot	Reboot or shutdown the system.
Chapter 5	Reboot Status	Check the schedule of system reboots.
Chapter 6	Ping	Test network connectivity.
Chapter 7	Monitoring Refresh	Set the status and statistics screens to refresh automatically.
Chapter 8	Access Rights	Configure and control administrative access to the VPN Concentrator.
Chapter 9	File Management	Manage files on the VPN Concentrator. It describes how to copy, view, and delete system files; how to swap backup and boot configuration files; and how to transfer files to and from the VPN Concentrator using TFTP, or to the VPN Concentrator using HTTP.

Chapter	Title	Explains How To...
Chapter 10	Certificate Management	Enroll and install digital certificates automatically (using Simple Certificate Enrollment Protocol, SCEP) or manually. It describes how to manage installed certificates, for example, how to view, delete, and renew them. It also explains how to enable digital certificates on the VPN Concentrator.
Part Two	**Monitoring**	
Chapter 11	Monitoring	Access the Monitoring screens.
Chapter 12	Routing Table	View routing statistics.
Chapter 13	Dynamic Filters	View external RADIUS filters in use on the VPN Concentrator.
Chapter 14	Filterable Event Log	View and manage the event log file.
Chapter 15	System Status	View the status of SEP modules, system power supplies, network interfaces, and several software and hardware variables.
Chapter 16	Sessions	View data for all active user and administrator sessions.
Chapter 17	Statistics	View statistics for traffic on the VPN Concentrator and for current tunneled sessions, plus statistics in standard MIB-II objects for interfaces, TCP/UDP, IP, ICMP, and the ARP table.
Appendix A	Using the Command-Line Interface	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 Concentrator Manager.
Appendix B	Troubleshooting and System Errors	Correct common errors that can occur while configuring the system. It also describes all system and module LED indicators.

Related Documentation

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

VPN 3000 Series Concentrator Documentation

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

The VPN Concentrator Manager also includes online help that you can access by clicking the Help icon on the toolbar in the Manager window.

The *VPN 3000 Series Concentrator Getting Started* manual takes you from unpacking and installing the VPN 3000 Series Concentrator, through configuring the minimal parameters to make it operational (called quick configuration).

The short document *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator* explains how to upgrade the VPN Concentrator memory. It also explains how to upgrade the VPN Concentrator software image and bootcode to versions that support the increased memory.

VPN Client Documentation

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

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

VPN 3002 Hardware Client Documentation

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

The *VPN 3002 Hardware Client 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 available only online.

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

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

Documentation on VPN Software Distribution CDs

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

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.
- *Virtual Private Networking: An Overview*. Microsoft Corporation: 1999. (Available from Microsoft website.)
- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

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

Notes use the following conventions:

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

Tips use the following conventions:

Tips Means *the following are useful tips.*

Cautions use the following conventions:

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

Warnings use the following conventions:

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.**

Data Formats

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

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

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

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

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

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

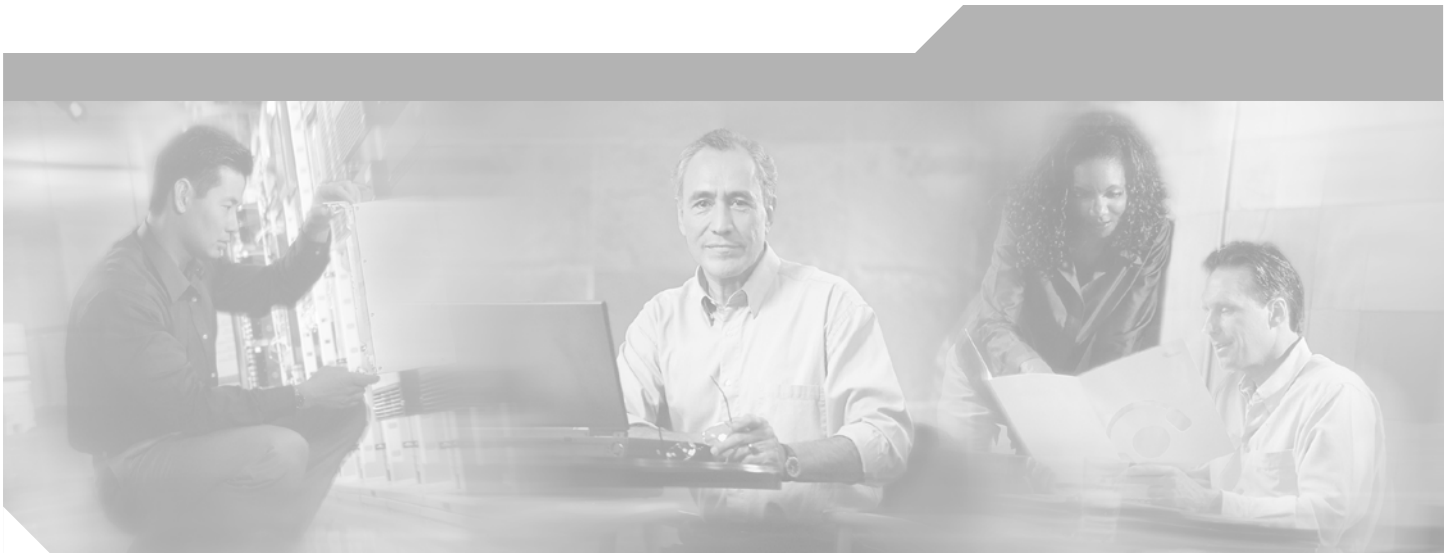
  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



PART 1

Administration

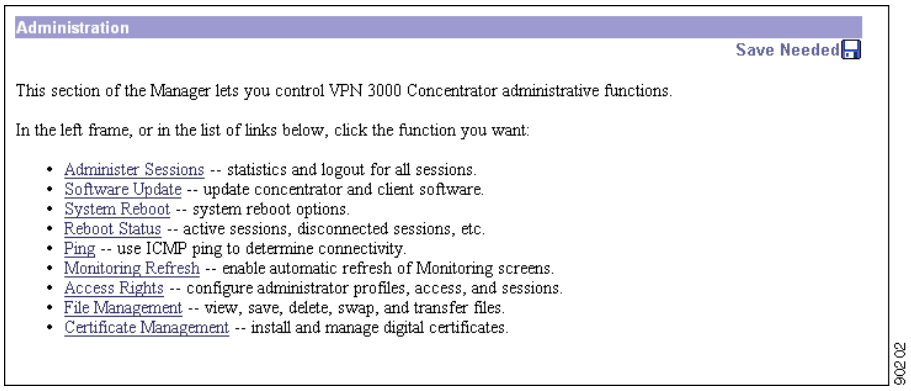
Administration

Administering the VPN 3000 Concentrator Series 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. Only administrators can use the VPN Concentrator Manager.

Administration

Step 1 In the VPN Concentrator Manager table of contents, click **Administration**. The Administration screen opens.

Figure 1-1 Administration Screen



This section of the Manager lets you control administrative functions on the VPN Concentrator:

- Administer Sessions: View statistics for, log out, and ping sessions.
- Software Update:
  - Concentrator: Upload and update the VPN Concentrator software image.
  - Clients: Upload and update the VPN client software image.
- System Reboot: Set options for VPN Concentrator shutdown and reboot.
- Reboot Status: Displays information about system reboots.
- Ping: Use ICMP ping to determine connectivity.
- Monitoring Refresh: Enable automatic refresh of status and statistics in the Monitoring section of the Manager.
- Access Rights: confiGure administrator profiles, access, and sessions.
  - Administrators: Configure administrator usernames, passwords, and rights.
  - Access Control List: Configure IP addresses for workstations with access rights.
  - Access Settings: Set administrative session idle timeout and limits.
  - AAA Servers: Set administrative authentication using TACACS+.
- File Management: Manage system files in flash memory.
  - Files: Copy, view, and delete system files.
  - Swap Configuration Files: Swap backup and boot configuration files.
  - TFTP Transfer: Use TFTP to transfer files to and from the VPN Concentrator.
  - File Upload: Use HTTP to transfer files to the VPN Concentrator.
- 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.

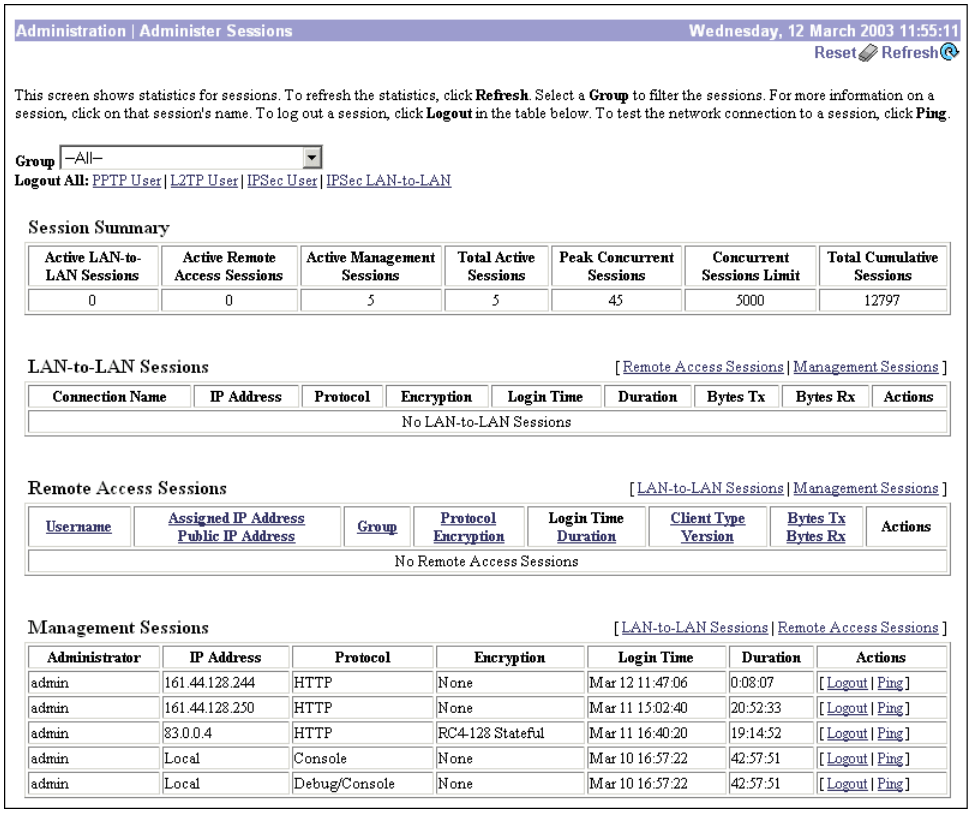
Administer Sessions

Administration | Administer Sessions

This screen shows comprehensive statistics for all active sessions on the VPN Concentrator.

You can also click the name of a session to see detailed parameters and statistics for that session. See Administration | Sessions | Detail.

Figure 2-1 Administration | Administer Sessions Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to monitor statistics for that group only. The default is --All-- which displays statistics for all groups.

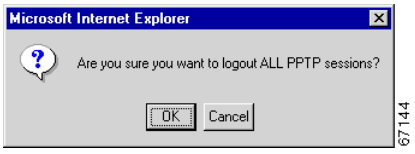
Logout All: PPTP User | L2TP User | IPSec User | L2TP/IPSec User | IPSec/UDP User | IPSec/TCP User | IPSec/LAN-to-LAN

These active labels let you log out *all* active sessions of a given tunnel type at once:

- PPTP User = PPTP remote-access users
- L2TP User = L2TP remote-access users
- IPSec User = IPSec remote-access users
- L2TP/IPSec User = L2TP over IPSec users
- IPSec/UDP User = IPSec through UDP users
- IPSec/TCP User = IPSec through TCP users
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN

To log out the sessions, click the appropriate label. The Manager displays a prompt to confirm the action.

Figure 2-2 Logout All Sessions Confirmation Prompt



Caution This action immediately terminates *all* sessions of the given tunnel type. *There is no user warning or undo.*

The Manager refreshes the screen after it terminates the sessions.

Session Summary table

This table shows summary totals for LAN-to-LAN, remote access, and management sessions.

A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

Active LAN-to-LAN Sessions

The number of IPSec LAN-to-LAN sessions that are currently active.

Active Remote Access Sessions

The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.

Active Management Sessions

The number of administrator management sessions that are currently active.

Total Active Sessions

The total number of sessions of all types that are currently active.

Peak Concurrent Sessions

The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.

Concurrent Sessions Limit

The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent, for example: model 3060 = 5000 sessions.

Total Cumulative Sessions

The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

LAN-to-LAN Sessions table

This table shows parameters and statistics for all active IPSec LAN-to-LAN sessions, sorted alphanumerically by connection name. Each session here identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

[Remote Access Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Connection Name

The name of the IPSec LAN-to-LAN connection.

To display detailed parameters and statistics for this connection, click this name. See the Administration | Sessions | Detail screen.

IP Address

The IP address of the remote peer VPN Concentrator or other secure gateway that initiated this LAN-to-LAN connection.

Protocol, Encryption, Login Time, Duration, Bytes TX, Bytes RX, Actions

See Table 2-1 for definitions of these parameters.

Remote Access Sessions table

This table shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the VPN Concentrator. Remote-access sessions include PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions.

Click a column header in this table to sort the table entries in ascending alphanumeric order, using that column as the sort key field.

[LAN-to-LAN Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Username

The username or login name for the session. The field shows `Authenticating...` if the remote-access client is still negotiating authentication. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

To display detailed parameters and statistics for this session, click this name. See the Administration | Sessions | Detail screen.

Assigned IP Address
Public IP Address

For the indicated user, this column shows the Assigned IP Address and the Public IP Address stacked in that order.

- The top address, called the Assigned IP Address, is the private IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network.

Note If the remote client is a VPN 3002 using network extension mode, this field shows the network address of the private interface of the 3002. Therefore, you cannot ping the address.

- The bottom address is the Public IP Address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.

Group

The group name of the client for this remote-access session. Clicking the column head for Group sorts the table entries in ascending alphanumeric order and also sorts the usernames within each group in ascending alphanumeric order.

Client Type and Operating System

The client type of connected clients, and, when available, the associated operating system, sorted by username. For example:

Client Type	Operating System
VPN 3000 Hardware Client	VPN3002
Windows NT client	Windows NT 4.0, Windows 2000, and Windows XP
Windows 98 client	Windows 98
Windows 95client	Windows 95

Version

The software version number (for example, rel. 3.6,_int 50) for connected clients, sorted by username.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx, Actions

See Table 2-1 on page 2-7 for definitions of these parameters.

Management Sessions table

This table shows parameters and statistics for all active administrator management sessions on the VPN Concentrator.

[LAN-to-LAN Sessions | Remote Access Sessions]

Click these active links to go to the other session tables on this Manager screen.

Administrator

The administrator username or login name for the session.

The lock icon indicates the administrator who has the configuration lock, that is, the person who has the right to make changes to the active system configuration. See the "Configuration locked by" section of this chapter.

IP Address

The IP address of the manager workstation that is accessing the system. Local indicates a direct connection through the Console port on the system.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx, Actions

See Table 2-1 for definitions of these parameters.

Table 2-1 Parameter definitions for Administration | Administer Sessions Screen

Parameter	Definition
Protocol	The protocol this session is using. `Console` indicates a direct connection through the Console port on the system.
Encryption	The data encryption algorithm this session is using, if any.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Bytes Tx	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Bytes Rx	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Actions / Logout / Ping	To log out a specific session, click **Logout**. The screen refreshes and shows the new session statistics. **Caution** Clicking **Logout** terminates a session without warning! There is no undo. To test the network connection to a session, click **Ping**. The VPN Concentrator sends an ICMP **Ping** message to the session IP address. See the Administration | Ping screen for details and results.

Configuration locked by

The administrator (IP address or Console) who has the right to make changes to the active system configuration.

The configuration is locked by the administrator who first makes a change to the active (running) configuration. That administrator holds the lock until logout, or until the Session Idle Timeout period expires (see the Administration | Access Rights | Access Settings screen). For example, an administrator who is just viewing and refreshing statistics on a Monitoring screen for longer than the timeout period, loses the lock.

Administration | Administer Sessions | Detail

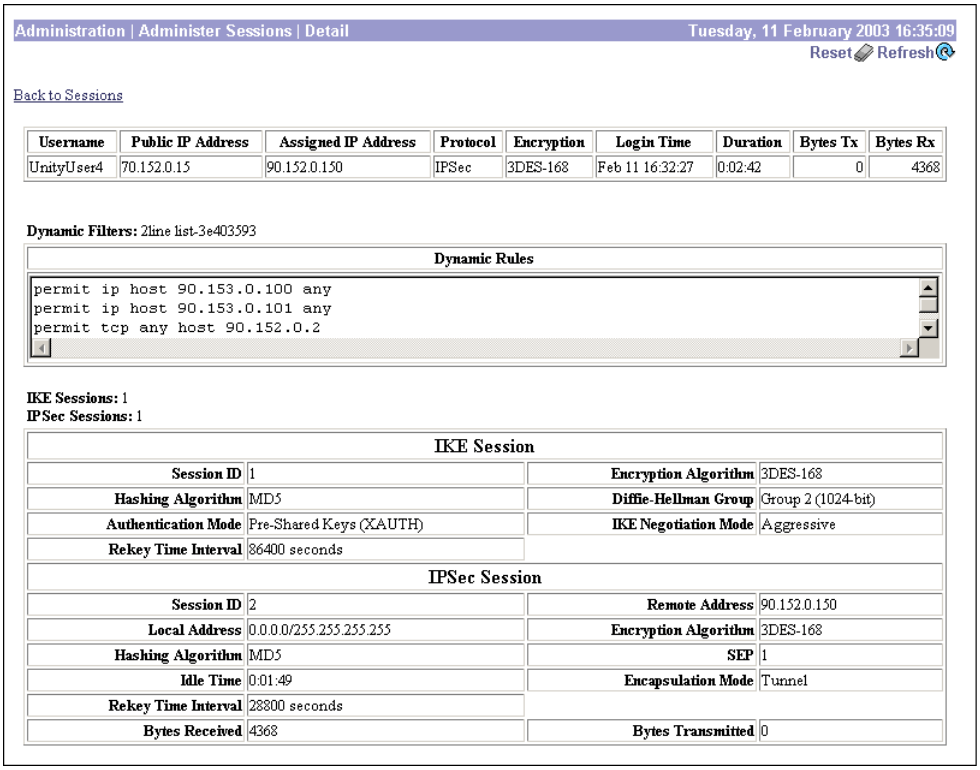
These Manager screens show detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. There are unique screens for:

- IPSec LAN-to-LAN (IPSec/LAN-to-LAN)
- IPSec remote access (IPSec User)
- IPSec through UDP (IPSec/UDP)
- IPSec through TCP (IPSec/TCP)
- L2TP
- L2TP over IPSec (L2TP/IPSec)
- PPTP

The Manager displays the appropriate screen when you click a highlighted connection name or username on the Administration | Administer Sessions screen. Figure 2-3 shows an example of one kind of detail screen. Depending on the type of connection you select, your detail screen might look somewhat different from the example shown. But, each session detail screen shows three tables: summary data, bandwidth statistics, and detail data. The summary data echoes the session data from the Administration | Administer Sessions screen. The Bandwidth Statistics table shows the effect of bandwidth policing on the session. The session detail table shows all the relevant parameters for each session and subsession.

See Table 2-2 for definitions of the possible session detail parameters, in alphabetical order.

Figure 2-3 Example Administration | Administer Sessions | Detail Screen



Administration | Administer Sessions | Detail Parameters

Table 2-2 Parameter Definitions for Administration | Administer Sessions | Detail Screens

Parameter	Definition
Assigned IP Address	The private IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network.
Authentication Mode	The protocol or mode used to authenticate this session.
Bytes Rx Bytes Received	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Bytes Tx Bytes Transmitted	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Compression	The data compression algorithm this session is using. LZS is the data compression algorithm used by IPComp. MPPC uses LZ.
Connection Name	The name of the IPSec LAN-to-LAN connection.
Diffie-Hellman Group	The algorithm and key size used to generate IPSec SA encryption keys.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Dynamic Filter	RADIUS user filter applied to this session.
Dynamic Rules	The rules that make up the dynamic filter. For the syntax of these rules, see Dynamic Filters, page 13-3.
Encapsulation Mode	The mode for applying IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication, in other words, what part of the original IP packet has ESP applied.
Encryption Encryption Algorithm	The data encryption algorithm this session is using, if any.
Hashing Algorithm	The algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Idle Time	The elapsed time (HH:MM:SS) between the last communication activity on this session and the last screen refresh.
IKE Negotiation Mode	The IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	The total number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
Interface	The interface this session is using.
IP Address	The IP address of the remote peer VPN Concentrator or other secure gateway that initiated the IPSec LAN-to-LAN connection.

Table 2-2 Parameter Definitions for Administration | Administer Sessions | Detail Screens (continued)

Parameter	Definition
IPSec Sessions	The total number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session might have two IPSec sessions: one showing the tunnel endpoints, and one showing the private networks reachable through the tunnel.
L2TP Sessions	The total number of user sessions through this L2TP or L2TP / IPSec tunnel; usually `1`.
Local Address	The IP address (and wildcard mask) of the destination host (or network) for this session.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Perfect Forward Secrecy Group	The Diffie-Hellman algorithm and key size used to generate IPSec SA encryption keys using Perfect Forward Secrecy.
PFS Group	The Perfect Forward Secrecy group: 1, 2, 3, 4, or 7.
PPTP Sessions	The total number of user sessions through this PPTP tunnel; usually `1`.
Protocol	The tunneling protocol that this session is using.
Public IP Address	The public IP address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
Rekey Data Interval	The lifetime in kilobytes of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	The lifetime in seconds of the IPSec (IKE) SA encryption keys.
Remote Address	The IP address (and wildcard mask) of the remote peer (or network) that initiated this session.
SEP	The Scalable Encryption Module that is handling cryptographic processing for this session.
Session ID	An identifier for session components (subsessions) on this screen. With IPSec, there is one identifier for each SA.
Traffic Rate (bytes)	The effect of bandwidth management on this session's traffic rate. • Conformed = The current rate of session traffic (as set by the bandwidth management policy). • Throttled = The rate at which packets are being throttled to maintain the conformed rate.

Table 2-2 Parameter Definitions for Administration | Administer Sessions | Detail Screens (continued)

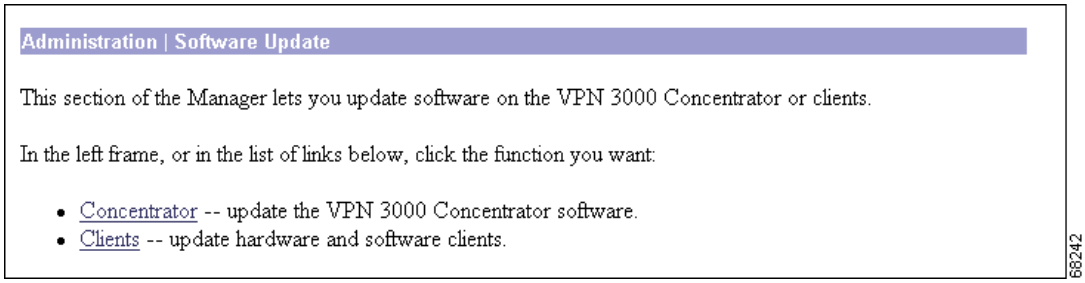
Parameter	Definition
Traffic Volume (kbps)	The effect of bandwidth management on this session's traffic volume. • Conformed = The number of bytes of session traffic (as set by the bandwidth management policy). • Throttled = The number of bytes being throttled to maintain the conformed rate. **Note** The Bandwidth Management Traffic Volume byte counters include the outer IP tunnel header and MAC layer and therefore show larger totals than those shown for user statistics.
UDP Port	The UDP port number used in an IPSec through NAT connection.
Username	The username or login name for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

Software Update

Administration | Software Update

This section of the Manager lets you update the VPN Concentrator executable system software and the VPN Client software.

Figure 3-1 Administration | Software Update Screen



- Concentrator: Uploads the executable system software (the software image) to the VPN Concentrator
- Client: Updates the VPN 3002 Hardware Client software

Administration | Software Update | Concentrator

This process uploads the executable system software to the VPN Concentrator, which then verifies the integrity of the software image.

The new image file must be accessible by the workstation you are using to manage the VPN Concentrator. Software image files ship on the Cisco VPN 3000 Concentrator 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 Concentrator. 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.

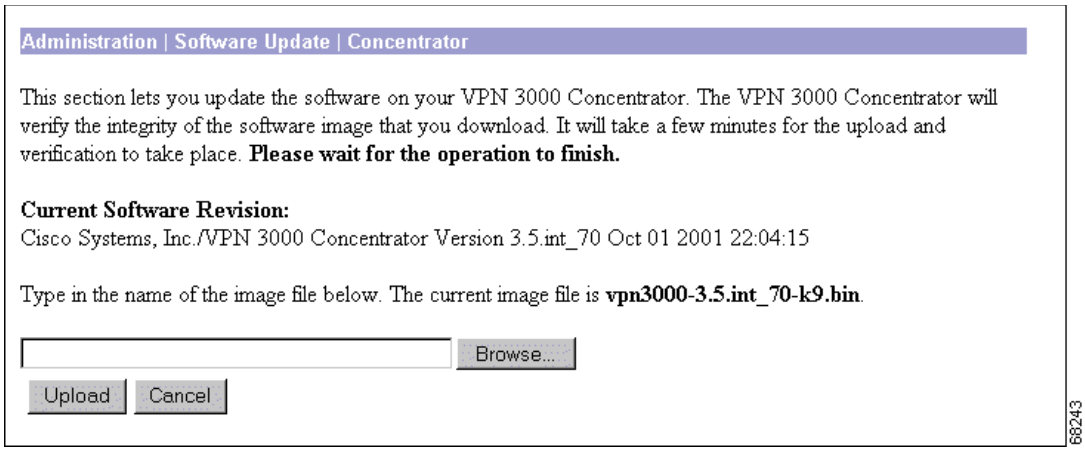
Note The VPN Concentrator has two locations for storing image files: the active location, which stores the image currently running on the system; and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. Updating *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.

Note 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 might corrupt memory.

Updating the software image also makes available any new Cisco-supplied configurable selections for filter rules, Security Associations, IKE proposals, base-group attributes, etc. 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. See Administration | File Management for ways to manage CONFIG files.

Figure 3-2 Administration | Software Update | Concentrator Screen



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 3000 Concentrator software image files are named:

- For model 3005 = vpn3005-<*Major Version*>.<*Minor Version*>.<*Sustaining Version*>.<*Patch Version*>-k9.bin. (For example, vpn3005-3.0.Rel-k9.bin.)
- For models 3015, 3030, 3060, and 3080 = vpn3000-<*Major Version*>.<*Minor Version*>.<*Sustaining Version*>.<*Patch Version*>-k9.bin. (For example, vpn3000-3.0.1-k9.bin.)

The Major and Minor Version numbers are always present; the initial Patch version is Rel; the Sustaining Version number is present only if needed.

The correct file must be selected for your VPN Concentrator model; otherwise the update will fail.

Upload / Cancel

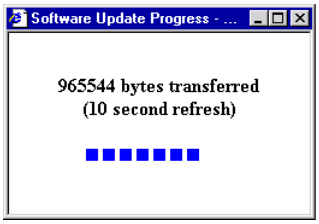
To upload the new image file to the VPN Concentrator, click **Upload**.

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 might 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 3-3 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.

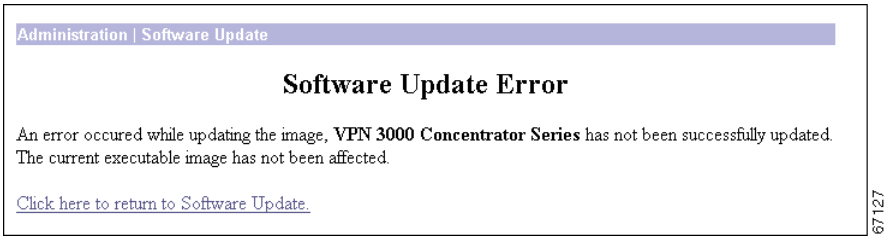
We strongly recommend that you clear the cache of your browser after you update the software image: delete all the browser's temporary internet files, history files, and location bar references.

Figure 3-4 Administration | Software Update Success Screen

Software Update Error

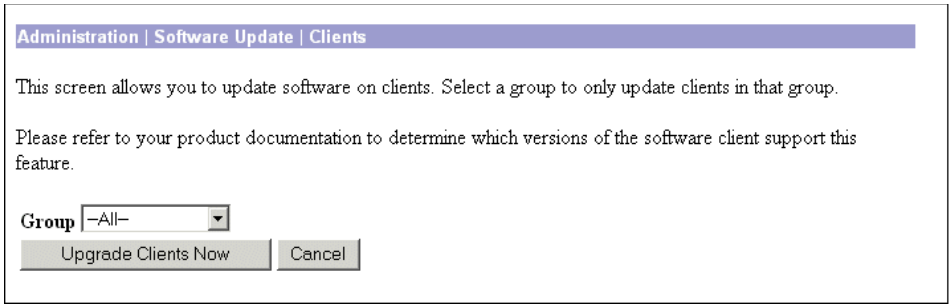
This screen appears if there was an error in uploading or verifying the image file. You might have selected the wrong file. Click the highlighted link to return to the Administration | Software Update screen and try the update again, or contact Cisco support.

Figure 3-5 Administration | Software Update Error Screen



Administration | Software Update | Clients

Figure 3-6 Administration| Software Update | Clients Screen



Group

Lets you select the VPN 3002 Hardware Client group for this update (the automatic update feature works on a group basis). The default is --All--, which lets you update the software for all groups. The Concentrator updates clients by group, in batches of ten, at 5-minute intervals.

Upgrade Clients Now

To update the VPN 3002 hardware Client software for the group you have selected, click **Upgrade Clients Now**.

Cancel

If you decide not to update client software now, click **Cancel**. The Manager returns to the Administration | Software Update screen, without updating software for any client(s).

System Reboot

Administration | System Reboot

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

Caution We strongly recommend that you shut down the VPN Concentrator 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.

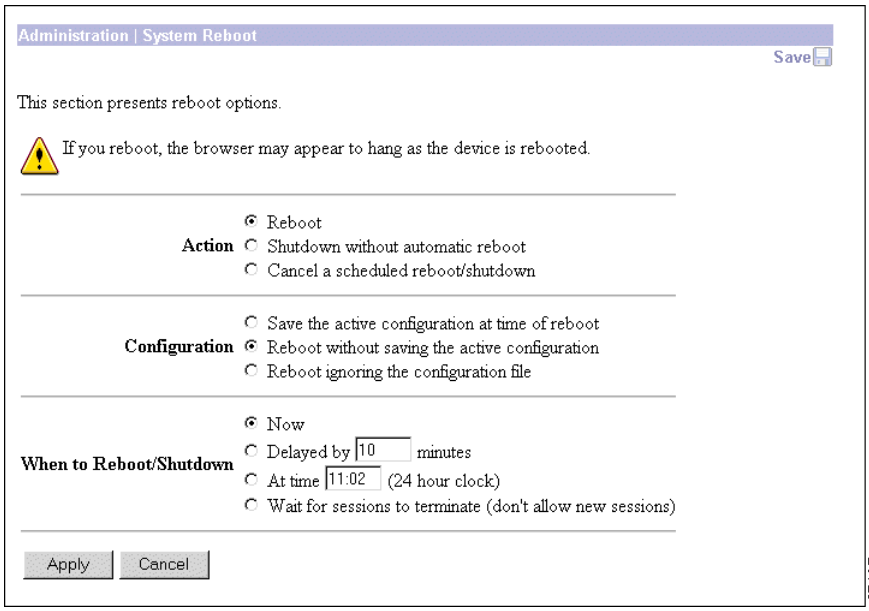
If you are logged in the Manager when the system reboots or halts, it automatically logs you out and displays the main login screen. The browser may appear to hang during a reboot; that is, you cannot log in and you must wait for the reboot to finish. You can log back in while the VPN Concentrator is in a shutdown state, before you turn power off. On the Models 3015–3080, all 10 blue usage monitor LEDs on the VPN Concentrator front panel blink when the system is in a shutdown state. On the Model 3005, the System LED blinks.

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 does not wait for sessions to terminate. It terminates all active sessions without warning and prevents new user sessions.

The VPN Concentrator 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 | File Management, and Monitoring | Filterable Event Log for more information on the event log file.

Figure 4-1 Administration | System Reboot Screen



Action

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

- Reboot = Reboot the VPN Concentrator. 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 Concentrator; 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 System LED (Model 3005) or the blue usage LEDs (Models 3015–3080) 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 Concentrator 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 (do not 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.)

Reboot Status

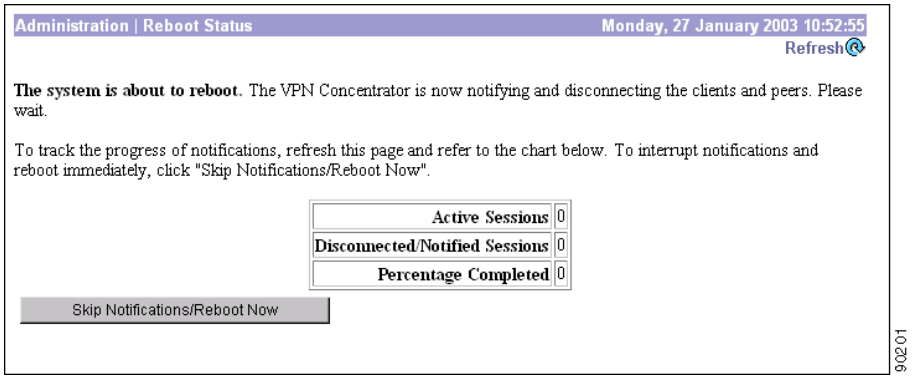
Administration | Reboot Status

This screen displays reboot status for the VPN Concentrator. It has various options, shown in the figures that follow.

Reboot Now

When you choose the Reboot/Shutdown Now option on the Administration | System Reboot screen, this screen displays.

Figure 5-1 Administration | Reboot Status Screen, Reboot Now



Active Sessions

Total number of active sessions prior to this reboot.

Disconnected/Notified Sessions

Number of sessions notified and disconnected.

Percentage Completed

Percentage of active sessions notified and disconnected.

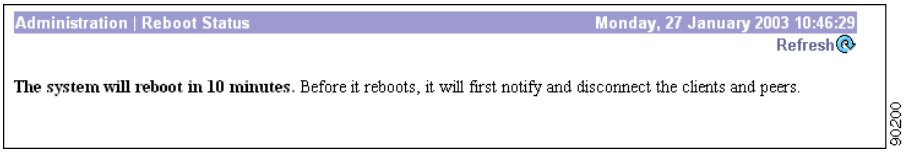
Skip Notifications/Shutdown Now

Click this button to shutdown all sessions immediately, without notification.

Reboot in <*n*> Minutes

When you choose the Reboot/Shutdown Delayed by <*n*> minutes option on the Administration | System Reboot screen, this screen displays.

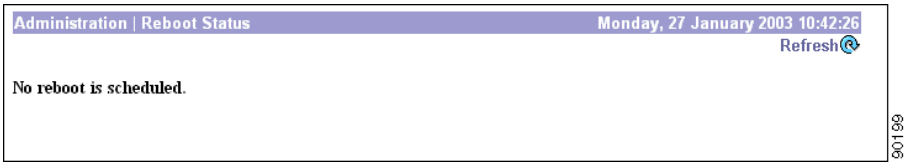
Figure 5-2 Administration | Reboot Status Screen, Reboot in 10 Minutes



No Reboot

When you choose to have no scheduled reboot, or when you cancel a scheduled reboot, this screen displays.

Figure 5-3 Administration | Reboot Status Screen, No Reboot Scheduled



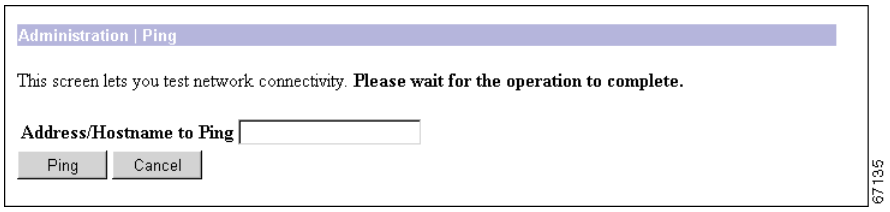
Ping

Administration | Ping

This screen lets you use the ICMP `ping` (Packet Internet Groper) utility to test network connectivity. Specifically, the VPN Concentrator 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 6-1 Administration | Ping Screen



Address/Hostname to Ping

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

Ping / Cancel

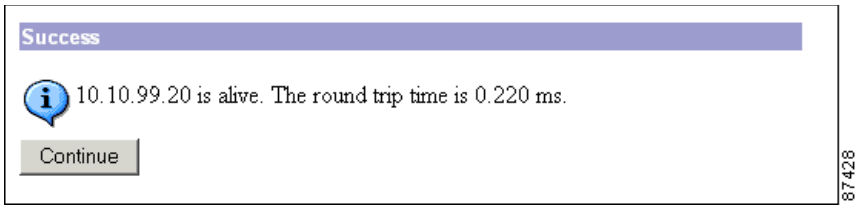
To send the ping message, click **Ping**. The Manager pauses during the test, which may take a few moments; *please wait for the operation to finish*. The Manager then displays either a Success or Error screen.

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. It also shows the length of elapsed time between when the request was sent and when the response was received.

Figure 6-2 Administration | Ping | Success Screen



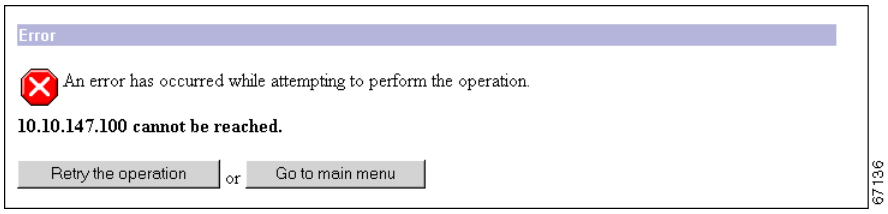
Continue

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

Error (Ping)

If the system is unreachable for any reason, (for example: host down, ICMP not running on host, route not configured, intermediate router down, or network down or congested), 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 6-3 Administration | Ping | Error Screen



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

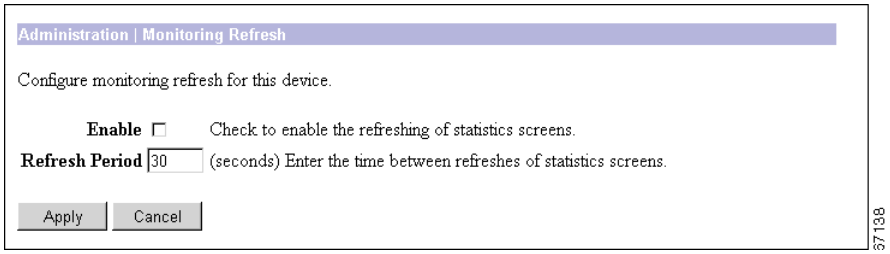
To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

Monitoring Refresh

Administration | Monitoring Refresh

This screen lets you enable automatic refresh of all status and statistics screens in the Monitoring section of the VPN Concentrator Manager except the Event Log.

Figure 7-1 Administration | Monitoring Refresh Screen



Enable

To enable automatic refresh, check the **Enable** check box. The box is unchecked by default.

Refresh Period

Enter the refresh period in seconds. The minimum period is 1 second. The default period is 30 seconds. The maximum period is 2000000000 seconds (about 63 years). Very short periods may affect system performance.

The refresh period timer begins *after* the Manager fully displays a given screen.

Apply / Cancel

To save your settings in the active configuration, click **Apply**. The Manager goes to the main Administration 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 goes to the main Administration screen.

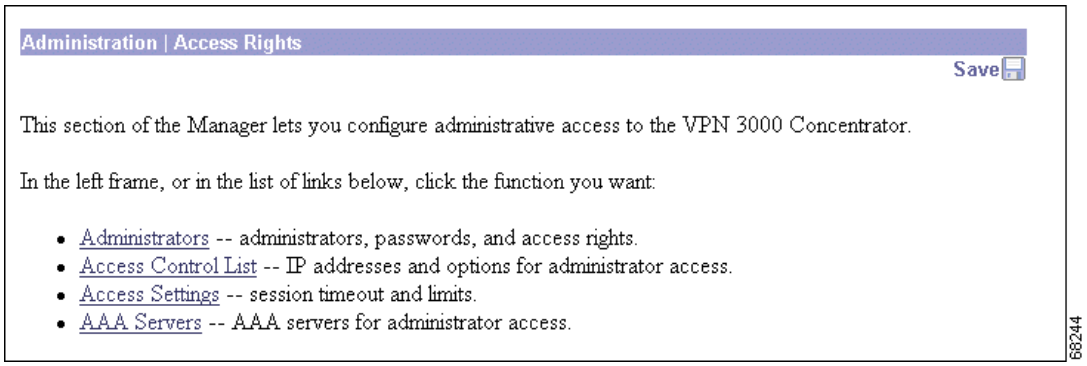
Access Rights

Administration | Access Rights

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

- Administrators: Configure administrator usernames, passwords, and rights.
- Access Control List: Configure IP addresses for workstations with access rights.
- Access Settings: Set administrative session timeout and limits.
- AAA Servers: Set administrative authentication using TACACS+.

Figure 8-1 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 VPN Concentrator. Only administrators can use the VPN Concentrator Manager.

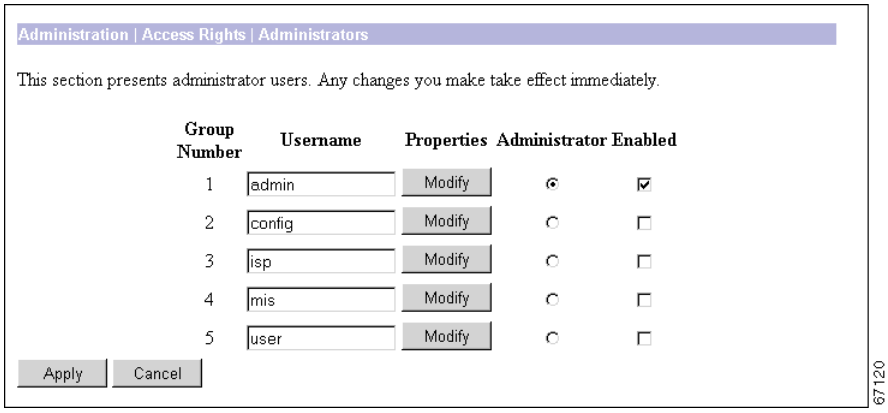
Cisco provides five predefined administrators:

- 1 - admin = System administrator with access to, and rights to change, all areas. This is the only administrator enabled by default. This is the only administrator who can log in to, and use, the VPN Concentrator Manager as supplied by Cisco.
- 2 - config = Configuration administrator with all rights except SNMP access.
- 3 - isp = Internet service provider administrator with limited general configuration rights.
- 4 - mis = Management information systems administrator with the same rights as config.
- 5 - user = User administrator with rights only to view system statistics.

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

Note The VPN Concentrator saves Administrator parameter settings from this screen and the Modify Properties 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.

Figure 8-2 Administration | Access Rights | Administrators Screen



Group Number

This is a reference number for the administrator. Cisco assigns these numbers so you can refer to administrators by groups of properties. The numbers cannot be changed.

Username

The username, or login name, of the administrator. You can change this name on the Administration | Access Rights | Administrators | Modify Properties screen.

Note *The default passwords that Cisco supplies are the same as the usernames. We strongly recommend that you change these passwords.*

Properties / Modify

To modify the username, password, and access rights of the administrator, click **Modify**. See the Administration | Access Rights | Administrators | Modify Properties screen.

Administrator

To assign "system administrator" privileges to one administrator, click the radio button. Only the "system administrator" can access and configure properties in this section. You can select only one. By default, admin is selected.

Enabled

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

Apply / Cancel

To save the settings of this screen 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 | Administrators | Modify Properties

This screen lets you modify the username, password, and rights for an administrator. Any changes affect new sessions as soon as you click **Apply** or **Default**.

Figure 8-3 Administration | Access Rights | Administrators | Modify Properties Screen

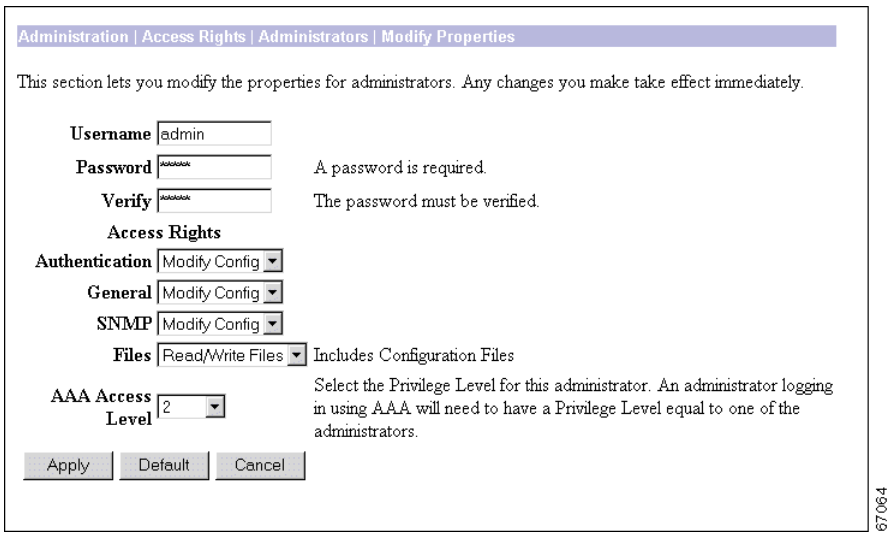


Table 8-1 shows the matrix of Cisco-supplied default rights for the five administrators.

Table 8-1 Cisco-Supplied Default Administrator Rights

Administrator	Authentication	General	SNMP	Files
1 - admin	Modify Config	Modify Config	Modify Config	Read/Write Files
2 - config	Modify Config	Modify Config	Stats Only	Read/Write Files
3 - isp	Stats Only	Modify Config	Stats Only	Read Files
4 - mis	Modify Config	Modify Config	Stats Only	Read Files
5 - user	Stats Only	Stats Only	Stats Only	Read Files

Username

Enter or edit the unique username for this administrator. The maximum length is 31 characters.

Password

Enter or edit the unique password for this administrator. The maximum length 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.

Access Rights

The Access Rights determine access to and rights in VPN Concentrator Manager functional areas (Authentication or General), or via SNMP. Click the **Access Rights** drop-down menu button and choose the access rights:

- None = No access or rights.
- Stats Only = Access to only the Monitoring section of the VPN Concentrator Manager. No rights to change parameters.
- View Config = Access to permitted functional areas of the VPN Concentrator Manager, but no rights to change parameters.
- Modify Config = Access to permitted functional areas of the VPN Concentrator Manager, and rights to change parameters.

Authentication

This area consists of VPN Concentrator Manager functions that affect authentication:

- Configuration | User Management
- Configuration | Policy Management | Access Hours
- Configuration | System | Servers | Authentication and Configuration | System | Servers | Accounting.

General

This area consists of all VPN Concentrator Manager functions except authentication and administration. (The Administrator radio button on the Administration | Access Rights | Administrators screen controls access to administration functions.)

SNMP

This parameter governs limited changes to the VPN Concentrator Manager via SNMP, using a network management system. In other words, it determines what the administrator can do via SNMP.

Files

This parameter governs rights to access and manage files in VPN Concentrator Flash memory, and to save the active configuration in a file. (Flash memory acts like a disk.) Click the **Files** drop-down menu button and choose the file management rights:

- None = No file access or management rights.
- List Files = See a list of files in VPN Concentrator Flash memory.
- Read Files = Read (view) files in Flash memory.
- Read/Write Files = Read and write files in Flash memory, clear or save the event log, and save the active configuration to a file.

AAA Access Level

This parameter governs the level of access for administrators authenticated by a TACACS+ server. On the TACACS+ server you configure levels of privilege, maximum 0-15, to suit your environment. You can set the number of privilege levels and order them as you choose (numbered in ascending order, descending order, or whatever scheme meets your requirements). You then set this AAA Access Level parameter to one of the levels configured on the TACACS+ server. Administrators have access privileges corresponding to the level you assign.

Apply / Default / Cancel

To save your settings in nonvolatile memory, click **Apply**. The settings take effect immediately. The Manager returns to the Administration | Access Rights | Administrators screen.

To restore the Cisco-supplied access rights for this administrator, and to save your settings in nonvolatile memory, click **Default**. The settings take effect immediately. *This action does not restore the default username or password.* The Manager returns to the Administration | Access Rights | Administrators screen.

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

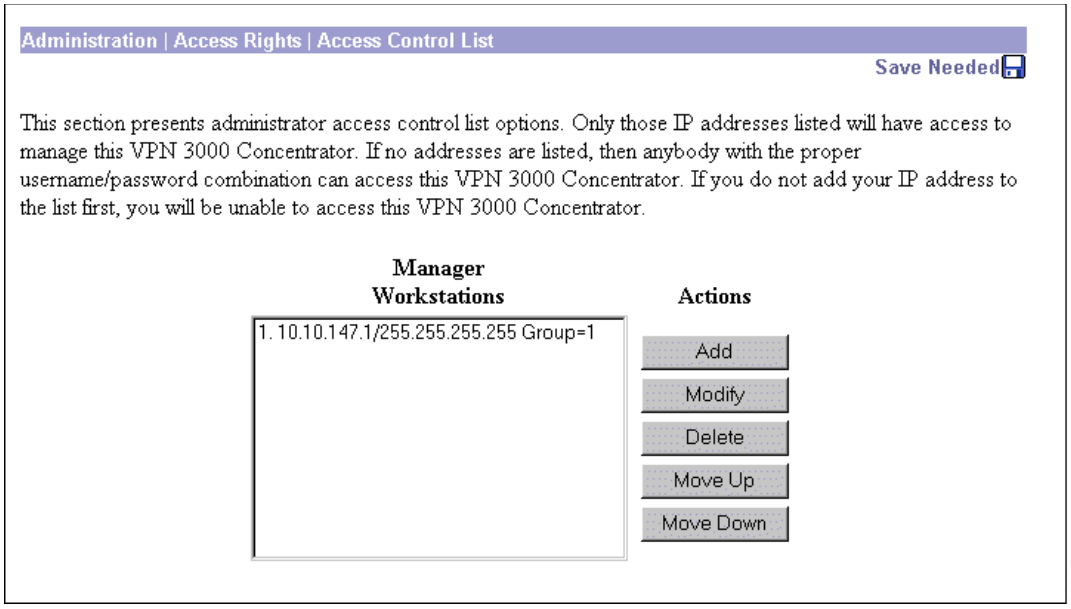
Administration | Access Rights | Access Control List

This section of the Manager lets you configure and prioritize the systems (workstations) that are allowed to access the VPN Concentrator Manager. For example, you might want to allow access only from one or two PCs that are in a locked room. If no systems are listed, then anyone who knows the VPN Concentrator IP address and the administrator username/password combination can gain access.

As soon as you add a workstation to the list, access control becomes effective for new sessions. Therefore, the first entry on the list should be the IP address of the workstation you are now using to configure the VPN Concentrator. Otherwise, if you log out or time out, you will not be able to access the Manager from the workstation.

These entries govern administrator access and management by any remote means: HTTP, HTTPS, FTP, TFTP, SNMP, Telnet, SSH, etc.

Figure 8-4 Administration | Access Rights | Access Control List Screen



Manager Workstations

The Manager Workstations list shows the configured workstations that are allowed to access the VPN Concentrator Manager, in priority order. Each entry shows the priority number, IP address/ mask, and administrator group number, for example: 1. 10.10.1.35/255.255.255.255 Group=1. If no workstations have been configured, the list shows --Empty--.

Add / Modify / Delete / Move

To configure a new manager workstation, click **Add**. The Manager opens the Administration | Access Rights | Access Control List | Add screen.

To modify a configured manager workstation, select the entry from the list and click **Modify**. The Manager opens the Administration | Access Rights | Access Control List | Modify screen.

To remove a configured manager workstation, select the entry from the list and click **Delete**. The Manager refreshes the screen and shows the remaining entries in the Manager Workstations list.

To change the priority order for configured manager workstations, select the entry from the list and click **Move Up** or **Move Down** The Manager refreshes the screen and shows the reordered Manager Workstations list.

Reminder:

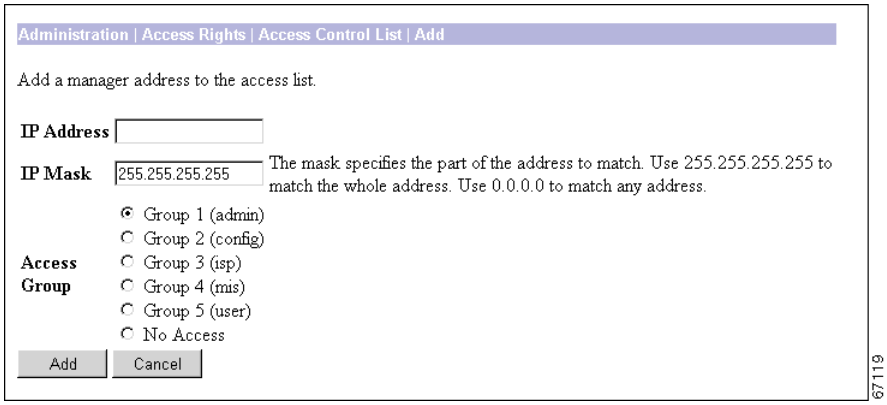
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Administration | Access Rights | Access Control List | Access Control List: Add or Modify

These screens let you:

- Add a manager workstation to the list of those that are allowed to access the VPN Concentrator Manager.
- Modify a previously configured workstation that is allowed to access the VPN Concentrator Manager.

Figure 8-5 Administration | Access Rights | Access Control List | Add or Modify Screen



Priority (Modify screen only)

This field shows the priority number of this workstation in the list of Manager Workstations. You cannot edit this field. To change the priority, use the Move buttons on the Administration | Access Rights | Access Control List screen.

IP Address

Enter the IP address of the workstation in dotted decimal notation, for example: 10.10.1.35.

IP Mask

Enter the mask for the IP address in dotted decimal notation. This mask lets you restrict access to a single IP address, a range of addresses, or all addresses. To restrict access to a single IP address, enter **255.255.255.255** (the default). To allow all IP addresses, enter **0.0.0.0**. To allow a range of IP addresses, enter the appropriate mask. For example, to allow IP addresses 10.10.1.32 through 10.10.1.35, enter the mask **255.255.255.252**.

Access Group

To assign rights of an administrator group to this IP address, click the appropriate radio button. The default choice is Group 1 (admin). You can assign only one group, or you can specify No Access.

Add or Apply / Cancel

To add this workstation to the list, click **Add**. Or to apply your changes to this workstation, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Administration | Access Rights | Access Control List screen. Any new entry appears at the bottom of the Manager Workstations list.

Reminder:

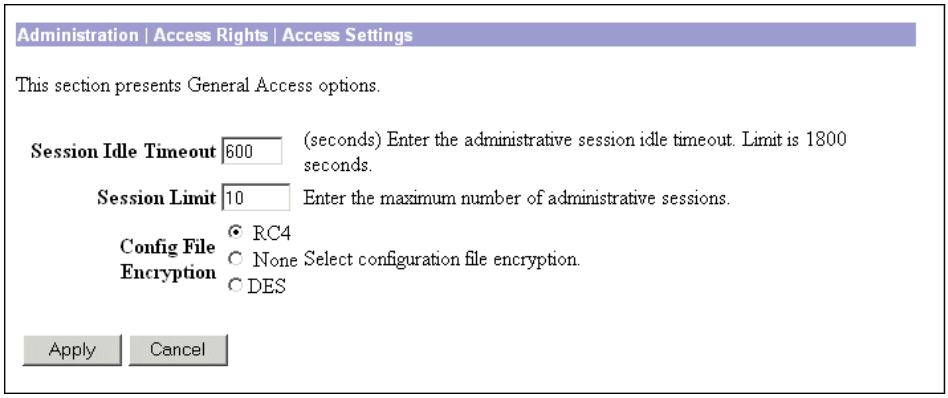
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Administration | Access Rights | Access Control List screen, and the Manager Workstations list is unchanged.

Administration | Access Rights | Access Settings

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

Figure 8-6 Administration | Access Rights | Access Settings Screen



Session Idle Timeout

Enter the idle timeout period in seconds for administrative sessions. If there is no activity for this period, the VPN Concentrator Manager session terminates. The minimum period is 1 second. The default period is 600 seconds. The maximum period 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.

If you close out of the Manager without logging off, no one can change the configuration from a different PC until the logout time has been reached. Either you must log in and then log out, or the other user must wait until the session idle timeout limit has occurred.

Session Limit

Enter the maximum number of simultaneous administrative sessions allowed. The minimum is 1 session. The default is 10 sessions. The maximum is 50 sessions.

Config File Encryption

The CONFIG file is in ASCII text format (.INI format). The **Config File Encryption** radio button allows you to encrypt sensitive entries in this file, such as passwords, keys, and user information.

- RC4 = Encrypt sensitive entries in the CONFIG file, using RC4 encryption. This option is the default.
- None = Use clear text for all CONFIG file entries. For maximum security, we do *not* recommend this option.
- DES = Encrypt sensitive entries in the CONFIG file, using DES encryption.

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 | Access Rights | AAA Servers

This section lets you configure AAA servers to authenticate administrators for this VPN Concentrator.

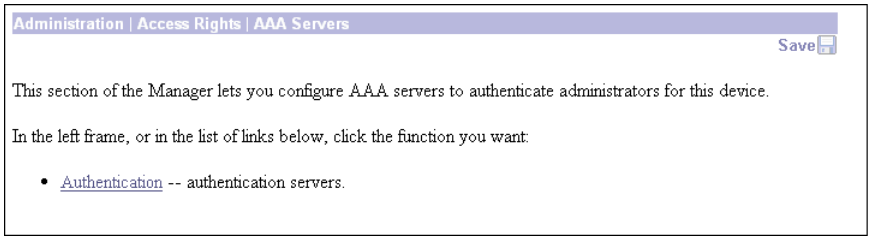
Before you configure a TACACS+ server here, be sure that the server you reference is itself properly configured and that you know how to access it (IP address or host name, TCP/UDP port, secret/password, etc.). The VPN Concentrator functions as the client of these servers.

You can configure and prioritize up to 10 TACACS+ servers. The first server of a given type is the primary server for that type, and the rest are backup servers in case the primary is inoperative.

Note In addition to configuring AAA servers, to use TACACS+ you must set a value in the AAA Access Level parameter; see Administration | Access Rights | Administrators | Modify.

Caution Misconfiguration of TACACS+ can lock an administrator out of the Concentrator HTML interface. If that happens, you can access the Concentrator by logging in through the console port, using your administrator username and password.

Figure 8-7 Administration | Access Rights | AAA Servers Screen

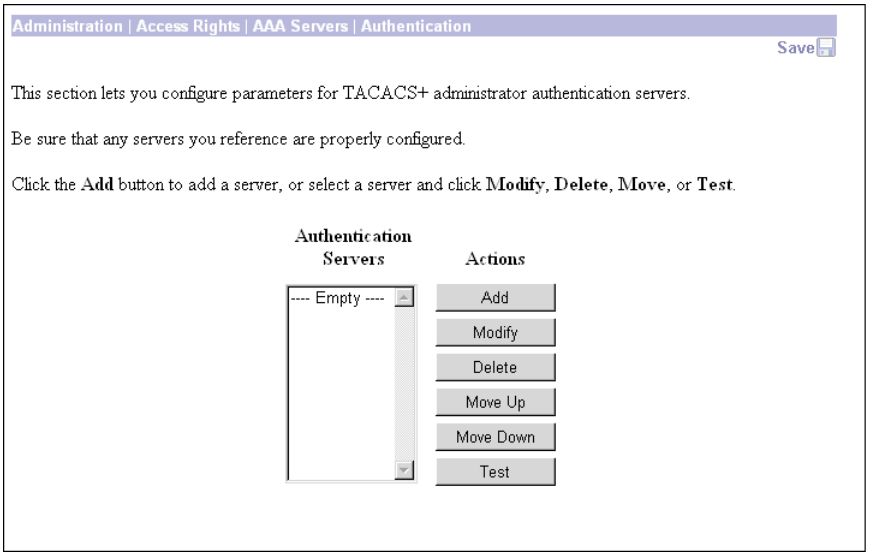


To configures TACACS+ servers, click **Authentication--authentication servers**.

Administration | Access Rights | AAA Servers | Authentication

The Manager displays the Administration | Access Rights | AAA Servers | Authentication screen. This screen lets you add, modify, delete, or change the priority order of TACACS+ administrator authentication servers.

Figure 8-8 Administration | Access Rights | AAA Servers | Authentication Screen



Authentication Servers

The Authentication Servers list shows the configured TACACS+ servers, in priority order. Each entry shows the server identifier. If no servers have been configured, the list shows --Empty--. The first server of each type in the list is the primary TACACS+ server, the rest are backup.

Add / Modify / Delete / Move / Test

To configure and add a new TACACS server, click **Add**. The Manager opens the Administration | Access Rights | AAA Servers | Add screen.

To modify parameters for an authentication server that has been configured, select the server from the list and click **Modify**. The Manager opens the Administration | Access Rights | AAA Servers | Modify screen.

To remove a server that has been configured, select the server from the list and click **Delete**.

Note There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining servers in the list.

To change the priority order for a TACACS+ server, click **Move Up** or **Move Down** to move it up or down on the list of servers configured for this group.

When you are finished configuring TACACS+ servers, click **Done**. This action includes your settings in the active configuration. The Manager returns to the Administration | Access Rights screen.

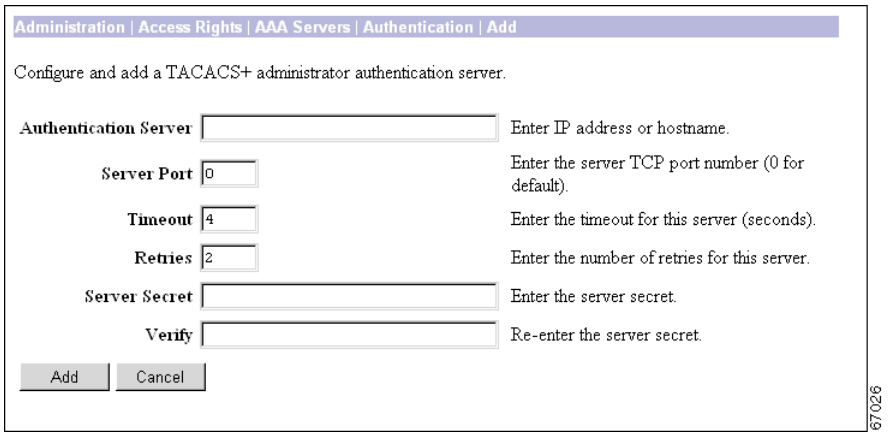
Reminder:

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

Administration | Access Rights | AAA Servers | Authentication | Add or Modify

These screens let you add or modify TACACS+ administration authentication servers.

Figure 8-9 Administration | Access Rights | AAA Servers | Add or Modify Screens



Authentication Server

Enter the IP address or host name of the TACACS+ authentication server, for example: 192.168.12.34. The maximum length is 32 characters. (If you have configured a DNS server, you can enter a host name in this field; otherwise, enter an IP address.)

Server Port

Enter the TCP port number by which you access the server. Enter `0` (the default) to have the system supply the default port number, 49.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. The minimum time is 1 second. The default time is 4 seconds. The maximum time is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next TACACS+ authentication server in the list. The minimum number of retries is 0. The default number is 2. The maximum is number is 10.

Server Secret

Enter the TACACS+ server secret (also called the shared secret), for example: C8z077f. The maximum length is 32 characters. The field shows only asterisks.

Verify

Re-enter the TACACS+ server secret to verify it. The field shows only asterisks.

Add/Apply or Cancel

To add the new server to the list of configured user TACACS+ servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Administration | Access Rights | AAA Servers | Authentication screen. Any new server appears at the bottom of the TACACS+ Authentication 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 Administration | Access Rights | AAA Servers | Authentication screen, and the TACACS+ Authentication Servers list is unchanged.

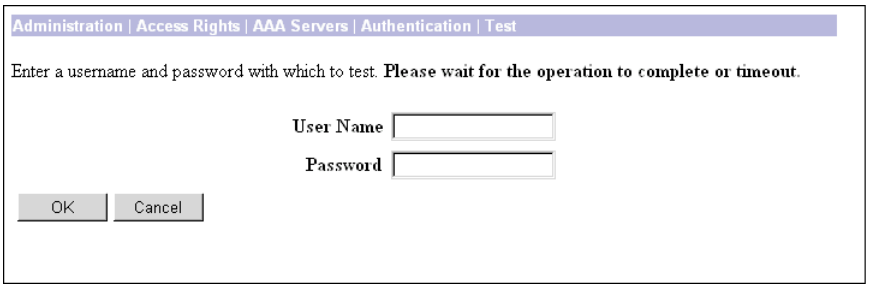
Administration | Access Rights | AAA Servers | Test

This screen lets you test a configured TACACS+ server to determine that:

- The VPN Concentrator is communicating properly with the TACACS+ server.
- The server correctly authenticates a valid administrator.
- The server correctly rejects an invalid user.

Caution Misconfiguration of TACACS+ can lock an administrator out of the Concentrator HTML interface. If that happens, you can access the Concentrator by logging in through the console port, using your administrator username and password.

Figure 8-10 Administration | Access Rights | AAA Servers | Test Screen



User Name

To test connectivity and valid authentication, enter the username for a valid user who has been configured on the TACACS+ server. The maximum length is 32 characters. Entries are case-sensitive.

To test connectivity and authentication *rejection*, enter a username that is *invalid* on the TACACS+ server.

Password

Enter the password for the username. The maximum length is 32 characters. Entries are case-sensitive. The field displays only asterisks.

OK / Cancel

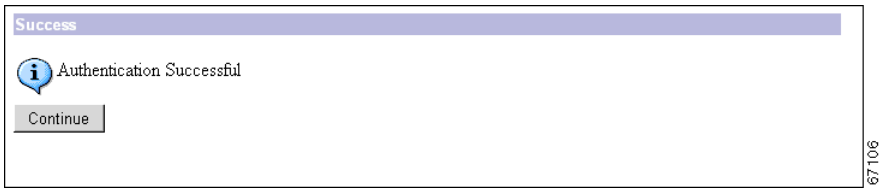
To send the username and password to the selected TACACS+ server, click **OK**. The authentication and response process takes a few seconds. The Manager displays a Success or Error screen.

To cancel the test and discard your entries, click **Cancel**. The Manager returns to the Administration | Access Rights | AAA Servers | Authentication screen.

Success (AAA)

If the authentication succeeds, the Manager displays a success screen.

Figure 8-11 Administration | Access Rights | AAA Servers | Authentication Success Screen

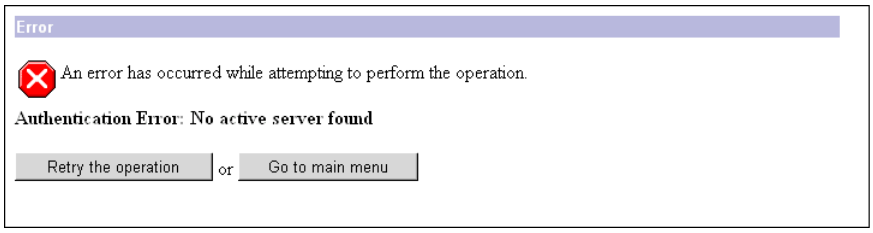


Continue

To return to the Administration | Access Rights | AAA Servers screen, click **Continue**.

If the authentication is unsuccessful for any reason—invalid username or password, no active server, etc.—the Manager displays an Error screen.

Figure 8-12 Administration | Access Rights | AAA Servers | Authentication Error Screen



Error (AAA)

To return to the Administration | Access Rights | AAA Servers | Authentication Test screen, click **Retry the operation**.

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

Note You must set a value in the AAA Access Level parameter; see Administration | Access Rights | Administrators | Modify.

File Management

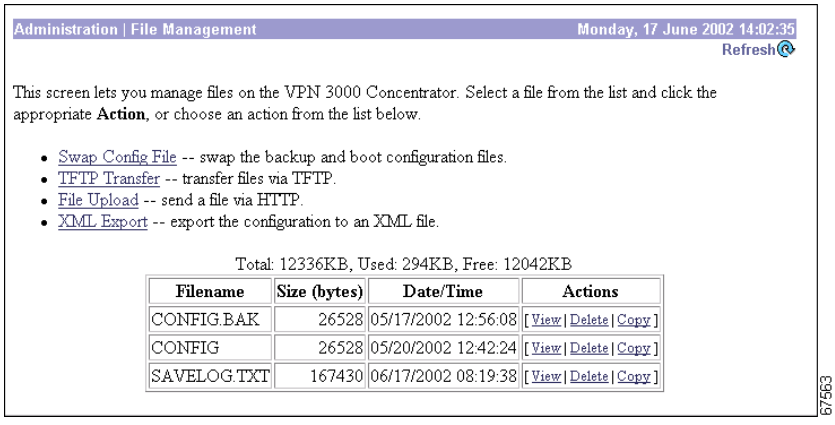
Administration | File Management

This section of the Manager lets you manage files in VPN Concentrator Flash memory. (Flash memory acts like a disk.) Such files include CONFIG, CONFIG.BAK, saved log files, and copies of any of these files that you have saved under different names.

- Swap Config File: Swap backup and boot configuration files.
- TFTP Transfer: Use TFTP to transfer files to and from the VPN Concentrator.
- File Upload: Use HTTP to transfer files to the VPN Concentrator.
- XML Export: Export the configuration to an XML file stored on the VPN Concentrator.

The screen shows a table listing all files in Flash memory, one file per table row. Use the frame scroll controls (if present) to display more files in the table.

Figure 9-1 Administration | File Management Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total, Used, Free KB

The total size of Flash memory in kilobytes, the amount used by the files listed, and the remaining free space in Flash memory.

Filename

The name of the file in Flash memory. The VPN Concentrator stores filenames as uppercase in the 8.3 naming convention.

Size (bytes)

The size of the file in bytes.

Date/Time

The date and time the file was created. The format is MM/DD/YY HH:MM:SS, with time in 24-hour notation. For example, 05/07/01 15:20:24 is May 7, 2001at 3:20:24 PM.

Actions

For a selected file, click the desired action link. The actions available to you depend on your Access Rights to Files; see the Administration | Access Rights | Administrators | Modify Properties screen.

View (Save)

Note When saving a configuration file on your PC via your browser, be sure to save the configuration file as a `.TXT` file, not an `.HTM` file. Some browser versions default to saving the file as an `.HTM` file, so you may need to change the file type. Saving the file as an `.HTM` file causes some data to be added to the top of the configuration file that is not valid configuration data. If you later upload this file to the VPN Concentrator, it will contain that invalid data and might cause unpredictable results.

To view the selected file, click **View**. 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 VPN Concentrator.

Alternatively, you can use the secondary mouse button to click **View** on this Manager screen. A pop-up menu presents choices the exact wording of which 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.
- Save Target As..., Save Link As... = Save a copy of the file on your PC. Your system prompts for a filename and location. The default filename is the same as on the VPN Concentrator.

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.

Copy

To copy a selected file within Flash memory, click **Copy**. The Manager opens a dialog box for you to enter a filename for the copy, and to confirm the action. Filenames must adhere to the 8.3 naming convention. If you confirm, the Manager refreshes the screen and shows the revised list of files.

Import

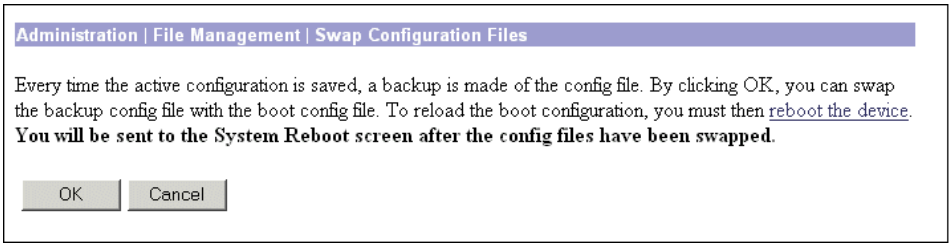
To import an XML file, click **Import**. The Manager opens the Administration | File Management | Import XML File screen and displays the file status. The Import option is only available for files with a ".XML" extension.

Administration | File Management | Swap Configuration 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 9-2 Administration | File Management | Swap Configuration 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.

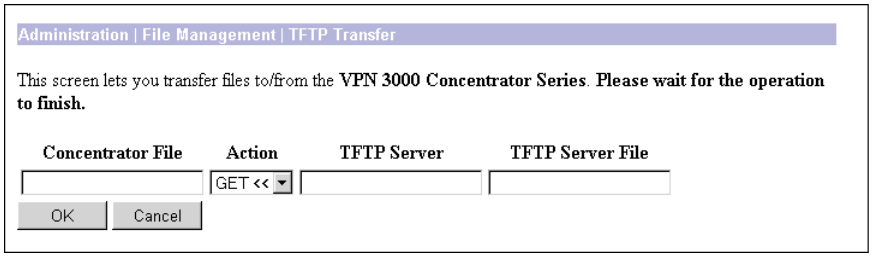
Administration | File Management | TFTP Transfer

This screen lets you use TFTP (Trivial File Transfer Protocol) to transfer files to and from VPN Concentrator Flash memory. (Flash memory acts like a disk.) The VPN Concentrator acts as a TFTP client for these functions, accessing a TFTP server running on a remote system. All transfers are made in binary (octet) mode, and they copy—rather than move—files.

To use these functions, you must have Access Rights to Read/Write Files. See the Administration | Access Rights | Administrators | Modify Properties screen.

You can list, view, and manage VPN Concentrator files on the Administration | File Management | Files screen.

Figure 9-3 Administration | File Management | TFTP Transfer Screen



Concentrator File

Enter the name of the file on the VPN Concentrator. This filename must conform to the 8.3 naming convention.

Action

Click the **Action** drop-down menu button and choose the TFTP action:

- GET << = Get a file from the remote system. Copy a file from the remote system to the VPN Concentrator.
- PUT >> = Put a file on the remote system. Copy a file from the VPN Concentrator to the remote system.

TFTP Server

Enter the IP address or host name of the remote system running the TFTP server. (If you configured a DNS server, you can enter a host name; otherwise, enter an IP address.)

TFTP Server File

Enter the name of the file on the remote system. This filename must conform to naming conventions applicable to the remote system. *Do not include a path*; the configuration of the remote TFTP server determines the location (path) of the file.

Caution If either filename is the same as an existing file, TFTP overwrites the existing file without asking for confirmation.

OK / Cancel

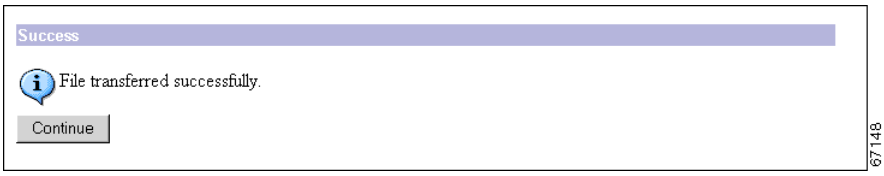
To transfer the file, click **OK**. The Manager pauses during the transfer, which might take a few moments; *please wait for the operation to finish*. The Manager then displays either a Success or Error screen.

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

Success (TFTP)

If the TFTP transfer is successful, the Manager displays a Success screen.

Figure 9-4 Administration | File Management | TFTP Transfer | Success Screen



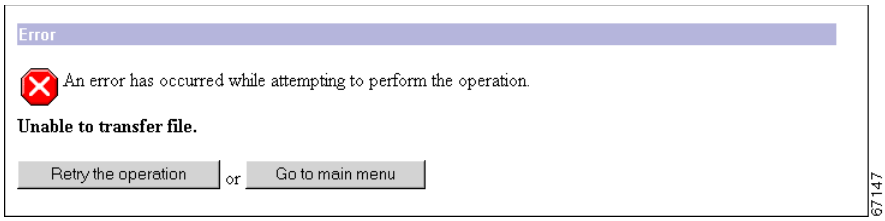
Continue

To return to the Administration | File Management | TFTP Transfer screen, click **Continue**.

Error (TFTP)

If the TFTP transfer is unsuccessful for any reason—no such file, incorrect action, remote system unreachable, TFTP server not running, incorrect server address, etc.—the Manager displays an Error screen.

Figure 9-5 Administration | File Management | TFTP Transfer | Error Screen



To return to the Administration | File Management | TFTP Transfer screen, click **Retry the operation**.

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

Administration | File Management | File Upload

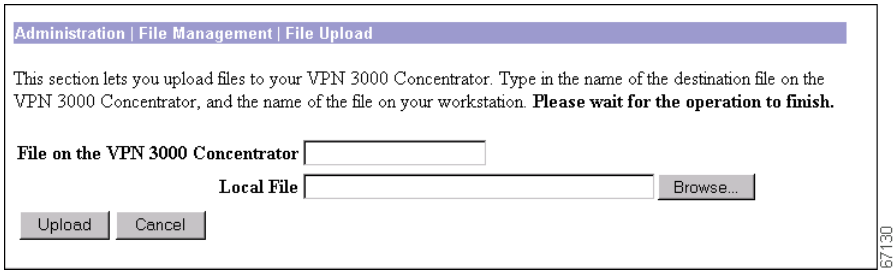
This screen lets you use HTTP (Hypertext Transfer Protocol) to transfer a configuration file from your PC—or a system accessible from your PC—to the VPN Concentrator Flash memory.

This function provides special handling for configuration (config) files. If the uploaded file has the VPN Concentrator 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 Access Rights to Read/Write Files. See the Administration | Access Rights | Administrators | Modify Properties screen.

Be sure there is sufficient space in Flash memory for the new file. You can list, view, and manage VPN Concentrator files, and check space available, on the Administration | File Management | Files screen.

Figure 9-6 Administration | File Management | File Upload Screen



File on VPN 3000 Concentrator Series

Enter the name for the file on the VPN Concentrator. This filename must conform to the 8.3 naming convention. See the previous discussion about special handling for config files.

Local File / Browse...

Enter the name of the file on your PC. In a Windows environment, enter the complete pathname using MS-DOS syntax, for example: c:\vpn3000\config0077. You can also click the **Browse** button to open a file navigation window, find the file, and select it.

Upload / Cancel

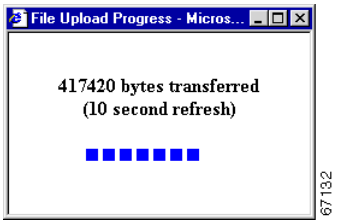
To upload the file to the VPN Concentrator, click **Upload**. The Manager opens the File Upload Progress window.

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 | File Management 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 9-7 Administration | File Management | File Upload Progress Window

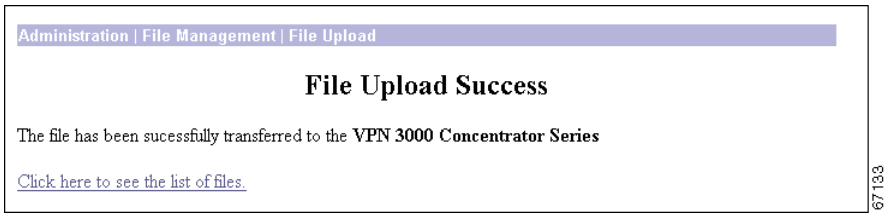


When the upload is finished, or if the upload is cancelled, the progress window closes.

File Upload Success

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

Figure 9-8 Administration | File Management | File Upload Success Screen



To go to the Administration | File Management | Files 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 might be full, or the file transfer might have been interrupted or cancelled.

Figure 9-9 Administration | File Management | File Upload Error Screen

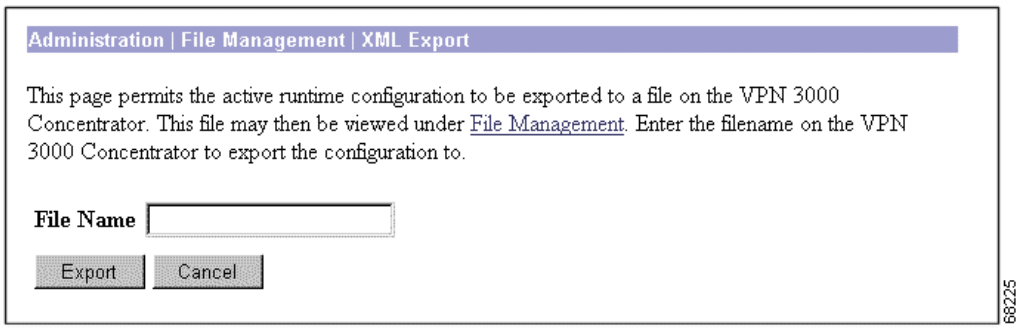
Click the link—**Click here to see the list of files**—to go to the Administration | File Management | Files screen and examine space and files in Flash memory.

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

Administration | File Management | XML Export

This screen lets you export the active runtime configuration from the VPN Concentrator to an XML file on the VPN 3000 Concentrator. You can then view, delete, copy, or import this file on the Administration | File Management screen.

Figure 9-10 Administration | File Management | XML Export Screen



File Name

Specify the file name in the **File Name** field. Click **Export** to export the configuration to that file on the VPN 3000 Concentrator.

Export/Cancel

Click **Export** to save the configuration to the named file. Click **Cancel** if you do not want to save the configuration to the file.

CHAPTER 10

Certificate Management

Digital certificates are a form of digital identification used for authentication. A digital certificate contains information that identifies a device or user, such as the name, serial number, company, department, or IP address. Certificate Authorities (CAs) issue digital certificates in the context of a Public Key Infrastructure (PKI), which uses public-key/private-key encryption to ensure security. CAs are trusted authorities that "sign" certificates to verify their authenticity, thus guaranteeing the identity of the device or user.

A *CA certificate* is one used to sign other certificates. A CA certificate that is self-signed is called a *root certificate*; one issued by another CA certificate is called a *subordinate certificate*. CAs also issue *identity certificates*, which are the certificates for specific systems or hosts.

For authentication using digital certificates, there must be at least one identity certificate (and its root certificate) on a given VPN Concentrator; there may be more. The maximum number of CA and identity certificates allowed depends on the VPN Concentrator model. Model 3005 allows a maximum of 6 root or subordinate CA certificates (including supporting RA certificates) and 2 identity certificates. The other VPN Concentrator models allow a maximum of 20 root or subordinate CA certificates (including supporting RA certificates) and 20 identity certificates.

The VPN Concentrator 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.

The VPN Concentrator stores digital certificates and private keys in Flash memory. You do not need to click **Save Needed** to store them, and they are not visible under Administration | File Management. All stored private keys are encrypted.

After you install an identity certificate on the VPN Concentrator, it is available in the Digital Certificate list for configuring IPSec LAN-to-LAN connections and IPSec SAs. See Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN and Configuration | Policy Management | Traffic Management | Security Associations.

You can also configure the VPN Concentrator to store certificate revocation list (CRL) information in volatile memory (RAM). CRL caching can potentially speed up the process of verifying the revocation status of certificates. With CRL caching enabled, when the VPN Concentrator needs to check the revocation status of a certificate, it first checks whether the required CRL exists in the cache and has not expired. Then the VPN Concentrator checks the serial number of the certificate against the list of revoked serial numbers in the CRL. If a match exists, the authentication fails. For detailed information about CRL caching, see the section "Enabling CRL Checking and Caching".

The VPN Concentrator 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 the "Installing the SSL Certificate in your Browser" section in Chapter 1 of the *VPN 3000 Series Concentrator Reference Volume I: Configuration*. See also Configuration | System | Management Protocols | HTTP/HTTPS and Telnet, and Configuration | System | Management Protocols | SSL.

The Role of Time

Digital certificates are time-sensitive in the following ways:

- Digital certificates indicate the time frame during which they are valid. Therefore, it is essential that the time on the VPN Concentrator is correct and synchronized with network time.
- You must complete the enrollment and certificate installation process within one week of generating the request. If you do not, the pending request is deleted.

Maximum Number of Certificates

For authentication with digital certificates, a VPN Concentrator must have at least one CA certificate and one identity certificate, but it can have more. The model 3005 can have six root or subordinate CA certificates and two identity certificates. The other VPN Concentrator models can have 20 root or subordinate CA certificates and 20 identity certificates.

Configuring Digital Certificates: SCEP and Manual Methods

To use digital certificates for authentication, you first enroll with a Certificate Authority (CA), and obtain and install a CA certificate on the VPN Concentrator. Then you enroll and install an identity certificate from the same CA.

You can enroll and install digital certificates on the VPN Concentrator in either of two ways:

- Using Cisco's Simple Certificate Enrollment Protocol (SCEP).

  SCEP is a secure messaging protocol that requires minimal user intervention. SCEP is the quicker method, and it lets you to enroll and install certificates using only the VPN Concentrator Manager. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet.

- Manually, exchanging information with the CA directly.

  The manual method involves more steps. You can do some of the steps using the Manager. Other steps require that you exchange information with the CA directly. You deliver your enrollment request and receive the certificate from the CA via the Internet, email, or a floppy disk.

Note If you install a CA certificate using the manual method, you must also use the manual method to request identity or SSL certificates from that CA. Conversely, to request identity and SSL certificates using SCEP, you must first use SCEP to obtain the CA certificate.

Tasks Summary

Whether you use SCEP or the manual method, you perform the following tasks to obtain and install certificates:

1. Obtain and install one or more CA certificate(s).
2. Create an enrollment request for one or more identity certificates.
3. Request an identity certificate from the same CA that issued the CA certificate(s).
4. Install the identity certificate on the VPN Concentrator.
5. Enable CRL checking and caching.
6. Enable certificates.

About the Documentation

The print version of this guide provides step-by-step examples of configuring digital certificates using SCEP and manually, and with both LAN-to-LAN and remote access connections, beginning with the next section, "Managing Certificates with SCEP."

The online Help and the print version both provide detailed information on the parameters for each of the Manager screens that you use to configure digital certificates.

Managing Certificates with SCEP

The following sections provide step-by-step instructions for using SCEP to enroll and install digital certificates.

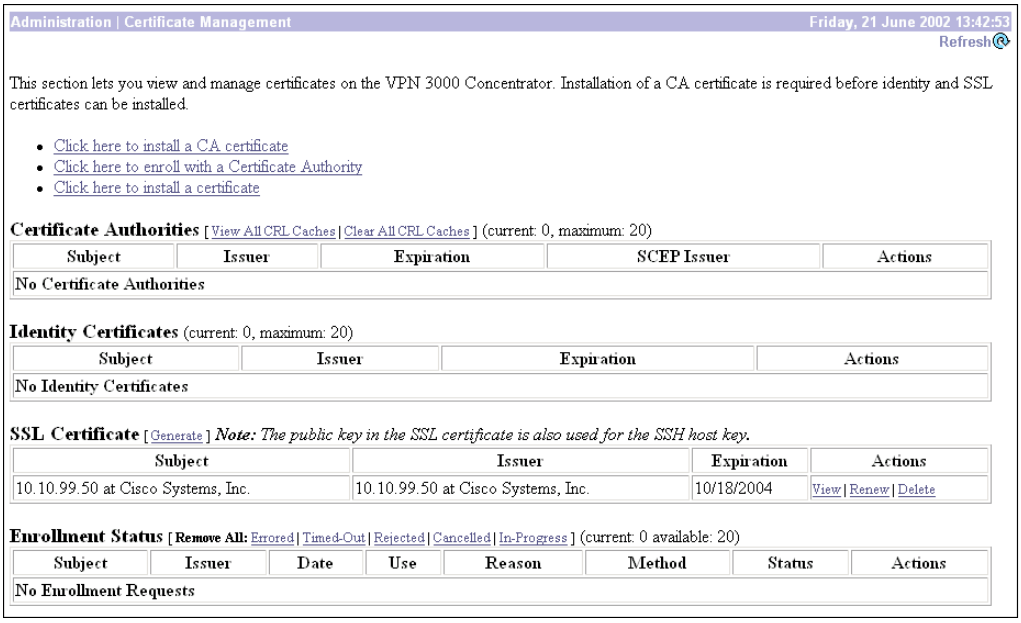
Obtaining and Installing CA Certificates Automatically Using SCEP

To use SCEP to enroll for identity or SSL certificates, you must also use SCEP to obtain the associated CA certificate. The Manager does not let you enroll for a certificate from a CA unless that CA certificate was installed using SCEP. A certificate that is obtained via SCEP and therefore capable of issuing other SCEP certificates, is called *SCEP-enabled*.

Tip To obtain CA certificates using SCEP, you need to know the URL of your CA. Find out your CA's SCEP URL before beginning the following steps.

Step 1 Using the VPN Concentrator Manager, display the Administration | Certificate Management screen. (See Figure 10-1.)

Figure 10-1 Administration | Certificate Management Screen

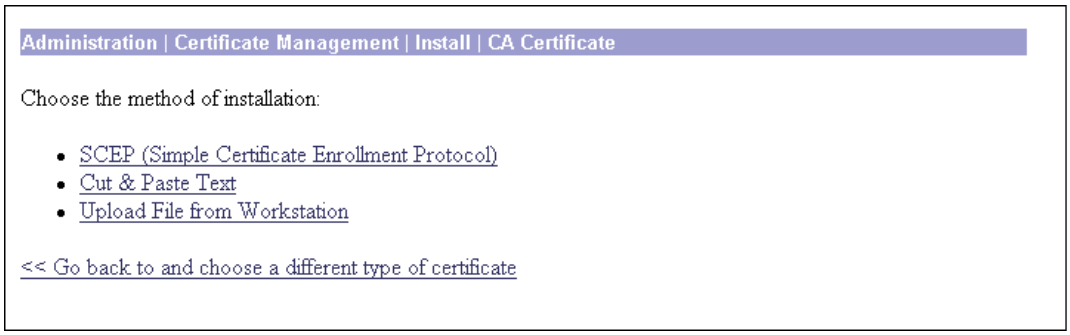


Step 2 Click **Click here to install a CA certificate**.

Note The Click here to install a CA certificate option is available from this window only when no CA certificates are installed on the VPN Concentrator. If you do not see this option, click **Click here to install a certificate.** The Manager displays the Administration | Certificate Management | Install screen. Then click **Install CA Certificate**.

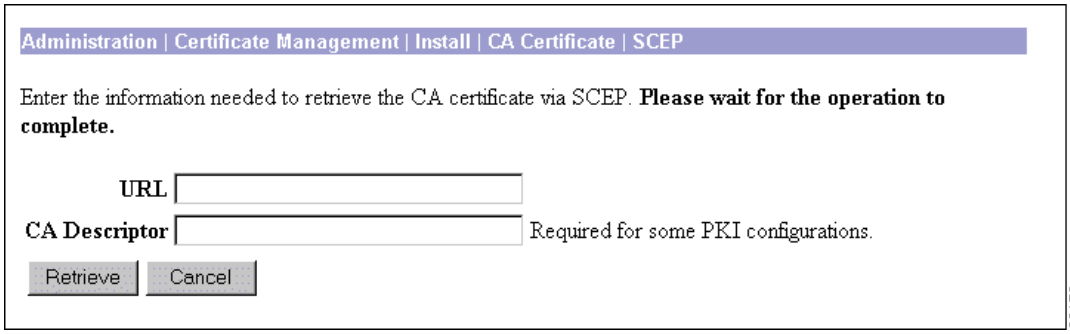
The Manager displays the Administration | Certificate Management | Install | CA Certificate screen. (See Figure 10-2.)

Figure 10-2 Administration | Certificate Management | Install | CA Certificate



Step 3 Click **SCEP (Simple Certificate Enrollment Protocol)**. The Manager displays the Administration | Certificate Management | Install | CA Certificate | SCEP screen. (See Figure 10-3.)

Figure 10-3 The Administration | Certificate Management | Install | CA Certificate | SCEP Screen



Step 4 Fill in the fields and click Retrieve.

- URL: Enter the URL of the CA's SCEP interface.
- CA Descriptor: Some CAs use descriptors to further identify the certificate. If your CA gave you a descriptor, enter it here. Otherwise enter a descriptor of your own. You must enter something in this field.
- Retrieve / Cancel:
  - To retrieve a CA certificate from the CA and install it on the VPN Concentrator, click **Retrieve**.
  - To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See Figure 10-1.)

The Manager installs the CA certificate on the VPN Concentrator and displays the Administration | Certificate Management screen. Your new CA certificate appears in the Certificate Authorities table.

Changing SCEP Parameters

To change SCEP parameters for a certificate, follow these steps:

Step 1 In the Administration | Certificate Management screen, click the **SCEP** link associated with the certificate (under Actions in the Certificate Authorities table). The Administration | Certificate Management | Configure CA Certificate screen displays.

Step 2 Edit one or more parameters.

- Enrollment URL: Enter the URL where the VPN Concentrator should send SCEP enrollment requests made to this CA. The default value of this field is the URL used to download this CA certificate.
- Polling Interval: If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request enters polling mode. In polling mode, the VPN Concentrator re-sends the certificate request to the CA for a specified period until the CA responds or the process times out.

  Enter the number of minutes the VPN Concentrator should wait between re-sends. The minimum number of minutes is 1; the maximum number of minutes is 60. The default value is 1
- Polling Limit: Enter the number of times the VPN Concentrator should re-send an enrollment request if the CA does not issue the certificate immediately. The minimum number of re-sends is 0; the maximum number is 100. If you did not want any polling limit, (in other words, you want infinite re-sends), enter `none`.

Step 3 Click **Apply**.

Note If you have trouble enrolling or installing digital certificates via SCEP, enable both the CLIENT and CERT event classes to assist in troubleshooting.

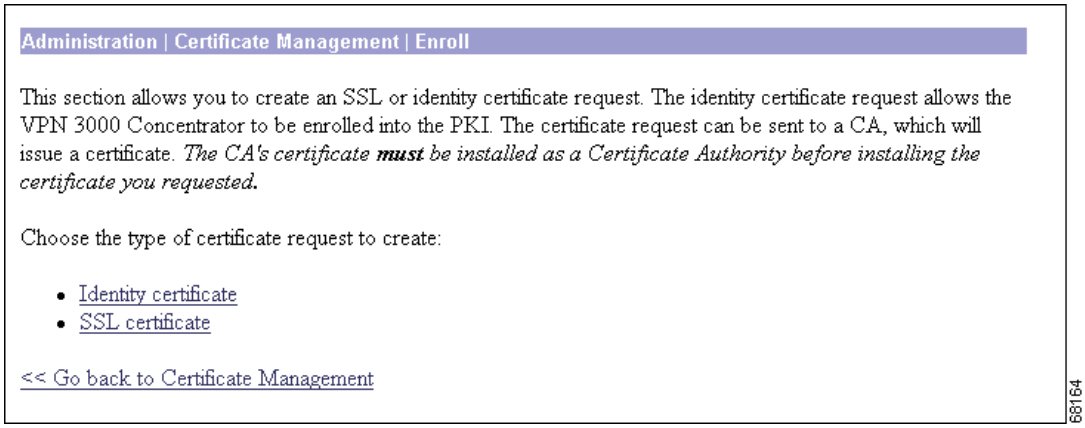
Enrolling and Installing Identity Certificates Automatically Using SCEP

Follow these steps for each identity certificate you want to obtain:

Step 1 Display the Administration | Certificate Management screen. (See Figure 10-1.)

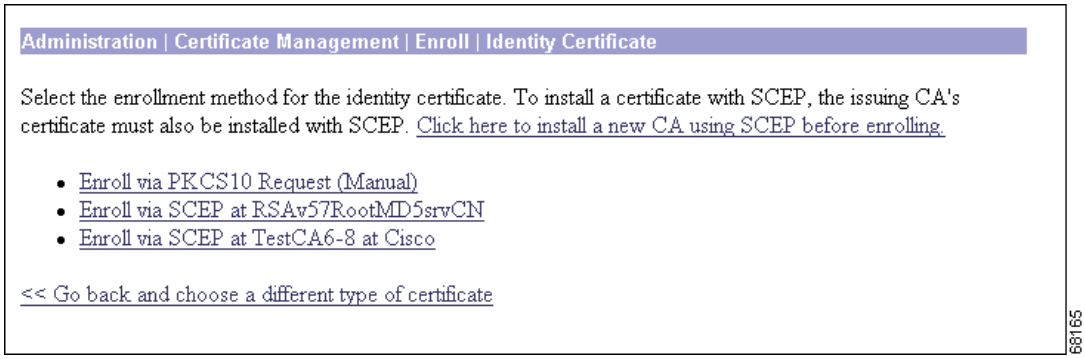
Step 2 Click **Click here to enroll with a Certificate Authority**. The Manager displays the Administration | Certificate Management | Enroll screen. (See Figure 10-4.)

Figure 10-4 Administration | Certificate Management | Enroll Screen



Step 3 Click **Identity Certificate**. The Manager displays the Administration | Certificate Management | Enroll | Identity Certificate screen. (See Figure 10-5.)

Figure 10-5 Administration | Certificate Management | Enroll | Identity Certificate Screen

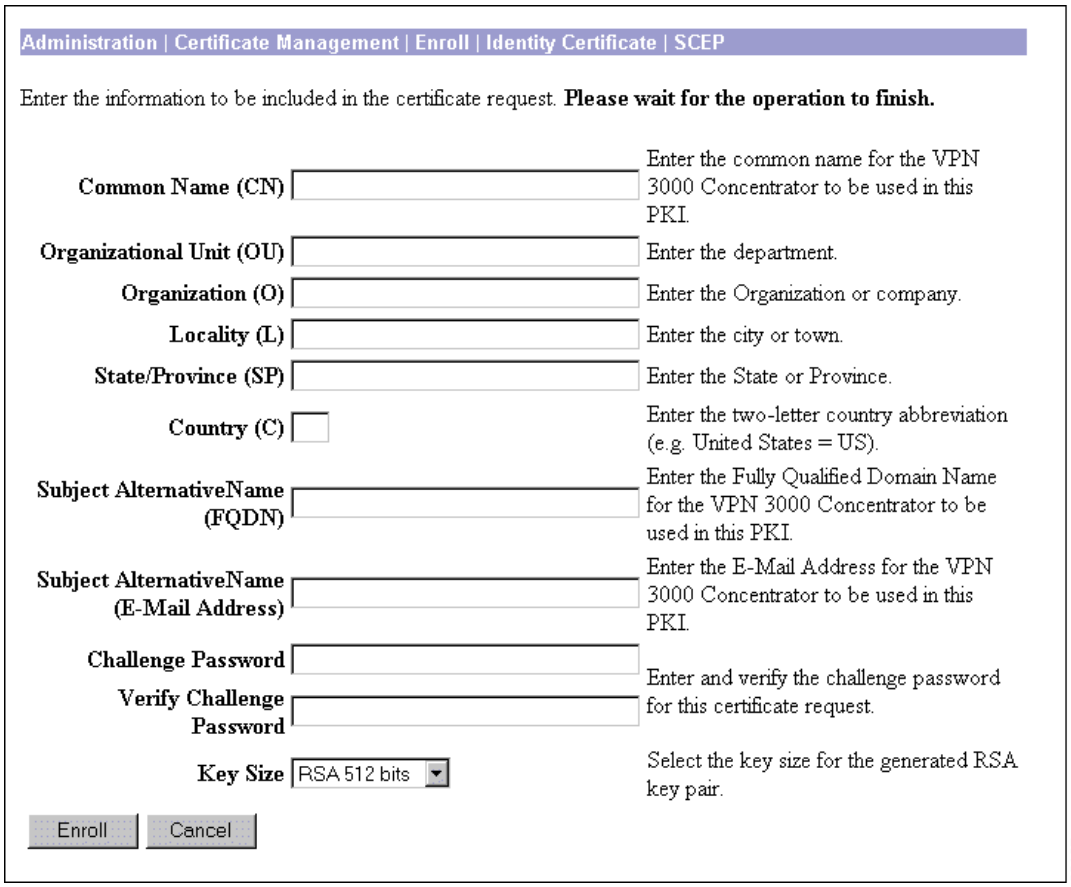


Notice that a link appears corresponding to each SCEP-enabled CA certificate on the VPN Concentrator. The title of the link depends on the name of the CA certificate: Enroll via SCEP at *Certificate Name*. For example, if you have a CA certificate on your VPN Concentrator named "TestCA6-8," the following link appears: Enroll via SCEP at TestCA6-8.

If you do not see any Enroll via SCEP options, there are no SCEP-enabled CA certificates on the VPN Concentrator. Follow the steps in the "Obtaining and Installing CA Certificates Automatically Using SCEP" section to obtain a CA certificate via SCEP before you proceed.

Step 4 Click **Enroll via SCEP at *Certificate Name***. The Administration | Certificate Management | Enroll | Identity Certificate | SCEP screen displays. (See Figure 10-6.)

Figure 10-6 Administration | Certificate Management | Enroll | Identity Certificate | SCEP Screen

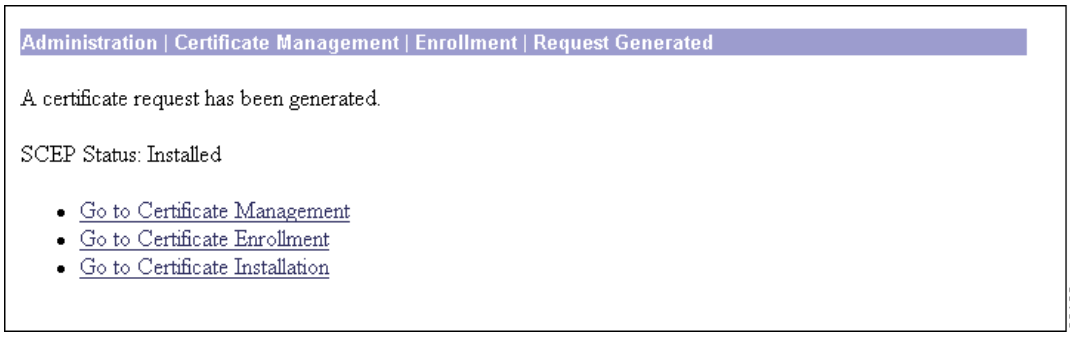


Step 5 Fill in the fields and click **Enroll**. (For information on the fields on this screen, see Table 10-2.) The VPN Concentrator sends the certificate request to the CA.

If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request could enter polling mode. In polling mode, the VPN Concentrator re-sends the certificate request to the CA a specified number of times at regular intervals until the CA responds or the process times out. (For information on configuring the polling limit and interval, see the Administration | Certificate Management | Configure CA Certificate screen.) The certificate request appears in the Enrollment Status table on the Administration | Certificate Management screen until the CA responds. Once the CA responds and issues the certificate, the VPN Concentrator installs it automatically.

If the CA responds immediately, the Manager installs the identity certificate on the VPN Concentrator and displays the Administration | Certificate Management | Enrollment | Request Generated screen. (See Figure 10-7.)

Figure 10-7 Administration | Certificate Management | Enrollment | Request Generated Screen



Click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen. Your new identity certificate appears in the Identity Certificates table.

Enrolling and Installing Certificates Manually

The following sections provide step-by-step instructions for enrolling and installing digital certificates manually.

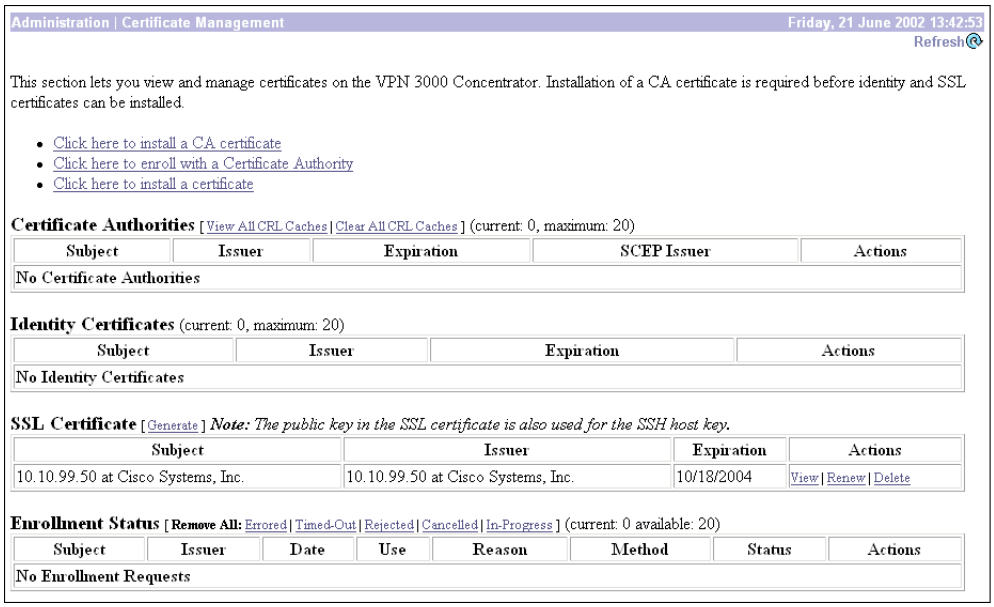
Obtaining and Installing CA Certificates Manually

Certificate authorities are trusted entities that "sign" certificates to verify their authenticity. A CA certificate is one used to sign other certificates. You obtain CA certificates according to the procedures of individual CAs.

Step 1 You can obtain a CA certificate via email, floppy disk, or over the Internet. Retrieve a CA certificate according to the policies and procedures of your CA, and download it to your management work station.

Step 2 To install the CA certificate, begin at the VPN Concentrator Manager **Administration | Certificate Management** screen. When you begin, there are no entries in the Certificate Authorities, Identity Certificates, SSL Certificates, or Enrollment Status fields.

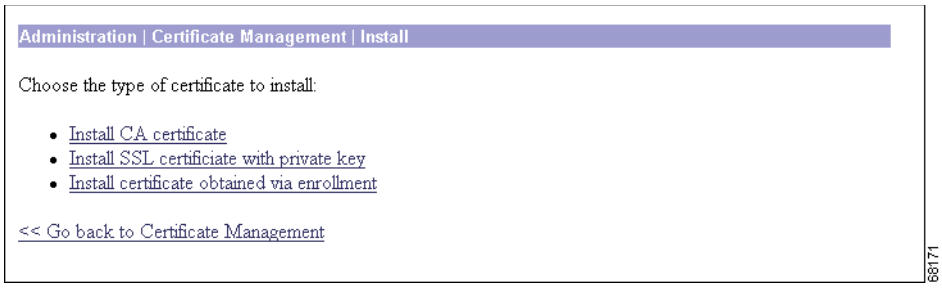
Figure 10-8 Administration | Certificate Management Screen



Step 3 Click **Click here to install a CA certificate**. The Administration | Certificate Management | Install screen displays.

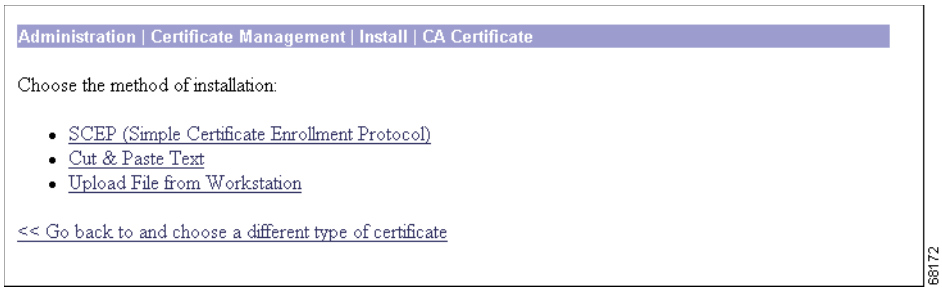
Note The *Click here to install a CA certificate* option is available from this screen only when no CA certificates are installed on the VPN Concentrator. If you do not see this option, click **Click here to install a certificate.** The Manager displays the Administration | Certificate Management | Install screen. Then click **Install CA certificate**.

Figure 10-9 Administration | Certificate Management | Install Screen



Step 4 Click **Install CA Certificate**. The Administration | Certificate Management | Install | CA Certificate screen displays.

Figure 10-10 Administration | Certificate Management | Install | CA Certificate Screen

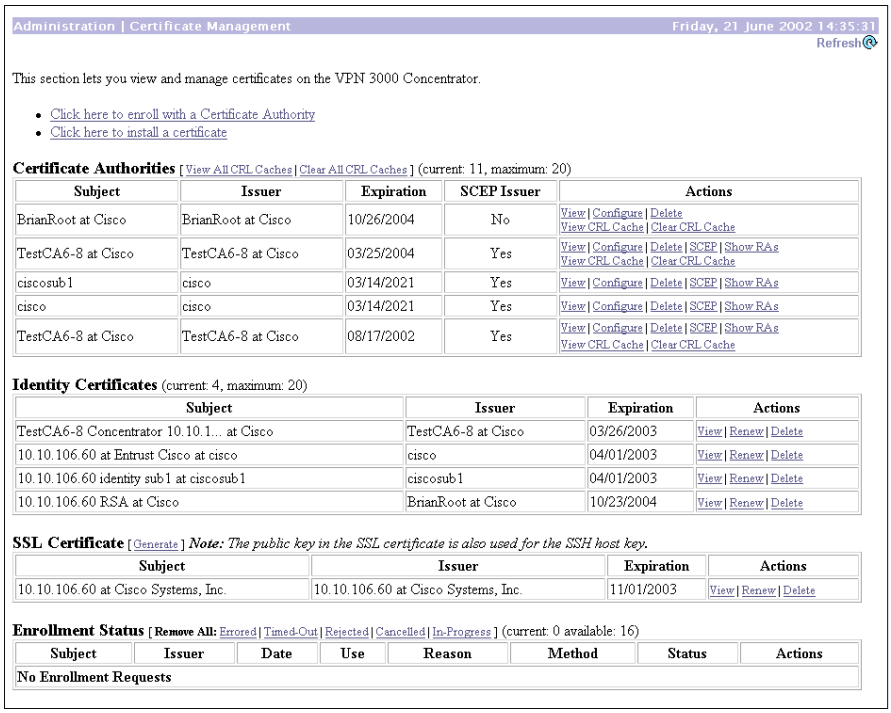


Step 5 Click **Upload File from Workstation** or **Cut and Paste Text,** depending on how you have retrieved the CA certificate. The Manager displays a screen appropriate to your choice.

Step 6 Include certificate information according to your chosen method.

Step 7 Click **Install**. The Manager installs the CA certificate on the VPN Concentrator. You return to the Administration | Certificate Management screen, which now displays the newly installed CA certificate.

Figure 10-11 Administration | Certificate Management Screen with CA Certificates Installed



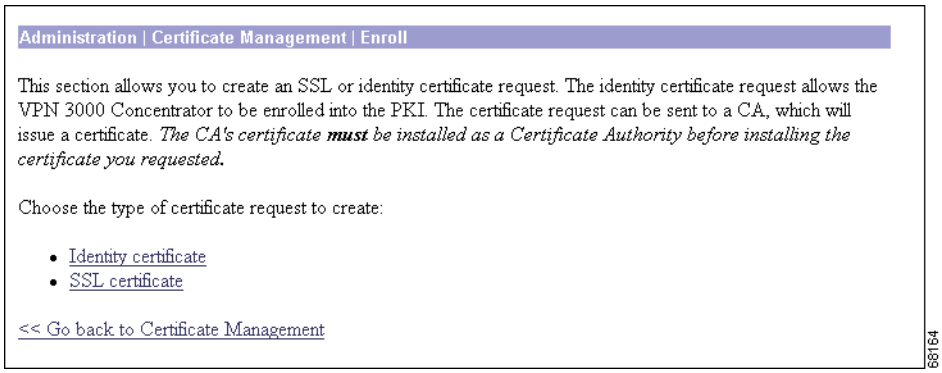
Creating an Enrollment Request for an Identity Certificate Manually

An enrollment request for an identity certificate consists of a base 64 encoded PKCS#10 file that the VPN Concentrator generates based on information you provide in the steps that follow.

Note You must get the identity certificate for a LAN-to-LAN connection from the same CA that issued its CA certificate.

Step 1 In the Administration | Certificate Management screen (Figure 10-1), click **Click here to enroll with a Certificate Authority.** The Administration | Certificate Management | Enroll screen displays.

Figure 10-12 Administration | Certificate Management | Enroll Screen

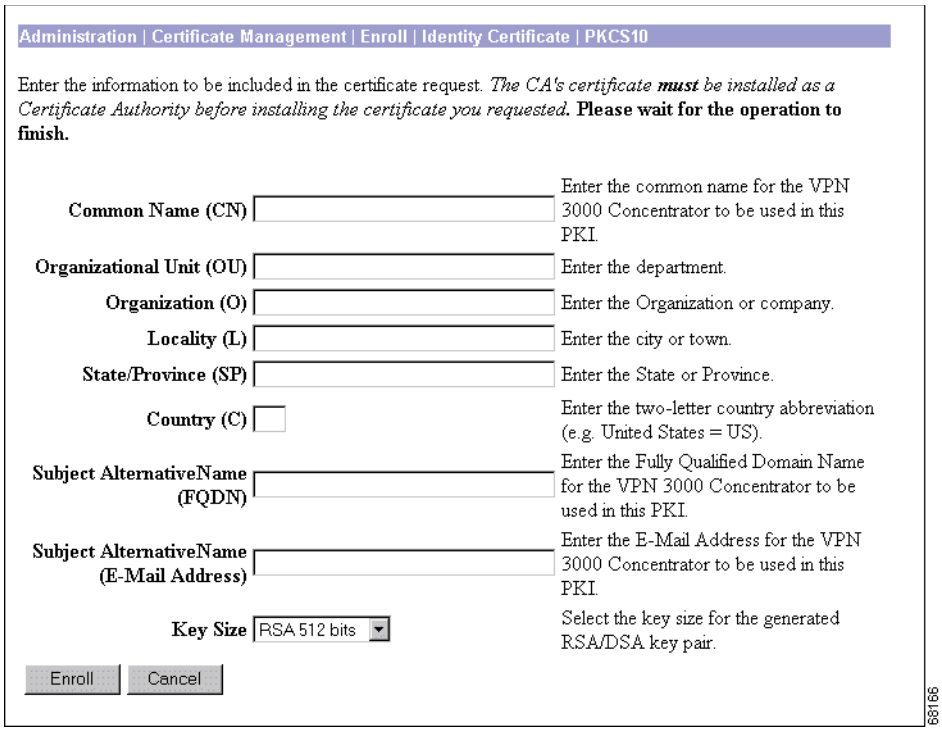


Step 2 Click **Identity certificate**. The Administration | Certificate Management | Enroll | Identity Certificate screen displays.

Figure 10-13 Administration | Certificate Management | Enroll | Identity Certificate Screen

Step 3 Click **Enroll via PKCS10 Request (Manual)**. The Administration | Certificate Management | Enroll | Identity Certificate | PKCS10 Screen displays.

Figure 10-14 Administration | Certificate Management | Enroll | Identity Certificate | PKCS10 Screen

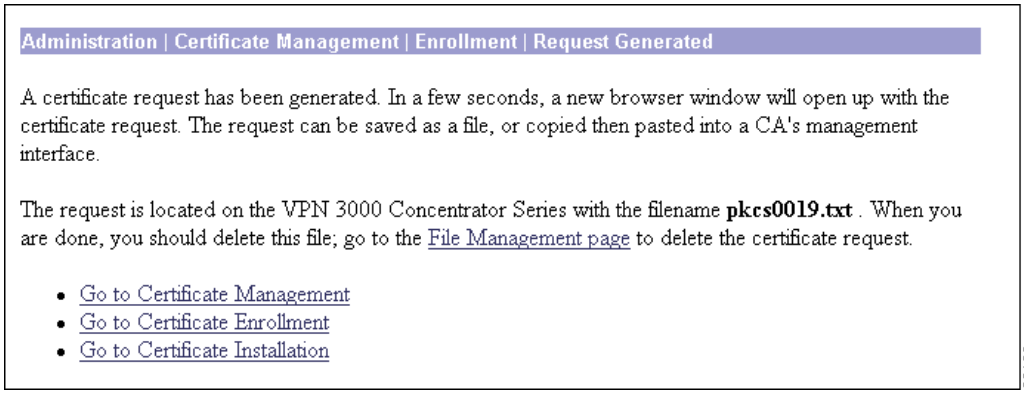


Step 4 Enter values in each of the fields on this screen. Table 10-2 defines these fields.

Step 5 When you have finished, click **Enroll**.

The Administration | Certificate Management | Enroll | Request Generated screen displays (Figure 10-15).

Figure 10-15 Administration | Certificate Management | Enroll | Request Generated Screen

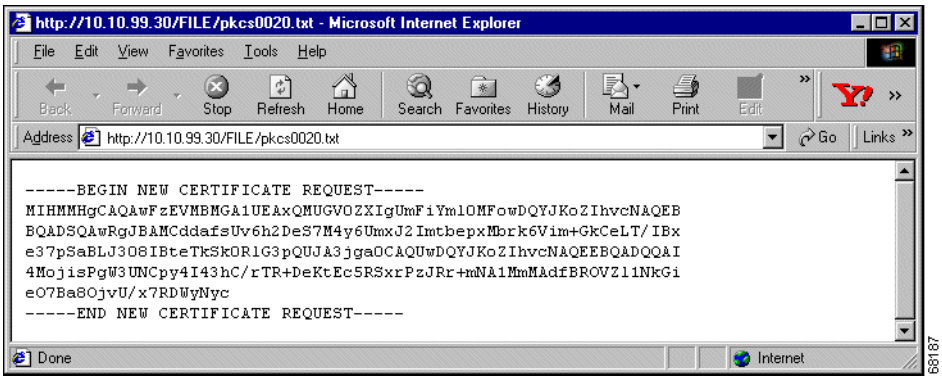


The Manager displays this screen when the system has successfully generated a certificate request.

Note You must complete the enrollment and certificate installation process within one week of generating the request. If you do not, the pending request is deleted.

As the screen text indicates, within a few seconds, a browser window opens with the certificate request.

Figure 10-16 Example of a Certificate Request



You have generated a base 64 encoded PKCS#10 file (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 browser (pkcs*NNNN*.txt).

In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN Concentrator in encrypted form.

Step 6 Save the request in one of the following ways:

- Save the request to a file (to transmit the file to the CA via email or floppy disk).
- Select and copy the request to the clipboard, and then paste the request into an email to the CA.
- Copy and paste the request into the CA's management interface via the Internet.

Some CAs let you paste the request in a web interface, some ask you to send a file; use the method your CA requires.

Step 7 Close this browser window when you have finished.

Requesting an Identity Certificate from a CA Manually

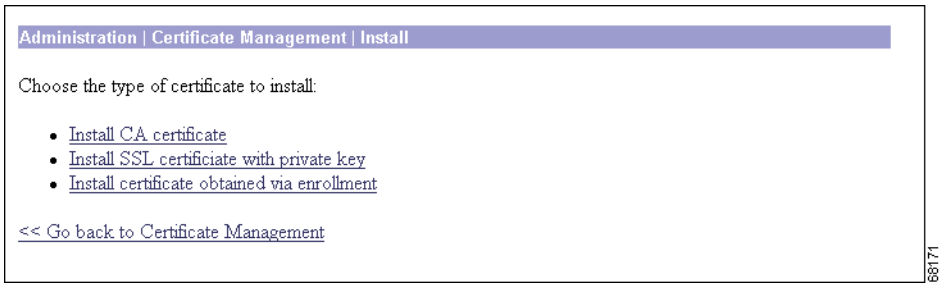
Next you submit the identity request to a CA. This must be the same CA that issued the CA certificate for this LAN-to-LAN connection. Submit the request and retrieve an identity certificate according to the procedures of your CA.

Installing the Identity Certificate on the VPN Concentrator Manually

The following steps provide instructions on installing an Identity certificate on the VPN Concentrator.

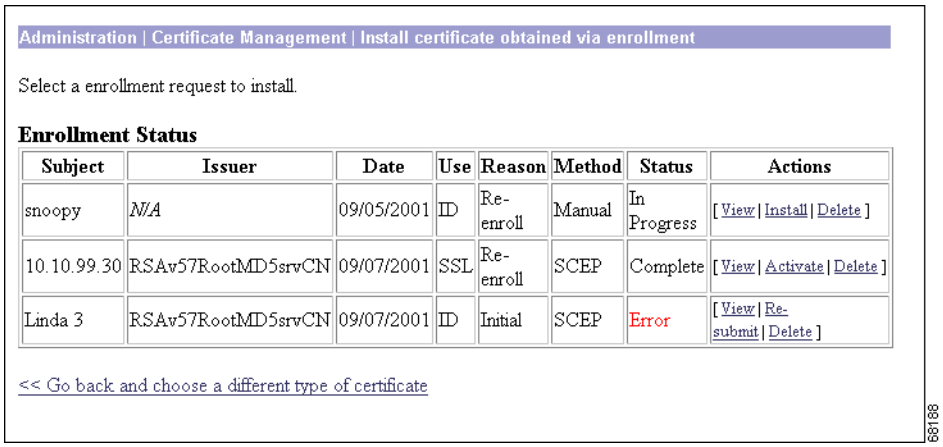
Step 1 From the Administration | Certificate Management screen, click **Click here to install a certificate** to navigate to the Administration | Certificate Management | Install screen.

Figure 10-17 Administration | Certificate Management | Install Screen



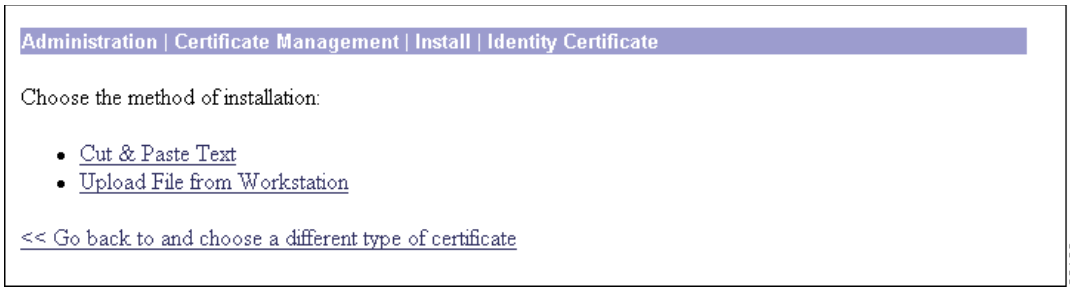
Step 2 Click **Install certificate obtained via enrollment**. The Administration | Certificate Management | Install certificate obtained via enrollment screen displays.

Figure 10-18 Administration | Certificate Management | Install certificate obtained via enrollment Screen



Step 3 In the **Actions** column of the Enrollment Status table, click **Install**. The Administration | Certificate Management | Install Identity Certificate screen displays.

Figure 10-19 Administration | Certificate Management | Install Identity Certificate Screen



Step 4 Choose either installation method: **Cut & Paste Text** or **Upload File from Workstation**.

Step 5 The Manager displays a screen appropriate to your choice. Include the certificate information according to your chosen method. Click **Install**. The Manager installs the identity certificate on the VPN Concentrator and displays the Administration | Certificate Management screen. Your new identity Certificate appears in the Identity Certificates table.

Step 6 Confirm that the Issuer fields for Certificate Authorities and Identity Certificates match for this LAN-to-LAN connection. You must get the Identity certificate and the CA certificate from the same CA.

Obtaining SSL Certificates

If you use a secure connection between your browser and the VPN Concentrator, the VPN Concentrator requires an SSL certificate. You only need one SSL certificate on your VPN Concentrator.

When you initially boot the VPN Concentrator, a self-signed SSL certificate is automatically generated. Because a self-signed certificate is self-generated, this certificate is not verifiable. No CA has guaranteed its identity. But this certificate allows you to make initial contact with the VPN Concentrator using the browser. If you want to replace it with another self-signed SSL certificate, follow these steps:

Step 1 Display the Administration | Certificate Management screen. (See Figure 10-1.)

Step 2 Click **Generate** above the SSL Certificate table. The new certificate appears in the SSL Certificate table, replacing the existing one.

If you want to obtain a *verifiable* SSL certificate (that is, one issued by a CA), follow the same procedure you used to obtain identity certificates. (See the "Enrolling and Installing Identity Certificates Automatically Using SCEP" section or the "Creating an Enrollment Request for an Identity Certificate Manually" section.) But this time, on the Administration | Certificate Management | Enroll screen, click **SSL certificate** (instead of Identity certificate).

Some web servers export their SSL certificates with the private key attached. If you have a PEM-encoded certificate with a corresponding private key that you want to install, follow the same procedure you used to obtain identity certificates. (See the "Enrolling and Installing Identity Certificates Automatically Using SCEP" section.) But this time, on the Administration | Certificate Management | Installation screen, click **Install SSL certificate with private key** (instead of Install certificate obtained via enrollment).

Enabling CRL Checking and Caching

When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a particular certificate before this time period expires. Certificates can be revoked for many reasons, such as security concerns or a change of name or association. CAs periodically issue a signed list of certificates that have been revoked and are no longer valid. This list is called a *certificate revocation list (CRL)*. To ensure that received peer certificates are valid, configure the VPN Concentrator to check them against the CRL. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the latest CRL to ensure that the certificate being verified has not been revoked.

CAs use LDAP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP access.

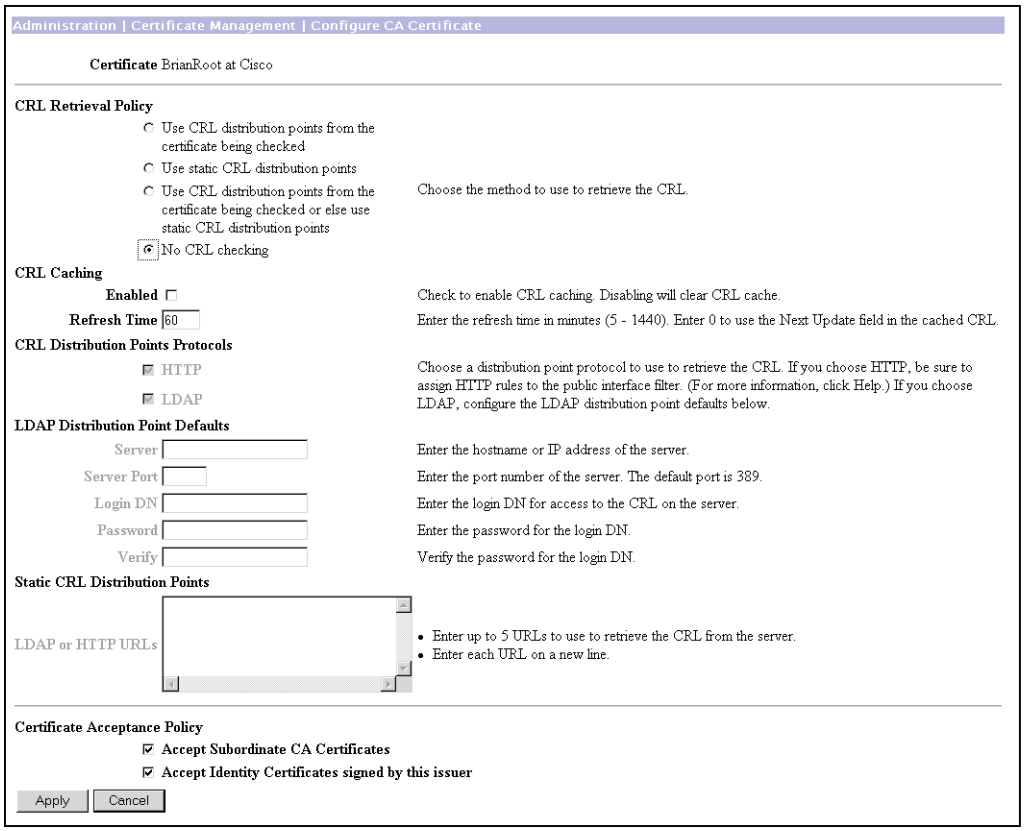
Since the system has to obtain and examine the CRL from a network distribution point, enabling CRL checking might slow system response times. Also, if the network is slow or congested, CRL checking might fail.

To avoid having to retrieve the same CRL from a CA again and again, the VPN Concentrator can store retrieved CRLs locally. Storing CRLs locally is called *CRL caching*.

Follow these steps to enable CRL checking and caching on the VPN Concentrator:

Step 1 On the Administration | Certificate Management screen, in the Certificate Authorities table, click **Configure** next to the CA certificate for which you want to enable CRL checking. The Manager displays the Administration | Certificate Management | Configure CA Certificate screen. For information on these fields, see the "Administration | Certificate Management | Configure CA Certificate" section or online Help.

Figure 10-20 Administration | Certificate Management | Configure CA Certificate Screen



Step 2 CRL checking is disabled by default. Choose the method to use to retrieve the CRL.

- If you choose to use CRL distribution points specified in the certificate being checked, be sure to specify the distribution point protocols for retrieving CRLs. If you choose the LDAP protocol, be sure to specify the LDAP distribution point defaults.
- If you choose to use static CRL distribution points, be sure to enter them under Static CRL Distribution Points further down.

Step 3 To enable CRL caching, check the **Enabled** check box. In the **Refresh Time** field, specify a time period for updating the CRL.

Step 4 Check the appropriate check boxes to indicate whether you want to accept Subordinate CA Certificates or accept Identity Certificates signed by this issuer.

Step 5 Click **Apply**. The Manager displays the Administration | Certificate Management screen.

Enabling Digital Certificates on the VPN Concentrator

Note Before you enable digital certificates on the VPN Concentrator, you must obtain at least one root and one identity certificate. If you do not have a root and an identity certificate installed on your VPN Concentrator, follow the steps in the previous sections before beginning this section.

For the VPN Concentrator to use the digital certificates you obtained, you must enable authentication using digital certificates. Table 10-1 outlines this procedure.

Table 10-1 Enabling Digital Certificates on the VPN Concentrator

For Remote Access Sessions	For IPSec LAN-to-LAN Connections
1. Edit and activate an IKE proposal.	1. Edit and activate an IKE proposal.
2. Configure an SA to use that IKE proposal and a particular identity certificate.	2. Configure the LAN-to-LAN connection to use that IKE proposal.
3. Configure the group to use that SA.	3. Configure the LAN-to-LAN connection to use a particular identity certificate.

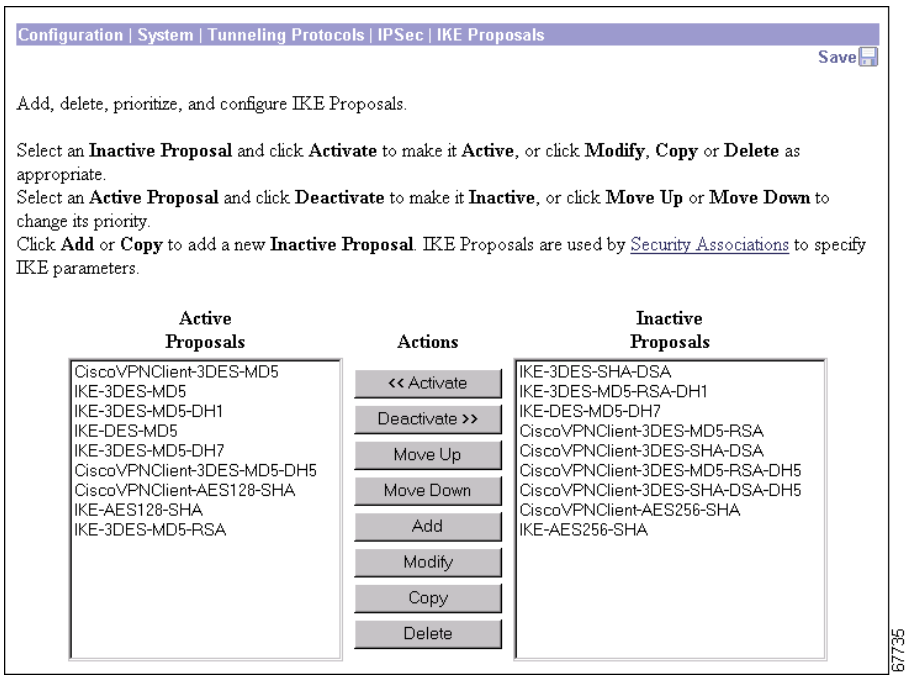
Enabling Digital Certificates for Remote Access Connections

To enable digital certificates for remote access connections, you must first edit and activate the appropriate IKE proposal:

Step 1 Display the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen. (See Figure 10-21.)

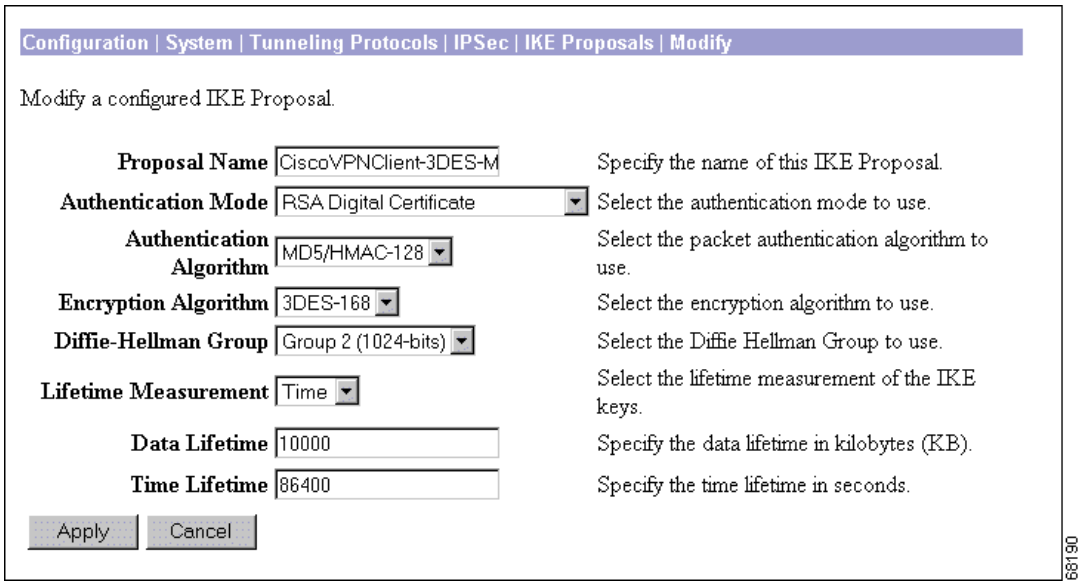
Step 2 Select an IKE proposal (or create a new one) for which you want to enable digital certificates.

Figure 10-21 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Screen



Step 3 Click **Modify** (or **Add**). The Manager displays the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify (or Add) screen. (See Figure 10-22.)

Figure 10-22 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify Screen



Step 4 Click the **Authentication Mode** drop-down menu. Choose any of the **Digital Certificates** options.

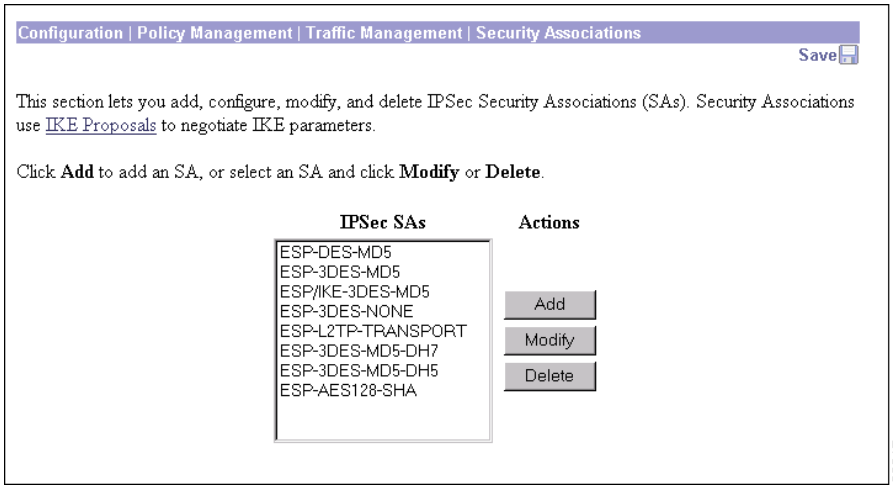
Step 5 Click **Apply** (or **Add**). The Manager returns to the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen. (See Figure 10-21.)

Step 6 Verify that the IKE proposal you just edited is in the Active Proposals column. If it is not, select the proposal and click **<< Activate**.

Next, follow these steps to configure the SA:

Step 1 Display the Configuration | Policy Management | Traffic Management | Security Associations screen. (See Figure 10-23.)

Figure 10-23 Configuration | Policy Management | Traffic Management | Security Associations Screen

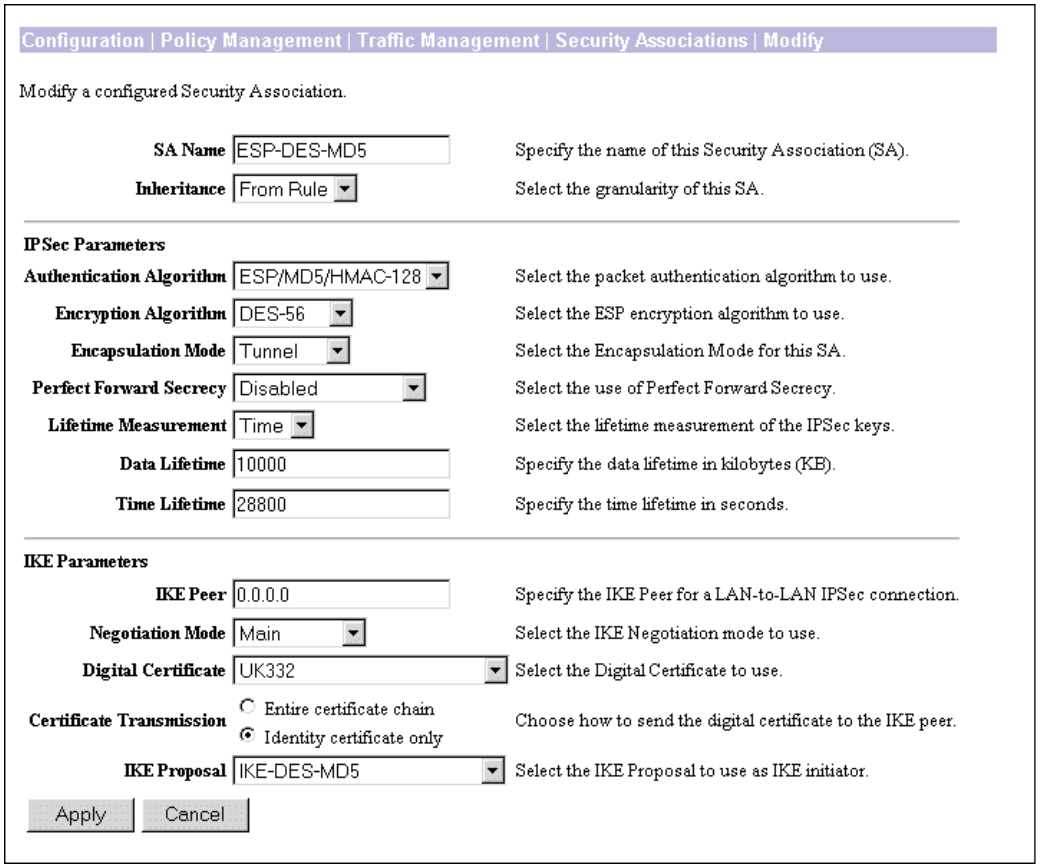


Step 2 Do one of the following:

- To edit an existing SA, select an SA on the IPSec SA list and click **Modify.**
- To create a new SA, click **Add**.

The Manager displays the Configuration | Policy Management | Traffic Management | Security Associations | Modify (or Add) screen. (See Figure 10-24.)

Figure 10-24 Configuration | Policy Management | Traffic Management | Security Associations | Modify (or Add) Screen



Step 3 Under IKE Parameters, choose the digital certificate you want to use from the **Digital Certificate** drop-down menu.

Step 4 Select a Certificate Transmission option. If you want the VPN Concentrator to send the peer the identity certificate and all issuing certificates (including the root certificate and any subordinate CA certificates), click **Entire certificate chain**. If you want to send the peer only the identity certificate, click **Identity certificate only**.

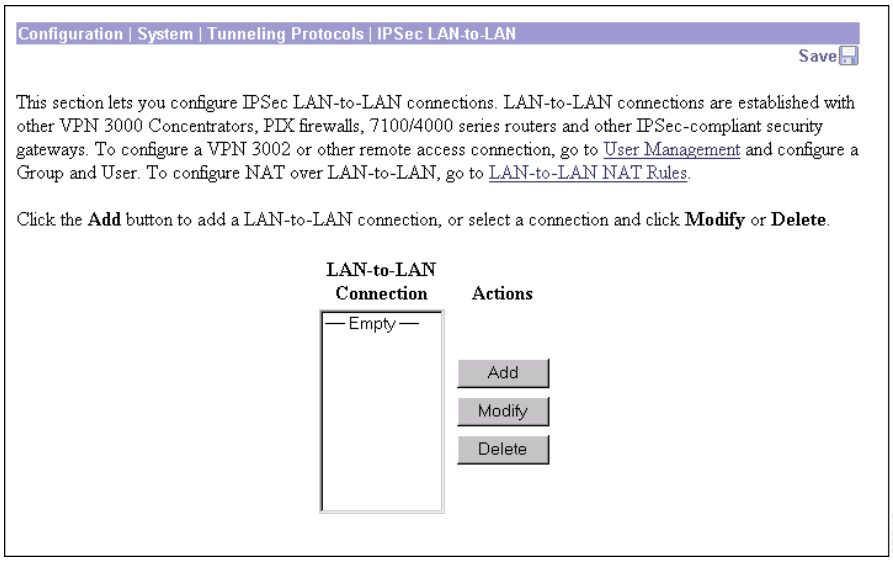
Step 5 Choose the name of the IKE proposal you just configured from the **IKE Proposal** drop-down menu.

Step 6 Click **Apply** (or **Add**). The Manager returns to the Configuration | Policy Management | Traffic Management | Security Associations screen.

Finally, follow these steps to configure the group to use the SA:

Step 1 Display the Configuration | User Management | Groups screen. (See Figure 10-25.)

Figure 10-25 Configuration | User Management | Groups Screen



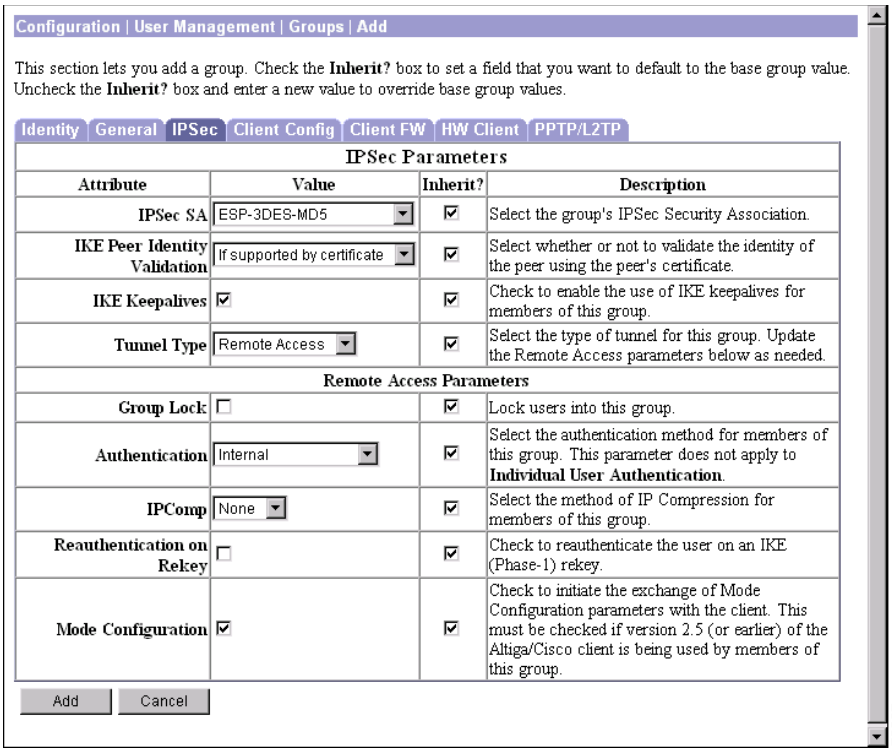
Step 2 Do one of the following:

- To edit an existing group, select a group on the Current Groups list and click **Modify Group**.
- To create a new group, click **Add Group**.

The Manager displays the Configuration | User Management | Groups | Modify (or Add) screen.

Step 3 Click the **IPSec** tab. (See Figure 10-26.)

Figure 10-26 Configuration | User Management | Groups | Modify (or Add) Screen, IPSec Tab



Step 4 Choose the name of the SA you just configured from the IPSec SA drop-down menu.

Step 5 Click **Apply** (or **Add**). The Manager displays the Configuration | User Management | Groups screen.

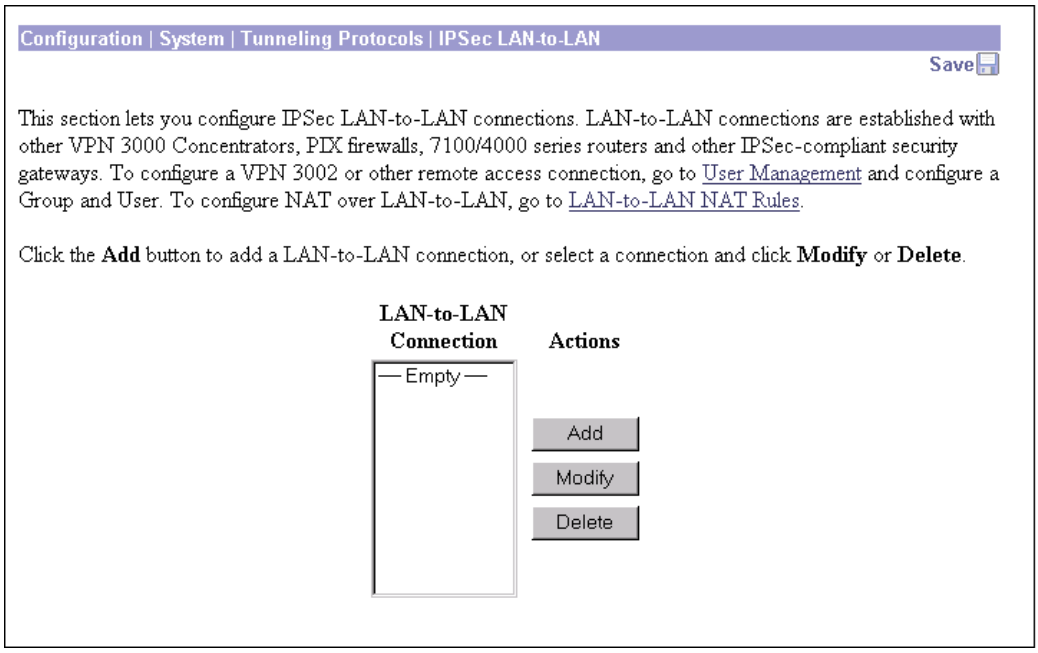
Step 6 Click the **Save Needed** icon to save your changes.

Enabling Digital Certificates for IPSec LAN-to-LAN Connections

To enable digital certificates for IPSec LAN-to-LAN connections, first edit and activate the appropriate IKE proposal. (Follow steps 1-6 in the "Enabling Digital Certificates for Remote Access Connections" section.) Then continue, following these steps:

Step 1 Display the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen. (See Figure 10-27.)

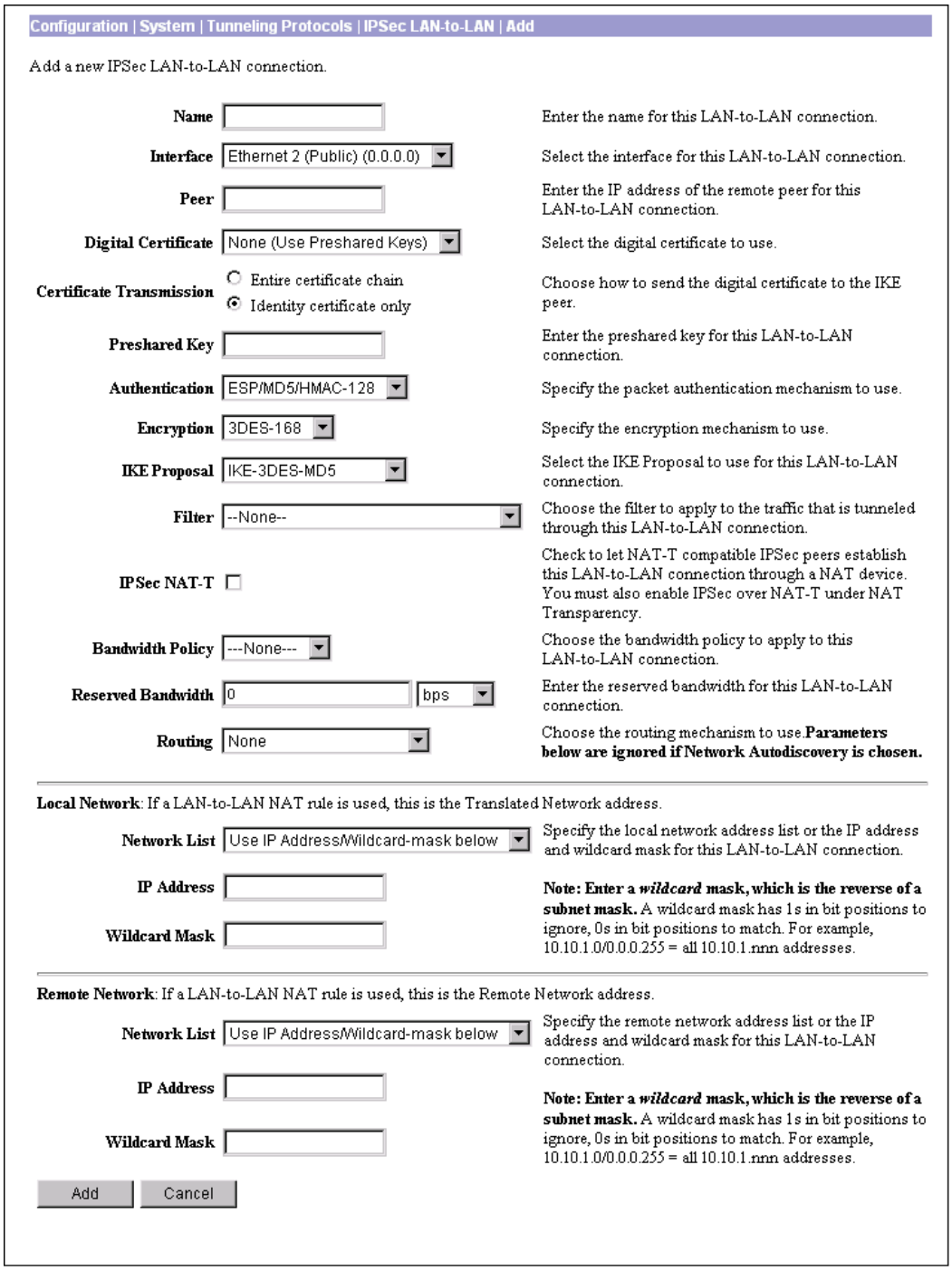
Figure 10-27 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN Screen



Step 2 Select the LAN-to-LAN connection (or create a new one) for which you want to enable digital certificates.

Step 3 Click **Modify** (or **Add**). The Manager displays the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify (or Add) screen. (See Figure 10-28.)

Figure 10-28 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify Screen



Step 4 Click the **Digital Certificate** drop-down menu and choose a digital certificate to use for this LAN-to-LAN connection.

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

Step 6 Click the **IKE Proposal** drop-down menu and choose an activate IKE proposal that is configured for digital certificate authentication.

Step 7 Click **Modify** (or **Add**). The Manager returns to the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen. (See Figure 10-27.)

Step 8 Click the **Save Needed** icon to save your changes.

Deleting Digital Certificates

Delete digital certificates in the following order:

1. Identity or SSL certificates
2. Subordinate certificates
3. Root certificates

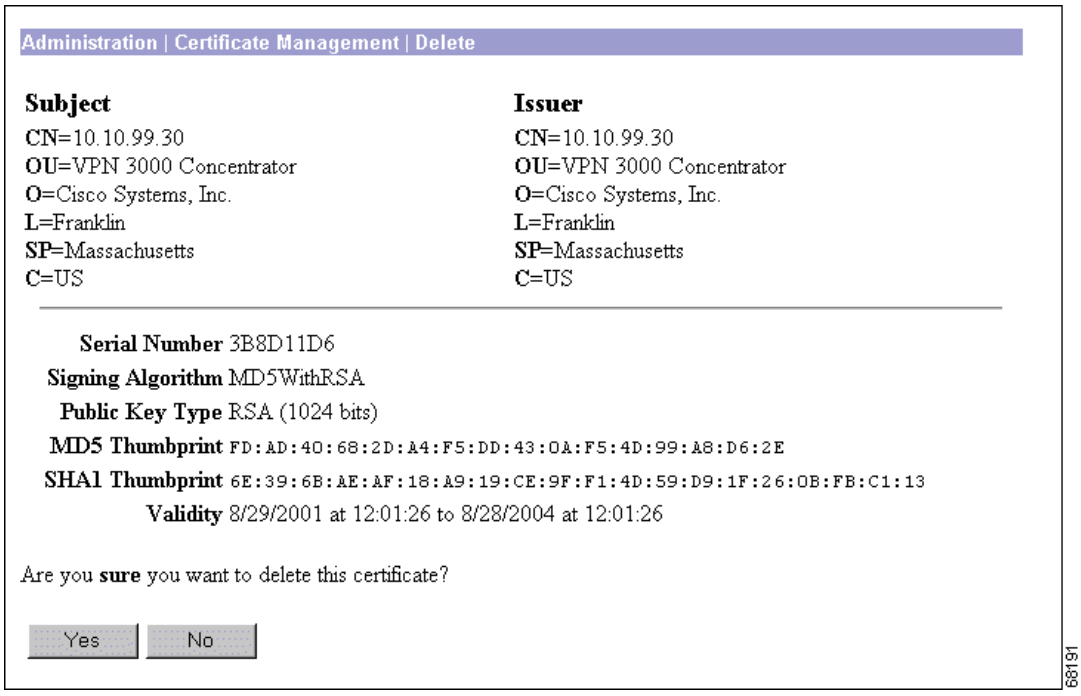
Note You cannot delete a certificate if it is in use by an SA, if it is the issuer of another installed certificate, or if it is referenced in an active certificate request.

Follow these steps to delete certificates:

Step 1 Display the Administration | Certificate Management screen. (See Figure 10-1.)

Step 2 Find the certificate you want to delete and click **Delete**. The Administration | Certificate Management | Delete screen appears.

Figure 10-29 Administration | Certificate Management | Delete Screen



Step 3 Click **Yes**. The Manager returns to the Administration | Certificate Management window.

Administration | Certificate Management

This section of the Manager shows outstanding enrollment requests and all the certificates installed on the VPN Concentrator, and it lets you manage them.

The links at the top of this screen guide you step-by-step through the process of enrolling and installing certificates.

- To install a CA certificate (via SCEP or manually), click on **Click Here to Install a CA Certificate.**

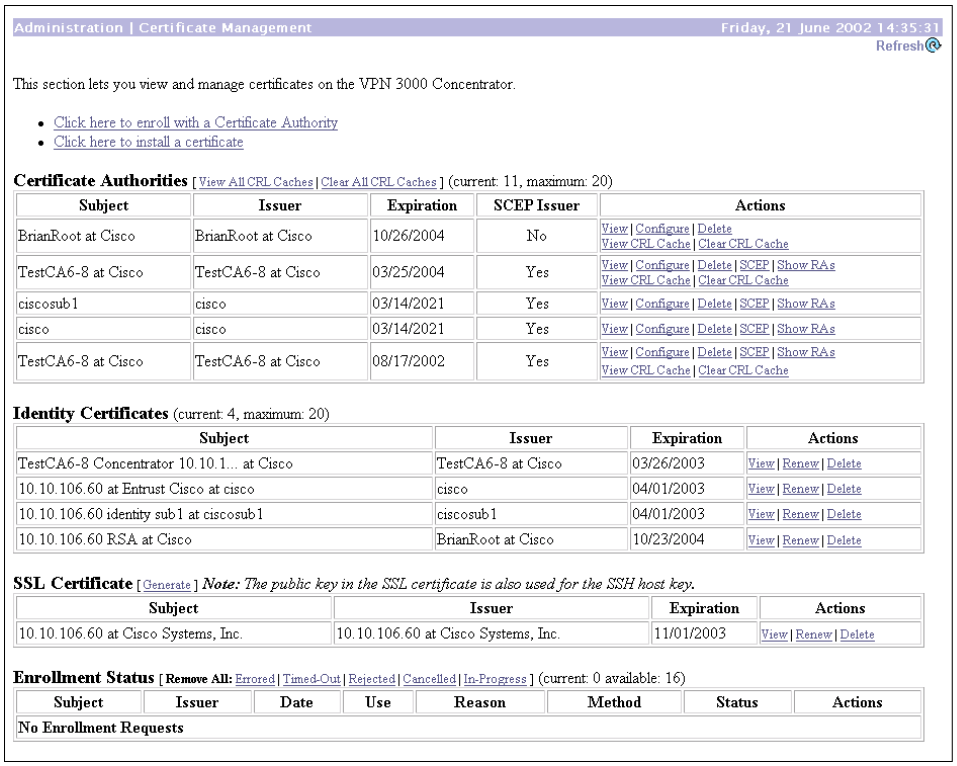
Note The Click here to install a CA certificate option is only available from this window when no CA certificates are installed on the VPN Concentrator. If you do not see this option, click **Click here to install a certificate.** The Manager displays the Administration | Certificate Management | Install. Then click **Install CA Certificate**.

- To create an SSL or identity certificate enrollment request, click on **Click Here to Enroll with a Certificate Authority.**
- To install the certificate obtained via enrollment, click on **Click Here to Install a Certificate.**

The VPN Concentrator notifies you (by issuing a severity 3 CERT class event) if any of the installed certificates are within one month of expiration.

The Manager displays this screen each time you install a digital certificate.

Figure 10-30 Administration | Certificate Management Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Certificate Authorities Table

This table shows root and subordinate CA certificates installed on the VPN Concentrator.

View All CRL Caches

Click the **View All CRL Caches** link to see details of all CRLs cached on the VPN Concentrator.

Clear All CRL Caches

When you delete a CRL from the cache, the next authentication attempt updates it. Use this option to force a cache refresh.

Click the **Clear All CRL Caches** link to delete all the CRLs cached on the VPN Concentrator and force a cache refresh.

Current

The actual number of CA certificates installed on the VPN Concentrator.

Maximum

The maximum possible number of CA certificates allowed on this VPN Concentrator. This limit varies by VPN Concentrator model.

Fields

These fields appear in the Certificate Authorities table:

Field	Content
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; for example, 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. The date format is MM/DD/YYYY.
SCEP Issuer	In order for a certificate to be available for SCEP enrollment, it must be installed via SCEP. This field indicates if the certificate is SCEP-enabled. • Yes = This certificate can issue identity and SSL certificates via SCEP. • No = This certificate cannot issue certificates via SCEP. **Note** If you want to use a certificate for SCEP enrollment, but that certificate is not SCEP-enabled, reinstall it using SCEP.
Actions	This column allows you to manage particular certificates. The actions available vary with type and status of the certificate. • View = View details of this certificate. • Configure = Enable CRL (Certificate Revocation List) checking for this CA certificate, configure CRL caching, or enable acceptance of subordinate CA certificates. • Delete = Delete this certificate from the VPN Concentrator. • View CRL Cache = View details of the CRL cache associated with this certificate. • Clear CRL Cache = Delete the CRL cache associated with this certificate. • SCEP = View or configure SCEP parameters for this certificate. • Show RAs = SCEP-enabled CA certificates sometimes have supporting (RA) certificates. View details of these certificates. (Only available for CA certificates.) • Hide RAs = Hide the details of the RA certificates.

Identity Certificates Table

This table shows installed server identity certificates. For a description of the fields, see the "Certificate Authorities Table" section.

SSL Certificate Table [Generate]

This table shows the SSL server certificate installed on the VPN Concentrator. 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.

This table shows installed server identity certificates. For a description of the fields, see the "Certificate Authorities Table" section.

Enrollment Status Table

This table tracks the status of active enrollment requests.

The number of enrollment requests you can make at any given time is limited to the VPN Concentrator's identity certificate capacity. Most VPN Concentrator models allow a maximum of 20 identity certificates. Thus, for example, if you already have five identity certificates installed, you will only be able to create up to 15 enrollment requests. The VPN 3005 Concentrator is an exception, supporting only two identity certificates. *On the VPN 3005 Concentrator only, y*ou can request a third certificate, even if there are already two certificates installed, but the VPN Concentrator does not install this certificate immediately. First you must delete one of the existing certificates. Then, activate the new certificate to replace the one you just deleted.

The VPN Concentrator automatically deletes entries that have the status "Timed-out," "Failed," "Cancelled," or "Error" and are older than one week.

[Remove All]

Click a **Remove All** option to delete all enrollment requests of a particular status.

- Errored = Delete all enrollment requests with the status "Error."
- Timed-out = Delete all enrollment requests with the status "Timed-out."
- Rejected = Delete all enrollment requests with the status "Rejected."
- Cancelled = Delete all enrollment requests with the status "Cancelled."
- In Progress = Delete all enrollment requests with the status "In Progress."

Current

The number of enrollment requests currently outstanding.

Available

The number of enrollment requests still available.

Fields

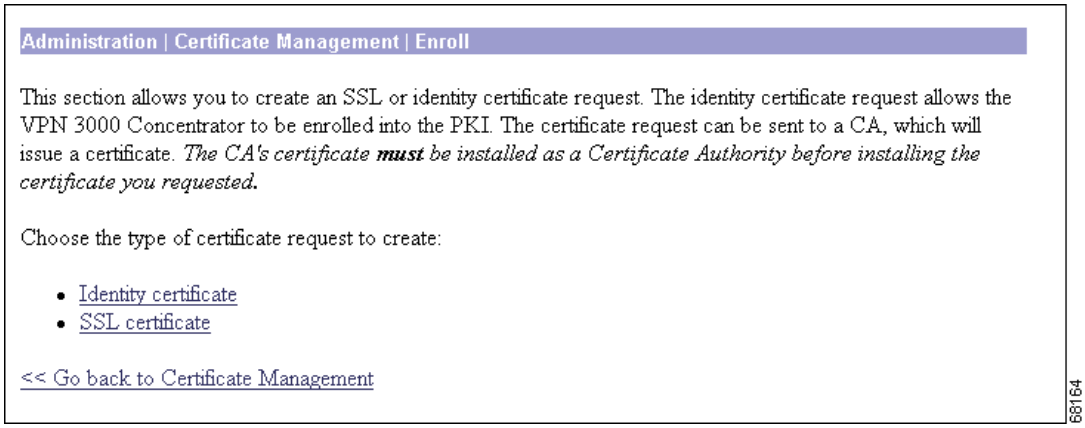
These fields appear in the Enrollment Status table:

Field	Content
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; for example, Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See Administration | Certificate Management | Certificates | View.
Date	The original date of enrollment.
Use	The type of certificate: identity or SSL.
Reason	The type of enrollment: initial, re-enrollment, or re-key.
Method	The method of enrollment: SCEP or manual.
Status	• In Progress = The request has been created, but the requested certificate has not yet been installed. This value is used only for PKCS10 (manual) enrollment requests. • Polling = The CA did not immediately fulfill the enrollment request; the VPN Concentrator has entered polling mode. This value is used only for enrollment request created using SCEP. • Timed-out = The SCEP polling cycle has ended after reaching the configured maximum number of retries. This value is used only for enrollment request created using SCEP. • Rejected = The CA refused to issue the certificate. This value is used only for enrollment request created using SCEP. • Cancelled = The certificate request was cancelled while the VPN Concentrator was in polling mode. • Complete = The CA has fulfilled the renewal request. To bring this new certificate into service, click **Activate**. • Error = An error occurred during the enrollment process. Enrollment was stopped. • Submitting = The certificate request is being sent to the CA.
Actions	This column allows you to manage enrollments requests. The actions available vary with the type and status of the enrollment request. • View = View details of this enrollment request. • Install = Install the enrollment request. This action is available only for PKCS10 (manual) enrollment requests. • Cancel = Cancel a request that is pending. This action is available only for SCEP enrollment requests with “Polling” status. • Re-submit = Re-initiate SCEP communications with the CA or RA using the previously entered request information. This action is available only for SCEP enrollment requests. • Activate = Bring this certificate into service. • Delete = Delete an enrollment request from the VPN Concentrator.

Administration | Certificate Management | Enroll

Choose whether you are creating an enrollment request for an identity certificate or an SSL certificate.

Figure 10-31 Administration | Certificate Management | Enrollment Screen



Identity Certificate

Click **Identity Certificate** to create a certificate request for an identity certificate. The Manager displays the Administration | Certificate Management | Enroll | Identity Certificate screen.

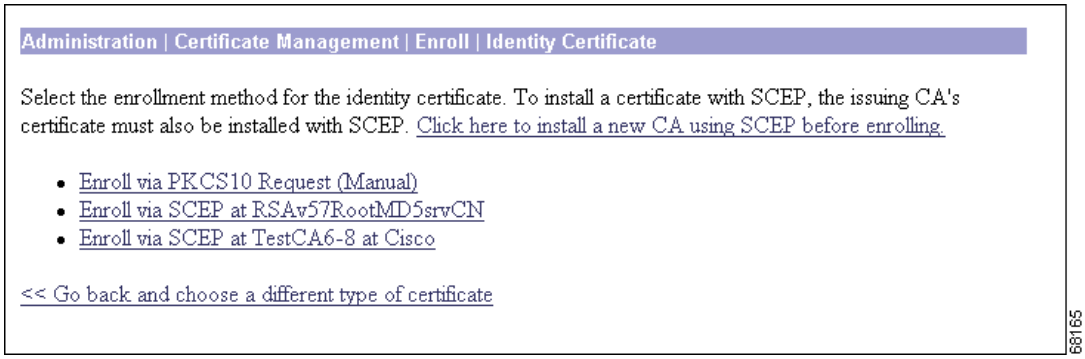
SSL Certificate

Click **SSL Certificate** to create a certificate request for an SSL certificate. The Manager displays the Administration | Certificate Management | Enroll | SSL Certificate screen.

Administration | Certificate Management | Enroll | *Certificate Type*

Choose the method for enrolling the (identity or SSL) certificate.

Figure 10-32 Administration | Certificate Management | Enroll | Identity Certificate Screen



Enroll via PKCS10 Request (Manual)

Click **Enroll via PKCS10 Request (Manual)** to enroll the certificate manually.

Enroll via SCEP at *[Name of SCEP CA]*

Click **Enroll via SCEP at *[Name of SCEP CA]*** to enroll the certificate automatically using SCEP.

You can enroll certificates using SCEP only if you installed the CA certificate using SCEP. One Enroll via SCEP at *[Name of SCEP CA]* link appears on this screen for each CA certificate on the VPN Concentrator that was installed using SCEP. To see which CA certificates on your VPN Concentrator were installed using SCEP, see the Certificate Authorities table on the Administration | Certificate Management screen. "Yes" in the SCEP Issuer column indicates that the CA certificate was installed using SCEP; "No" indicates it was installed manually. If no CA certificate on the VPN Concentrator was installed using SCEP, then no Enroll via SCEP at *[Name of SCEP CA]* link appears on this screen. You do not have the option of using SCEP to enroll the certificate.

Install a New SA Using SCEP before Enrolling

If you want to install a certificate using SCEP, but no Enroll via SCEP at *[Name of SCEP CA]* link appears here, click **Install a new SA Using SCEP before Enrolling**. Install a CA certificate using SCEP, then return to this screen to install the certificate. A SCEP link now appears.

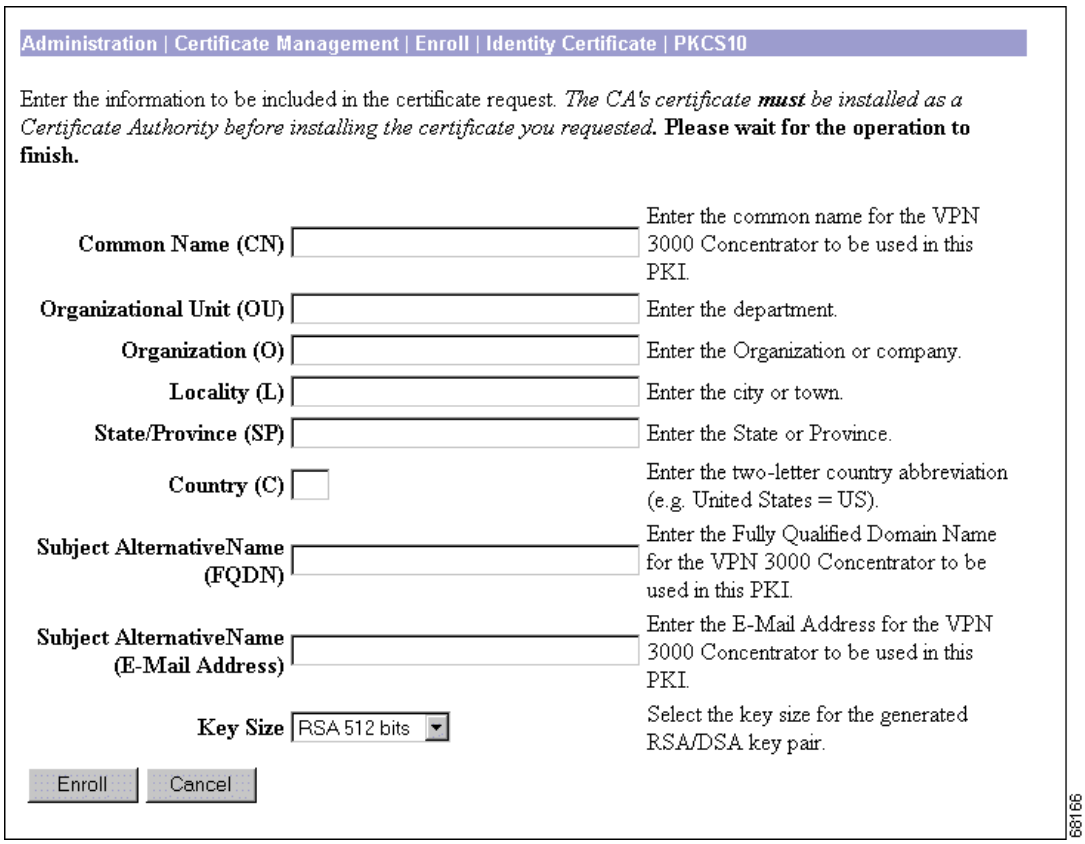
<< Go back and choose a different type of certificate

Click **<< Go back and choose a different type of certificate** to return to the Administration | Certificate Management | Enroll screen. (See Figure 10-31.)

Administration | Certificate Management | Enroll | *Certificate Type* | PKCS10

To generate an enrollment request for an SSL or identity certificate, you need to provide information about the VPN Concentrator.

Figure 10-33 Administration | Certificate Management | Enroll | Identity Certificate via PKCS10 Screen



Fields

For an explanation of each of the fields on this screen, see Table 10-2.

Table 10-2 Fields in a Certificate Request

Field Name	Manual	SCEP	Content
Common Name (CN)	Yes	Yes	The primary identity of the entity associated with the certificate, for example, Gateway A. Spaces are allowed. You must enter a name in this field.
Organizational Unit (OU)	Yes	Yes	The name of the department or other organizational unit to which this VPN Concentrator belongs, for example: VPNC. Spaces are allowed. ⚠ **Caution** The value you enter in this field must match on both ends of the connection.
Organization (O)	Yes	Yes	The name of the company or organization to which this VPN Concentrator belongs, for example: Cisco Systems. Spaces are allowed.
Locality (L)	Yes	Yes	The city or town where this VPN Concentrator is located, for example: Franklin. Spaces are allowed.
State/Province (SP)	Yes	Yes	The state or province where this VPN Concentrator is located, for example: Massachusetts. Spell the name out completely; do not abbreviate. Spaces are allowed.
Country (C)	Yes	Yes	The country where this VPN Concentrator is located, for example: US. Use two characters, no spaces, and no periods. This two-character code must conform to ISO 3166 country codes.
Subject Alternative Name (Fully Qualified Domain Name) (FQDN)	Yes	Yes	The fully qualified domain name that identifies this VPN Concentrator in this PKI, for example: Cisco.com. This field is optional. The alternative name is an additional data field in the certificate that provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.
Subject Alternative Name (E-mail Address) (E-mail)	Yes	Yes	The e-mail address of the VPN Concentrator administrator, for example: gatewaya@cisco.com.
Challenge Password	No	Yes	This field displays if you are requesting a certificate using SCEP. Use this field according to the policy of your CA: Your CA might have given you a password. If so, enter it here for authentication. Your CA might allow you to provide your own password to identify yourself to the CA in the future. If so, create your password here. Your CA might not require a password. If not, leave this field blank.
Verify Challenge Password	Mp	Yes	Re-enter the password.

Table 10-2 Fields in a Certificate Request (continued)

Field Name	Manual	SCEP	Content
Key Size	Yes	Yes	The algorithm for generating the public-key/private-key pair, and the key size. If you are requesting an SSL certificate, or if you are requesting an identity certificate using SCEP, only the RSA options are available. • RSA 512 bits = Generate 512-bit keys using the RSA (Rivest, Shamir, Adelman) algorithm. This key size provides sufficient security and is the default selection. It is the most common, and requires the least processing. • RSA 768 bits = Generate 768-bit keys using the RSA algorithm. This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key. • RSA 1024 bits = Generate 1024-bit keys using the RSA algorithm. This key size provides high security, and it requires approximately 4 to 8 times more processing than the 512-bit key. • RSA 2048 = Generate 2048-bit keys using the RSA algorithm. This key size provides very high security. It requires 8-16 times more processing than the 512-bit key.
	Yes	No	• 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.

Enroll / Cancel

To generate the certificate request, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen (See Figure 10-34.), and then opens a browser window showing the certificate request. (See Figure 10-35.) To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

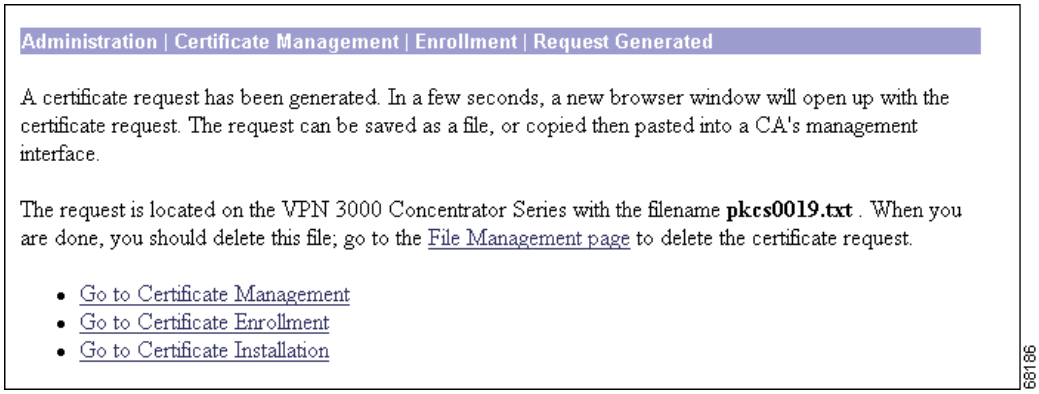
Administration | Certificate Management | *Enrollment* or *Renewal* | Request Generated

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 (pkcs*NNNN*.txt).

In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN Concentrator in encrypted form.

Note You must complete the enrollment and certificate installation process within one week of generating the request. If you do not, the pending request is deleted.

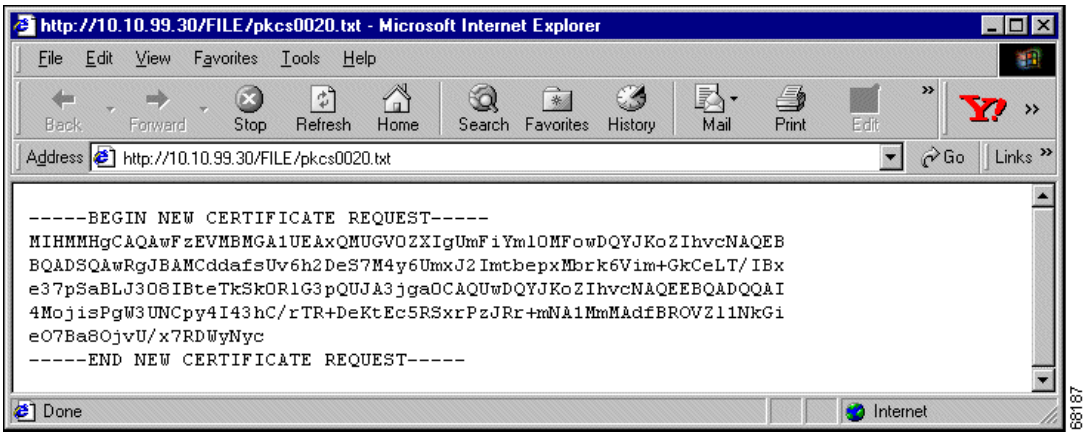
Figure 10-34 Administration | Certificate Management | Enrollment | Request Generated Screen



To go to the Administration | File Management | Files screen, click the highlighted **File Management page** link. From there you can view, copy, or delete the file in Flash memory.

The system also automatically opens a new browser window and displays the certificate request. You can select and copy the request to the clipboard, or you can save it as a file on your PC or a network host. Some CAs let you paste the request in a web interface, some ask you to send a file; use the method your CA requires.

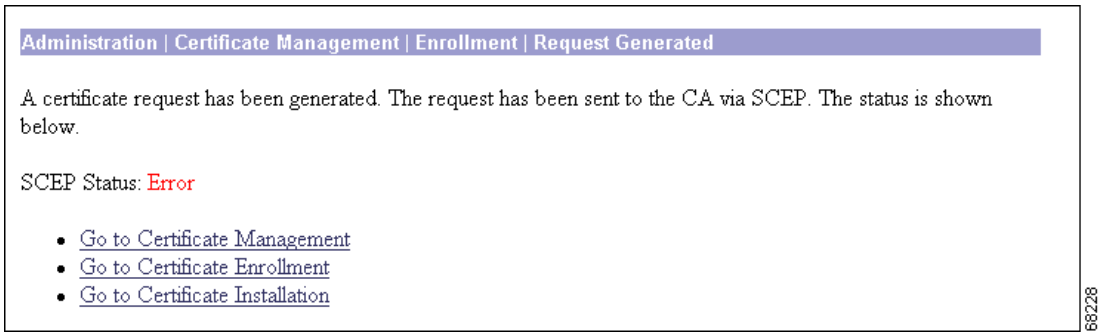
Figure 10-35 Browser Window Displaying Certificate Request



Close this browser window when you have finished.

If there is an error in generating your certificate request, a different version of this screen appears. (See Figure 10-36.) You can view the certificate request and re-submit it from the Administration | Certificate Management screen.

Figure 10-36 Administration | Certificate Management | Enrollment | Request Generated Screen—Error



Go to Certificate Management

If you want to view the certificate request, click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen. (See Figure 10-1.)

Go to Certificate Enrollment

If you want to enroll another certificate, click **Go to Certificate Enrollment**. The Manager displays the Administration | Certificate Management | Enroll screen.

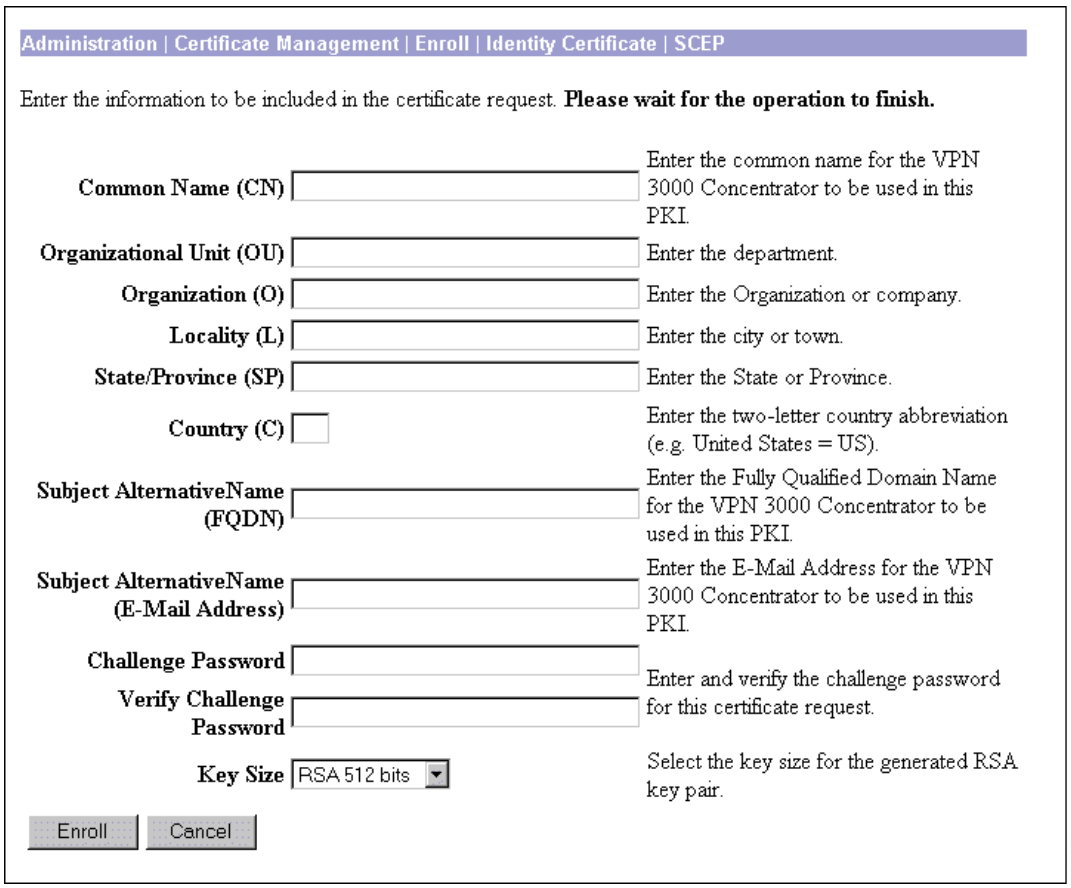
Go to Certificate Installation

If you want to install the certificate you have just enrolled, click **Go to Certificate Installation**. The Manager displays the Administration | Certificate Management | Install screen.

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

To generate an enrollment request for an identity certificate, you need to provide information about the VPN Concentrator.

Figure 10-37 Administration | Certificate Management | Enroll | Identity Certificate via SCEP Screen



Fields

For an explanation of each of the fields on this screen, see Table 10-2.

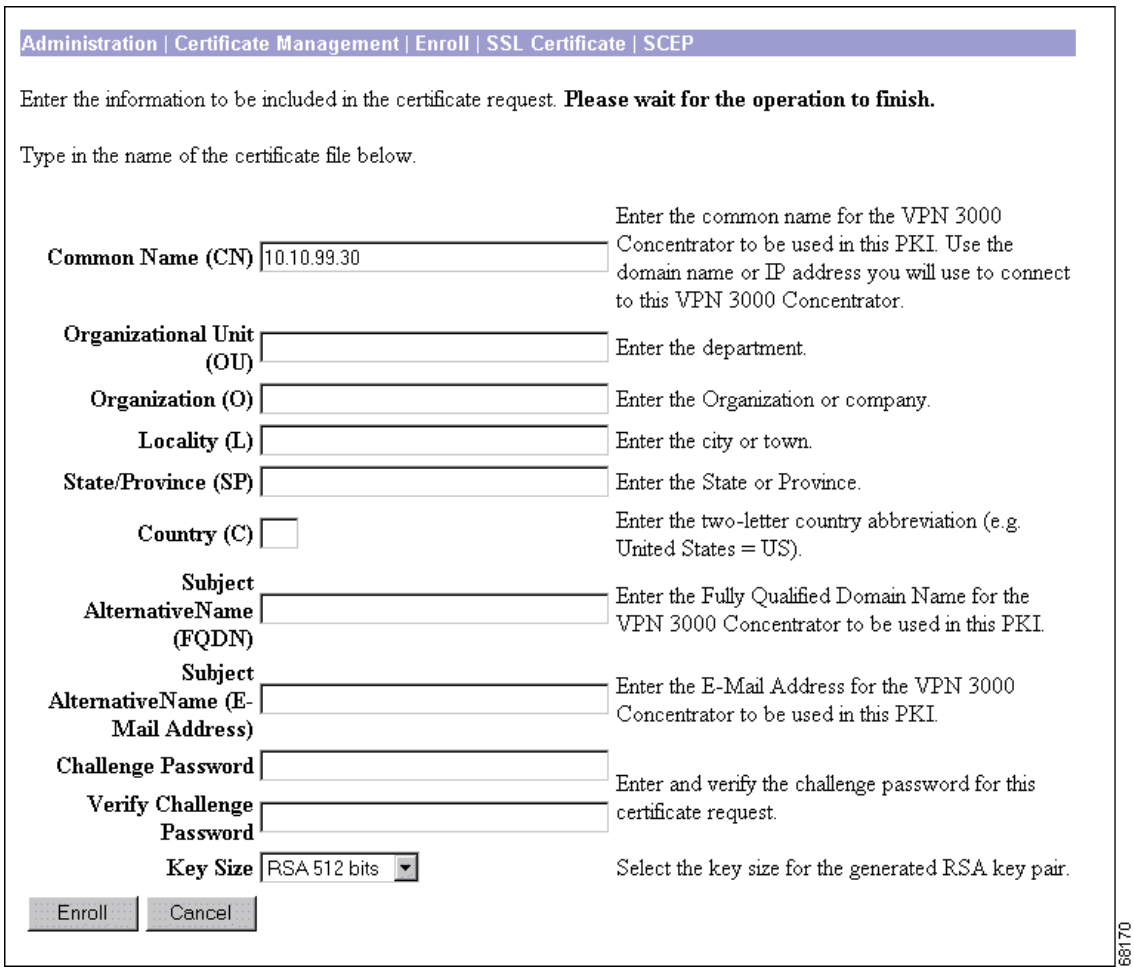
Enroll / Cancel

To generate the certificate request and install the identity certificate on the VPN Concentrator, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen. (See Figure 10-34.) To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See Figure 10-1.)

Administration | Certificate Management | Enroll | SSL Certificate | SCEP

To generate an enrollment request for an SSL certificate, you need to provide information about the VPN Concentrator.

Figure 10-38 Administration | Certificate Management | Enroll | SSL Certificate | SCEP Screen



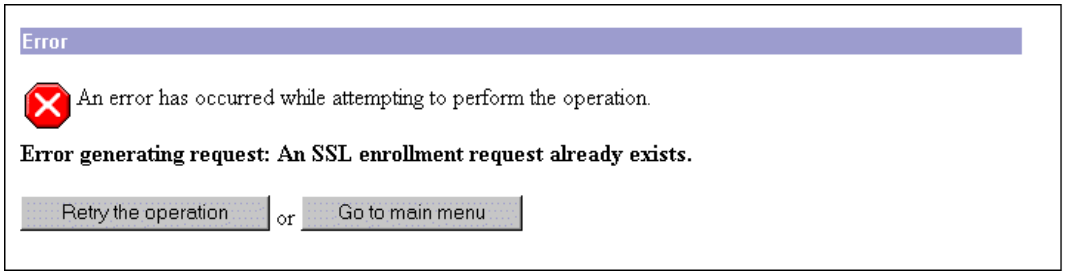
Fields

For an explanation of each of the fields on this screen, see Table 10-2.

Enroll

To generate the certificate request and install the SSL certificate on the VPN Concentrator, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen.

If there is already an active request for an SSL certificate on the VPN Concentrator, this error message appears.



To return to the Administration | Certificate Management | Enroll | SSL Certificate | SCEP screen, click **Retry the operation**.

To return to the Main screen, click **Return to main menu**.

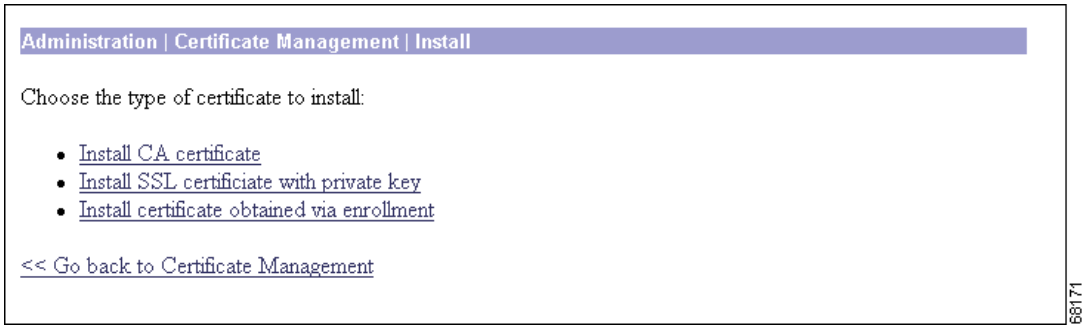
Cancel

To discard your entries and cancel the request, click **Cancel**. The Manager displays the Administration | Certificate Management screen.

Administration | Certificate Management | Install

Choose the type of certificate you want to install.

Figure 10-39 Administration | Certificate Management | Install Screen



Install CA Certificate

If you want to install a CA certificate, click **Install CA Certificate**. The Manager displays the Administration | Certificate Management | Install | CA Certificate screen.

Install SSL Certificate with Private Key

Some web servers export their SSL certificates with the private key attached. If you have a PEM-encoded certificate with a corresponding private key that you want to install, click **Install SSL Certificate with Private Key**. The Manager displays the Administration | Certificate Management | Install | SSL Certificate with Private Key screen.

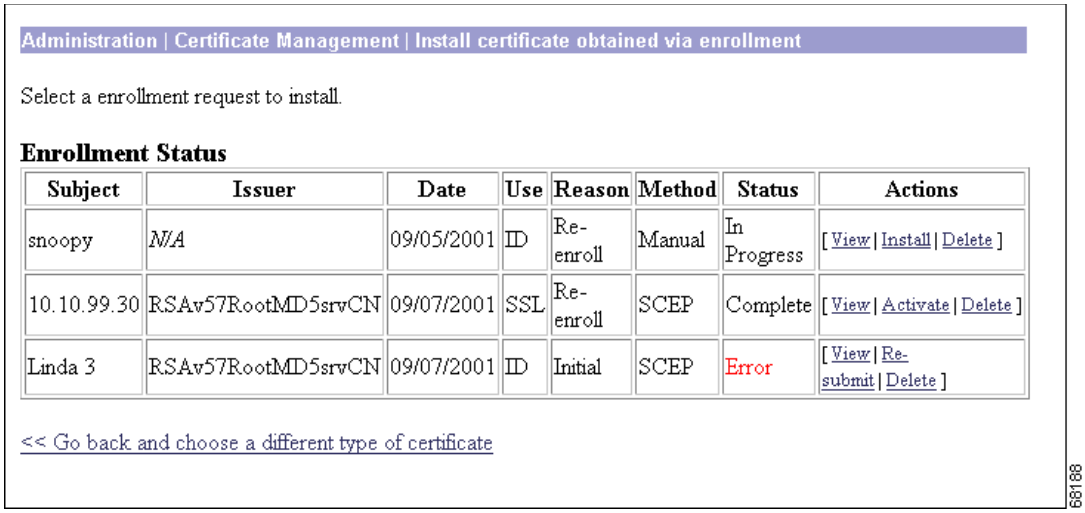
Install Certificate Obtained via Enrollment

If you want to install a certificate manually that you have obtained by enrolling a certificate request with a CA, click **Install Certificate Obtained via Enrollment**. The Manager displays the Administration | Certificate Management | Install Certificate Obtained via Enrollment screen.

Administration | Certificate Management | Install | Certificate Obtained via Enrollment

Once you have enrolled a certificate, you can install it. This screen allows you to install an enrolled certificate.

Figure 10-40 Administration | Certificate Management | Install | Certificate Obtained via Enrollment Screen



Enrollment Status Table

For a description of the fields in this table, see the "Enrollment Status Table".

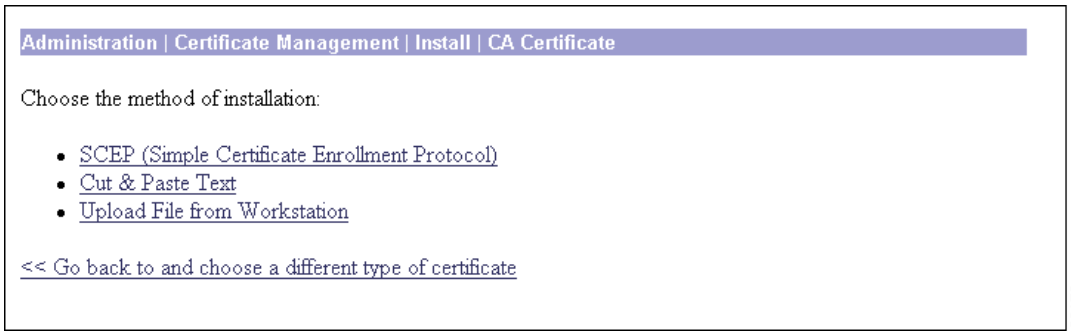
<< Go back and choose a different type of certificate

If you do not want to install a certificate that you have obtained via filing an enrollment request with your CA, click **<< Go back and choose a different type of certificate**. The Manager returns to the Administration | Certificate Management | Install screen.

Administration | Certificate Management | Install | *Certificate Type*

Choose the method you want to use to install the certificate.

Figure 10-41 Administration | Certificate Management | Install | CA Certificate



SCEP (Simple Certificate Enrollment Protocol)

Note This option is available only for CA certificates.

If you want to install the CA certificate automatically using SCEP, click SCEP **(Simple Certificate Enrollment Protocol)**. The Manager displays the Administration | Certificate Management | Install | CA Certificate | SCEP screen. (See Figure 10-42.)

Cut & Paste Text

If you want to cut and paste the certificate using a browser window, click **Cut & Paste Text**. The Manager displays the Administration | Certificate Management | Install | *Certificate Type* | Cut & Paste Text screen. (See Figure 10-43.)

Upload File from Workstation

If your certificate is stored in a file, click **Upload File from Workstation**. The Manager displays the Administration | Certificate Management | Install | *Certificate Type* | Upload File from Workstation screen. (See Figure 10-44.)

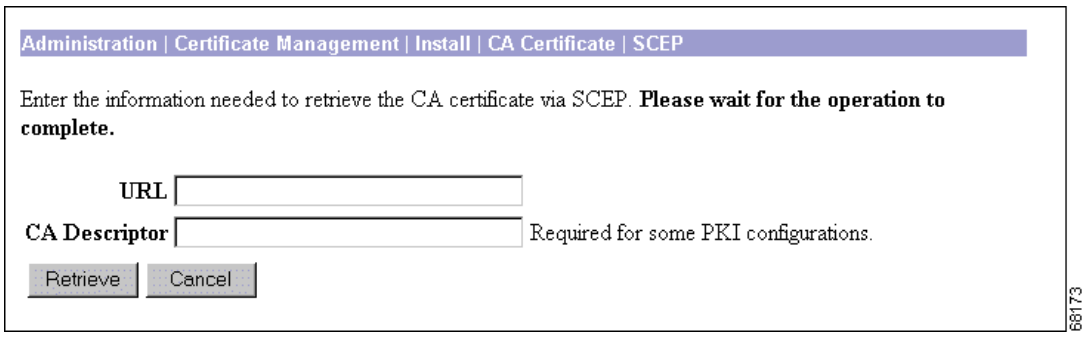
<< Go back and choose a different type of certificate

If you do not want to install a certificate, click **<< Go back and choose a different type of certificate** to display the Administration | Certificate Management | Install screen. (See Figure 10-39.)

Administration | Certificate Management | Install | CA Certificate | SCEP

In this screen, provide information about the certificate authority in order to retrieve and install a CA certificate automatically using SCEP.

Figure 10-42 Administration | Certificate Management | Install | CA Certificate | SCEP Screen



URL

Enter the URL of the SCEP interface of the CA.

CA Descriptor

Some CAs use descriptors to further identify the certificate. If your CA gave you a descriptor, enter it here. Otherwise enter a descriptor of your own. You must enter something in this field.

Retrieve / Cancel

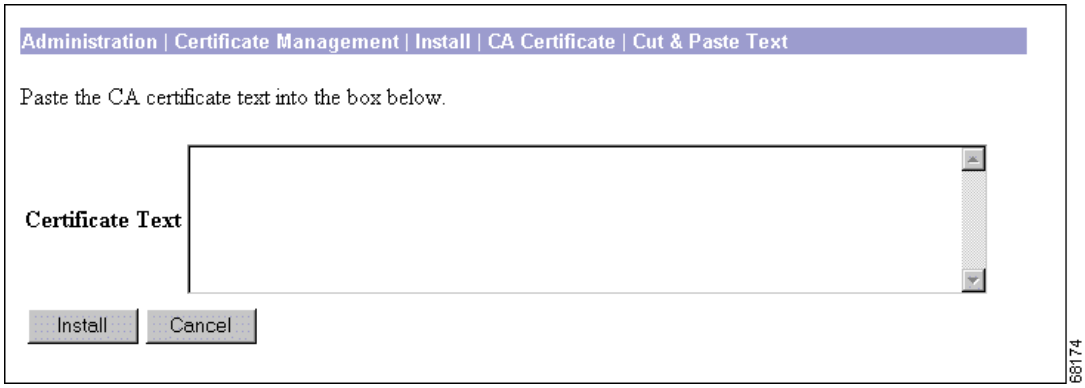
To retrieve a CA certificate from the CA and install it on the VPN Concentrator, click **Retrieve**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See Figure 10-1.)

Administration | Certificate Management | Install | *Certificate Type* | Cut and Paste Text

To install the certificate using the manual method, cut and paste the certificate text into the Certificate Text window.

Figure 10-43 Administration | Certificate Management | Install | CA Certificate | Cut and Paste Text Screen



Certificate Text

Paste the PEM or base-64 encoded certificate text from the clipboard into this window.

If you are installing an SSL certificate with a private key, include the encrypted private key.

Password

Note This field appears only if you are installing an SSL certificate with a private key.

Enter a password for decrypting the private key.

Install / Cancel

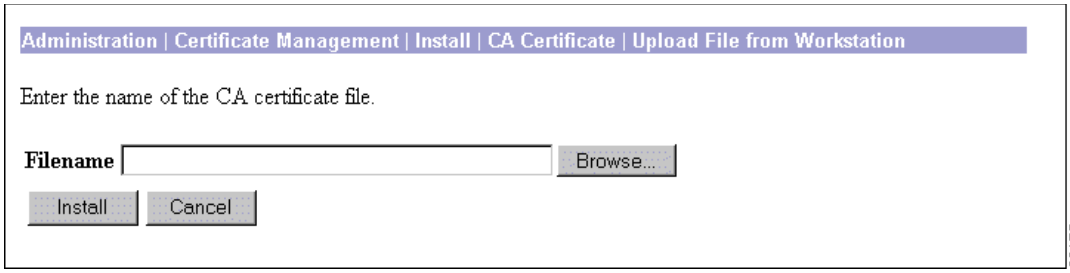
To install the certificate on the VPN Concentrator, click **Install**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See Figure 10-1.)

Administration | Certificate Management | Install | *Certificate Type* | Upload File from Workstation

If you want to install a certificate stored on your PC, use this screen to upload the certificate file to the VPN Concentrator.

Figure 10-44 Administration | Certificate Management | Install | CA Certificate | Upload File from Workstation Screen



Filename / Browse

Enter the name of the certificate file that is on your PC. In a Windows environment, enter the complete pathname using MS-DOS syntax, for example: c:\Temp\certnew.cer. You can also click the **Browse** button to open a file navigation window, find the file, and select it.

Password

Note This field appears only if you are installing an SSL certificate with a private key.

Enter a password for decrypting the private key.

Install / Cancel

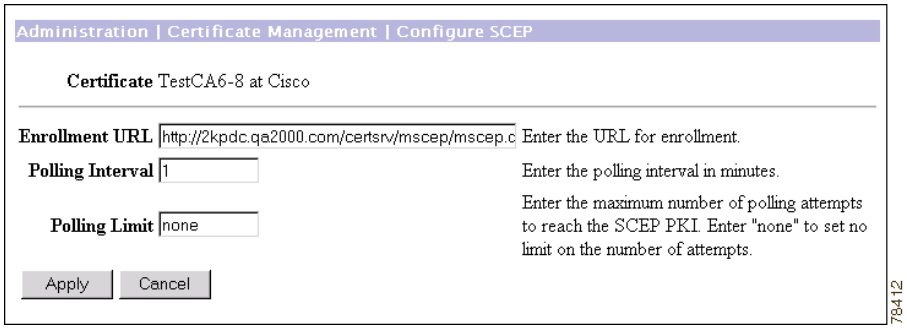
To install the certificate on the VPN Concentrator, click **Install**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See Figure 10-1.)

Administration | Certificate Management | Configure SCEP

The SCEP Configuration parameters are available only for CA certificates that support SCEP enrollment.

Figure 10-45 Administration | Certificate Management | Configure SCEP



Enrollment URL

Enter the URL where the VPN Concentrator should send SCEP enrollment requests made to this CA. The default value of this field is the URL used to download this CA certificate.

Polling Interval

If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request will enter polling mode. In polling mode, the VPN Concentrator re-sends the certificate request to the CA for a specified period until the CA responds or the process times out.

Enter the number of minutes the VPN Concentrator should wait between re-sends. The minimum number of minutes is 1; the maximum number of minutes is 60. The default value is 1

Polling Limit

Enter the number of times the VPN Concentrator should re-send an enrollment request if the CA does not issue the certificate immediately. The minimum number of re-sends is 0; the maximum number is 100. If you did not want any polling limit, (in other words, you want infinite re-sends), enter `none`.

Administration | Certificate Management | View CRL Cache

This window shows details of CRLs cached on the VPN Concentrator issued by a particular CA. If you clicked the View All CRL Caches link on the Administration | Certificate Management window to invoke this window, then the window shows details of all CRLs cached on the VPN Concentrator.

Figure 10-46 Administration | Certificate Management | View CRL Cache (of a particular CA)

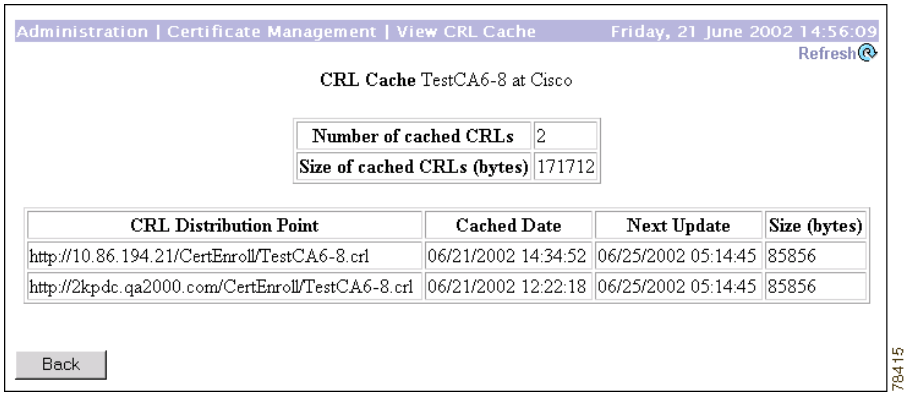
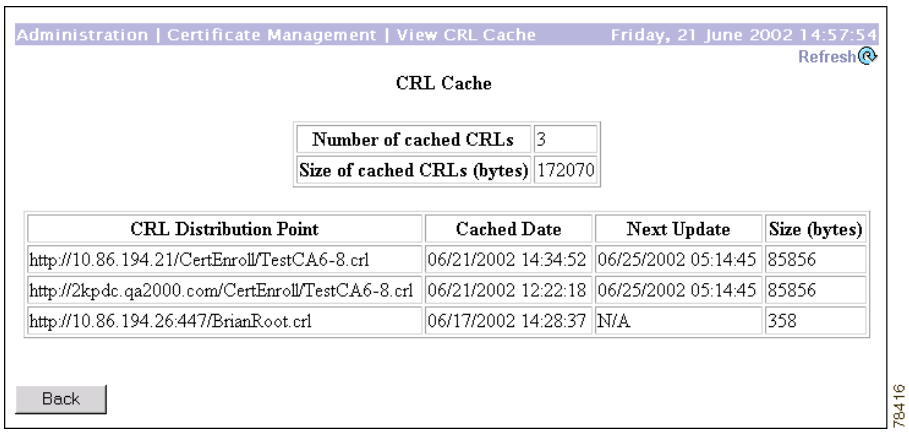


Figure 10-47 Administration | Certificate Management | View CRL Cache (of all CAs)



Number of Cached CRLs

The number of cached CRLs issued by a particular CA. Or, the number of cached CRLs issued by all CAs.

Size of Cached CRLs (in bytes)

The total size of all the CRLs issued by a particular CA. Or, the total size of all the CRLs issued by all CAs.

CRL Distribution Point

The location from which the CRL was retrieved.

Cached Date

The date and time the CRL was retrieved.

Next Update

The date and time when the CA is expected to issue an updated CRL.

Note During tunnel establishment the VPN Concentrator checks to see if the CRL associated with the connecting user is current. If the CRL has expired, the VPN Concentrator automatically reloads an updated CRL from that CA before attempting to validate the user.

Size (bytes)

The size of the CRL.

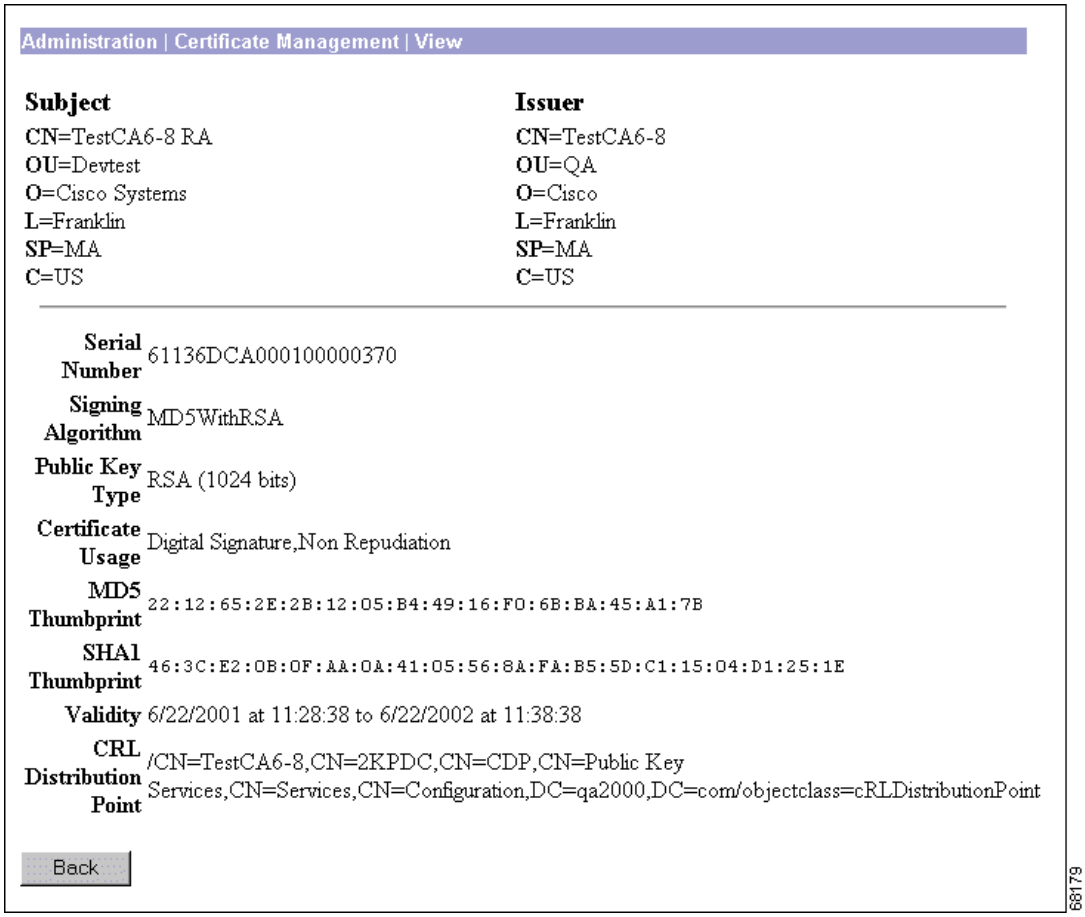
Administration | Certificate Management | View

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 10-48 Administration | Certificate Management | View Screen



Certificate Fields

A certificate contains some or all of the following fields:

Field	Content
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 Concentrator 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 Concentrator 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 must be unique among all certificates issued by that CA. CRL checking uses this serial number.
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 certified public key.
Certificate Usage	The purpose of the key contained in the certificate, for example: digital signature, certificate signing, nonrepudiation, key or data encipherment, etc.
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 root certificate's authenticity, you can check this value with the issuer.

Field	Content
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 to MM/DD/YYYY at HH:MM:SS. Time uses 24-hour notation, and is local system time. The Manager checks the validity against the VPN Concentrator system clock, and it flags expired certificates by issuing event log entries.
Subject Alternative Name (Fully Qualified Domain Name)	The fully qualified domain name for this VPN Concentrator 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.
CRL Distribution Point	All CRL distribution points from the issuer of this certificate.

Back

To return to the Administration | Certificate Management screen, click **Back.**

Administration | Certificate Management | Configure CA Certificate

This screen lets you enable certificate revocation list (CRL) checking for CA certificates installed in the VPN Concentrator.

A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to a name change, change of association between the subject and the CA, security compromise, etc., the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed certificate revocation list (CRL), where each revoked certificate is identified by its serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the CRL to ensure that the certificate being verified has not been revoked.

CAs use LDAP/HTTP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP/HTTP access.

Configuring CRL Checking

During IKE phase 1 negotiation, if CRL checking is enabled, the VPN Concentrator verifies the revocation status of the IKE peer certificate before allowing the tunnel to be established. CRLs exist on external servers maintained by Certificate Authorities. To verify the revocation status, the VPN Concentrator retrieves the CRL using one of the available CRL distribution points and checks the peer certificate serial number against the list of serial numbers in the CRL. If there are no matches, the VPN Concentrator assumes that the peer certificate has not been revoked.

The default is No CRL Checking. In this case, the VPN Concentrator neither retrieves a CRL nor performs revocation checking.

To enable CRL checking, choose the method to use to retrieve the CRL. A CRL distribution point is the location on a server from which a CRL can be downloaded.

You can configure the VPN Concentrator to retrieve the CRL from the distribution points specified in the certificate being checked, from a user-specified list of static CRL distribution points, or from a combination of these.

Enabling CRL Caching

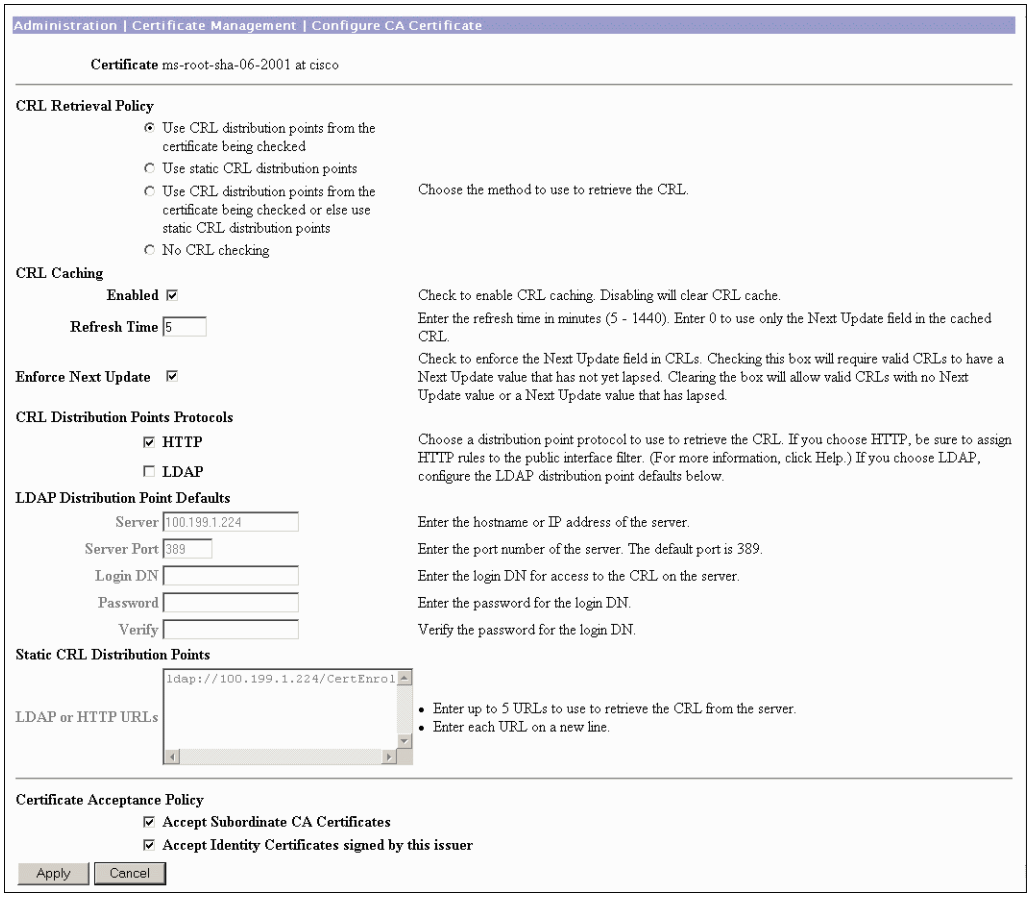
Since the system has to fetch and examine the CRL from a network distribution point, enabling CRL checking might slow system response times. Also, if the network is slow or congested, CRL checking might fail. To mitigate these potential problems, you can enable CRL caching. This stores the retrieved CRLs in local volatile memory, thus allowing the VPN Concentrator to verify the revocation status of certificates more quickly.

With CRL Caching enabled, when the VPN Concentrator needs to check the revocation status of a certificate, it first checks whether the required CRL exists in the cache and checks the serial number of the certificate against the list of serial numbers in the CRL. The certificate is considered revoked if its serial number is found. The VPN Concentrator retrieves a CRL from an external server either when it does not find the required CRL in the cache, when the validity period of the cached CRL has expired, or when the configured refresh time has elapsed. When the VPN Concentrator receives a new CRL from an external server, it updates the cache with the new CRL. The cache can contain up to 64 CRLs.

The total memory allocated for all combined CRL caches varies by VPN Concentrator model. Model 3005 can cache up to 128 KB. Models 3015 and 3030 can cache up to 256 KB. Models 3060 and 3080 can cache up to 1 MB.

Note The CRL cache exists in memory, so rebooting the VPN Concentrator clears the CRL cache. The VPN Concentrator repopulates the CRL cache with updated CRLs as it processes new peer authentication requests.

Figure 10-49 Administration | Certificate Management | Configure CA Certificate Screen



Certificate

The certificate for which you are configuring CRL checking. This is the name in the Subject field of the Certificate Authorities table on the Administration | Certificate Management screen.

CRL Retrieval Policy

Choose the appropriate option to enable or disable CRL checking on all certificates issued by this CA. The VPN Concentrator can:

- Use CRL distribution points from the certificate being checked = The VPN Concentrator retrieves up to five CRL distribution points from the CRL Distribution Point extension of the certificate being verified and augments their information with the configured default values, if necessary. If the concentrator's attempt to retrieve a CRL using the primary CRL distribution point fails, it retries using the next available CRL distribution point in the list. This continues until either a CRL is retrieved or the list is exhausted.

  If you choose this option, be sure to enable at least one CRL Distribution Point Protocol. If you choose a LDAP protocol, be sure to set the LDAP Distribution Point Defaults as well.

- Use static CRL distribution points = Use up to five static CRL distribution points, as specified on this screen.

  If you choose this option, you must enter at least one (and no more than five) URLs.

- Use CRL distribution points from the certificate being checked, or else use static distribution points = If the VPN Concentrator cannot find five CRL distribution points in the certificate, it adds static CRL distribution points, up to a limit of five.

  If you choose this option, be sure to enable at least one CRL Distribution Point Protocol. If you choose a LDAP protocol, be sure to set the LDAP Distribution Point Defaults as well. You also must enter at least one (and no more than five) Static CRL Distribution Points.

- No CRL Checking = Do not enable CRL checking.

CRL Caching

Specify whether you want to enable CRL caching, and if so, what the cache refresh period is.

Enabled

Check the Enabled check box to allow the VPN Concentrator to cache retrieved CRLs. The default is not to enable CRL caching. Disabling CRL caching (unchecking the check box) clears the CRL cache.

Refresh Time

Specify the refresh time in minutes for the CRL cache. The range is 5 to 1440 minutes; the default value is 60 minutes.

Enter 0 to use the Next Update field, if present, in the cached CRL. If the Next Update field is not present in the CRL, the CRL is not cached.

Enforce Next Update

The Enforce Next Update feature allows you to control how the VPN Concentrator responds to users authenticating with certificates when the CRL associated with those certificates is outdated.

When a user attempts to authenticate using a digital certificate, the VPN Concentrator looks for the most recent CRL associated with that certificate. The VPN Concentrator checks the Next Update field in its current CRL to determine if a newer CRL might be available. If the Next Update date is current, the VPN Concentrator uses the CRL to authenticate the user. However, if the date has lapsed, the VPN Concentrator contacts the certificate authority to request a newer CRL.

The certificate authority sends another CRL. The new CRL might or might not be more recent. If the Next Update field in the new CRL is current, the VPN Concentrator uses the new CRL to authenticate the user. However, it can happen that the certificate authority returns another CRL with an outdated Next Update field. If the Next Update date in this new CRL has already past, the VPN Concentrator can either use that CRL or not, depending on how you configure the Enforce Next Update option.

It is also possible that a CRL might not have a Next Update field.

Check the **Enforce Next Update** check box to require a current CRL. If enabled, the VPN Concentrator rejects CRLs that do not have Next Update fields and CRLs for which the Next Update field has lapsed.

Uncheck the box if you want the VPN Concentrator to be able to use CRLs without a Next Update field or CRLs for which the Next Update field has lapsed.

CRL Distribution Points Protocols

If you configured a CRL retrieval policy that uses CRL distribution points from the certificate being checked, choose a distribution point protocol to use to retrieve the CRL.

- If you choose HTTP, be sure to assign HTTP rules to the public interface filter.
- If you choose LDAP, configure the LDAP distribution point defaults below.

LDAP Distribution Point Defaults

If you chose to support LDAP distribution points, enter the following information. If the distribution point extension of the certificate being checked is missing any of the following fields, the VPN Concentrator uses these values.

Server

Enter the IP address or hostname of the CRL distribution server (LDAP server). Maximum 32 characters.

Server Port

Enter the port number for the CRL server. Enter 0 (the default) to have the system supply the default port number, 389 (LDAP).

Login DN

Enter the login DN (Distinguished Name)), which defines the directory path to access this CRL database, for example: cn=crl,ou=certs,o=CANam,c=US. The maximum field length is 128 characters.

Password

Enter the password for the Login DN. Maximum 128 characters.

Verify

Re-enter the password to verify it. Maximum 128 characters.

Static CRL Distribution Points

Enter HTTP or LDAP URLs that identify CRLs located on external servers. If you chose a CRL Retrieval Policy that uses static distribution points, you must enter at least one (and not more than five) valid URLs. Enter each URL on a single line. (Scroll right to enter longer values.) Examples of valid URLs are:

HTTP URL: `http://1.1.1.2/CertEnroll/TestCA6-8.crl`

LDAP URL: `ldap://100.199.7.6:389/CN=TestCA6-8,CN=2KPDC,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=qa2000,DC=com?certficateRevocationList?base?objectclass=cRLDistributionPoint`

Certificate Acceptance Policy

Accept Subordinate CA Certificates

During Phase 1 processing, an IKE peer might deliver a certificate subordinate to this one. This subordinate certificate might not be installed on the VPN Concentrator. Check the **Accept Subordinate CA Certificates** check box to allow the VPN Concentrator to use such subordinate certificates in certificate path validation. Uncheck the check box to disallow the feature.

Accept Identity Certificates Signed by this Issuer

Check the **Accept Identity Certificates Signed by this Issuer** check box to allow the VPN Concentrator to accept identity certificates signed by this issuer. Uncheck the check box to disallow the feature. If you disallow the feature, any IKE peer certificate signed by this issuer will be rejected.

Apply / Cancel

To configure the CA Certificate parameters for this certificate, click **Apply**. The Manager returns to the Administration | Certificate Management screen.

To discard your settings, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

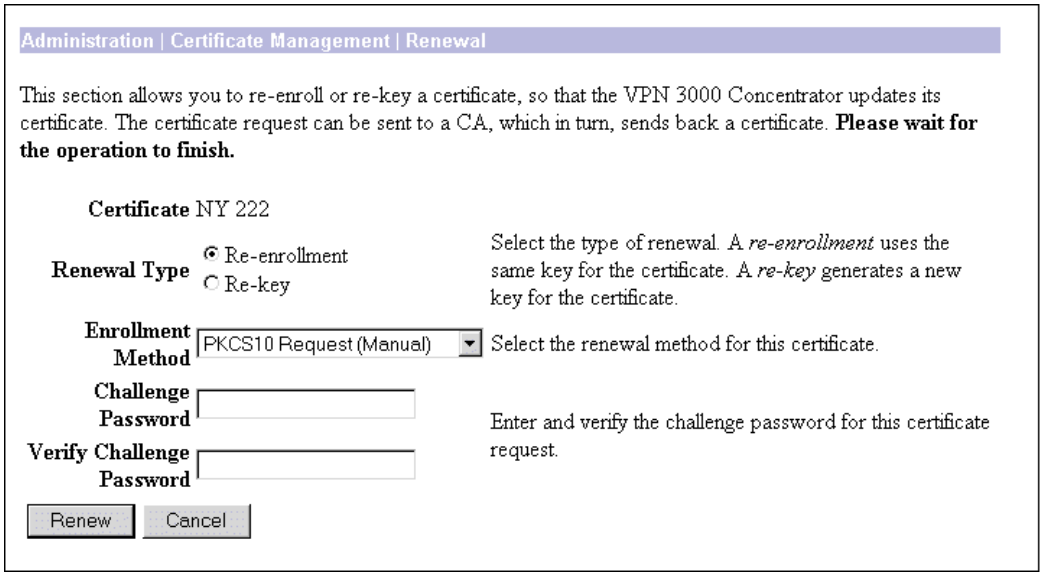
Administration | Certificate Management | Renewal

Certificate renewal is a shortcut that allows you to generate an enrollment request based on the content of an existing certificate.

When you renew a certificate via SCEP, the new certificate does not automatically overwrite the original certificate. It remains in the Enrollment Request table until you manually activate it.

Use this screen to re-enroll or re-key a certificate. If you *re-enroll* the certificate, the new certificate uses the same key pair as the expiring certificate. If you *re-key* the certificate, it uses a new key pair.

Figure 10-50 Administration | Certificate Management | Renewal



Certificate

This field displays the type of certificate that you are re-enrolling or re-keying.

Renewal Type

Specify the type of request:

- Re-enrollment = Use the same key pair as the expiring certificate.
- Re-key = Use a new key pair.

Enrollment Method

Choose an enrollment method:

- PKCS10 Request (Manual) = Enroll using the manual process.
- *Certificate Name* via SCEP = Enroll automatically using this SCEP CA.

Challenge Password

Your CA might have given you a password as a means of verifying your identity. If you have a password from your CA, enter it here.

If you did not receive a password from your CA, choose a password now. You can use this password in the future to identify yourself to your CA.

Verify Challenge Password

Re-type the challenge password you just entered.

Renew / Cancel

To renew the certificate, click **Renew**.

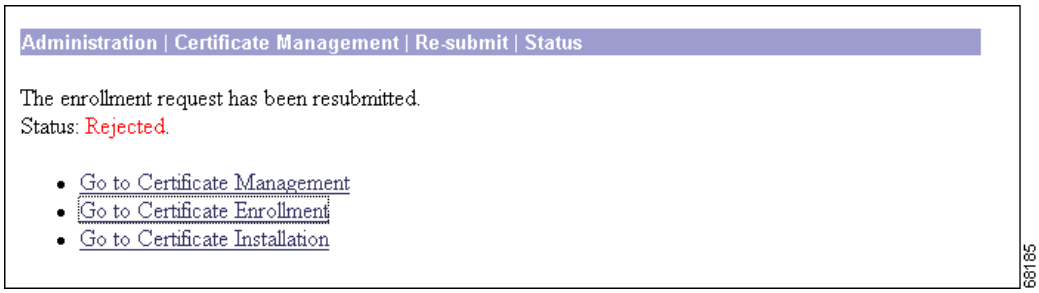
To discard your settings, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

Administration | Certificate Management | *Activate* or *Re-Submit* | Status

This status screen appears after you activate or re-submit an enrollment request. It displays the status of the request.

If you are installing an SSL certificate with a private key, include the encrypted private key.

Figure 10-51 Administration | Certificate Management | Re-Submit | Status Screen



Status

- Installed = The CA returned the certificate and it has been added to the certificate store.
- Rejected = The CA refused to issue a certificate.
- Polling = The CA has pended the approval request; or, CA is unavailable.
- Error = There has been an error processing the enrollment request.

Go to Certificate Management

If you want to view the certificate request, click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen. (See Figure 10-1.)

Go to Certificate Enrollment

If you want to enroll another certificate, click **Go to Certificate Enrollment**. The Manager displays the Administration | Certificate Management | Enroll screen. (See Figure 10-31.)

Go to Certificate Installation

If you want to install the certificate you have just enrolled, click **Go to Certificate Installation**. The Manager displays the Administration | Certificate Management | Install screen. (See Figure 10-39.)

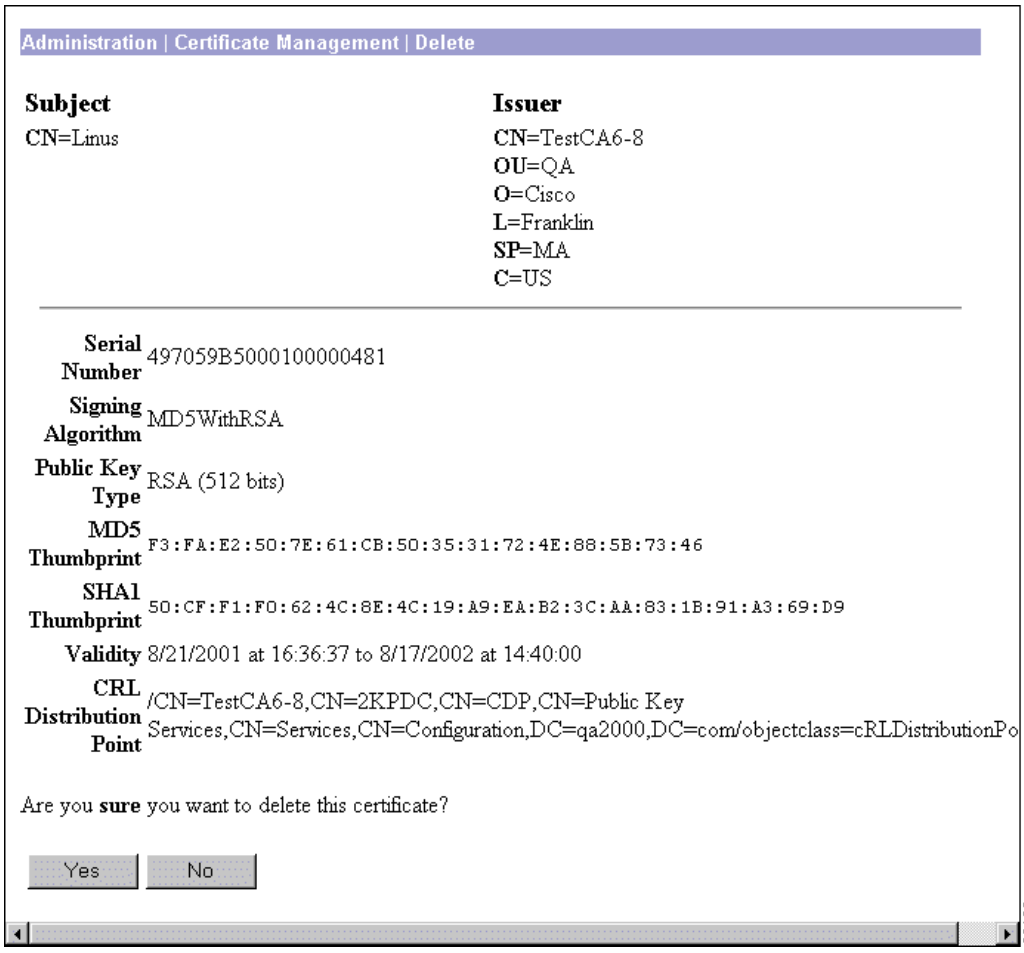
Administration | Certificate Management | Delete

The Manager displays this confirmation screen when you click **Delete** for a certificate on the Administration | Certificate Management screen. The screen shows the same certificate details as on the Administration | Certificate Management | View screen.

Please note:

- You must delete CA certificates from the bottom up: server identity first, then subordinate CA, then root CA certificates last. Otherwise, the Manager displays an error message.
- If the certificate is in use by an SA or referenced in an active enrollment request, the Manager displays an error message.

Figure 10-52 Administration | Certificate Management | Delete Screen



Fields

For a description of the fields in this certificate, see "Certificate Fields".

Yes / No

To delete this certificate, click **Yes**.

Note There is no undo.

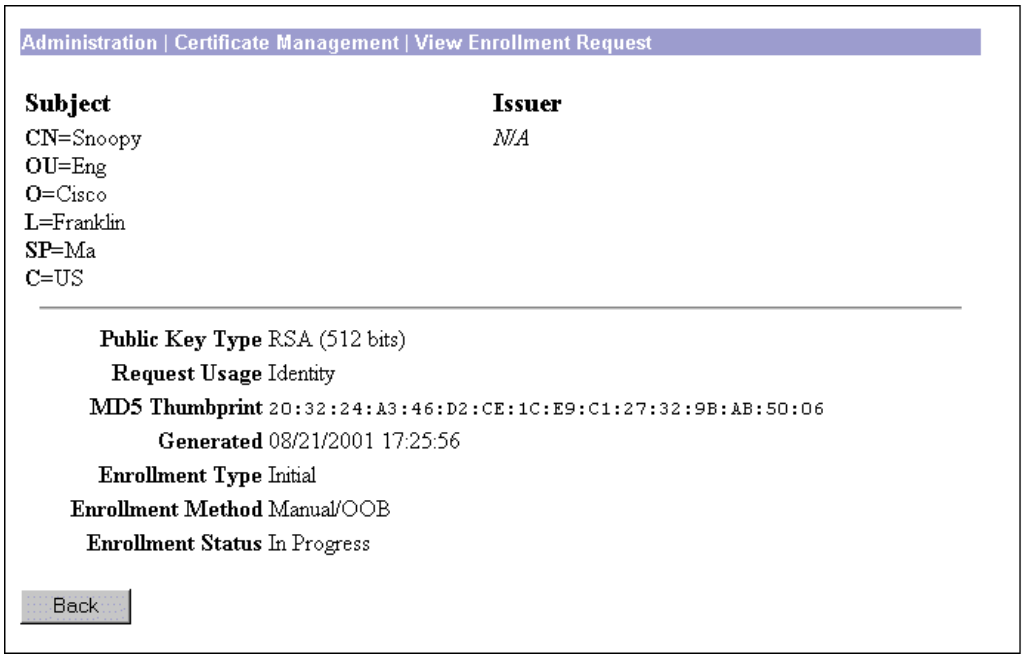
The Manager returns to the Administration | Certificate Management screen and shows the remaining certificates.

To retain this certificate, click **No**. The Manager returns to the Administration | Certificate Management screen, and the certificates are unchanged.

Administration | Certificate Management | View Enrollment Request

This screen allows you to view the details of an enrollment request.

Figure 10-53 Administration | Certificate Management | View Enrollment Request Screen



Enrollment Request Fields

An enrollment request contains some or all of the following fields:

Field	Content
Subject	The person or system that uses the certificate.
Issuer	The CA or other entity from whom the certificate is being requested. 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.

Field	Content
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 Concentrator 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 Concentrator 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.
Public Key Type	The algorithm and size of the public key that the CA or other issuer used in generating this certificate.
Request Usage	The type of certificate: Identity or SSL.
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.
Generated	The date the request was initiated.
Enrollment Type	The type of enrollment: initial, re-enroll, or re-key.
Enrollment Method	The method of enrollment: SCEP or manual.
Enrollment Status	The current status of the enrollment: complete, rejected, error, and so on.

Back

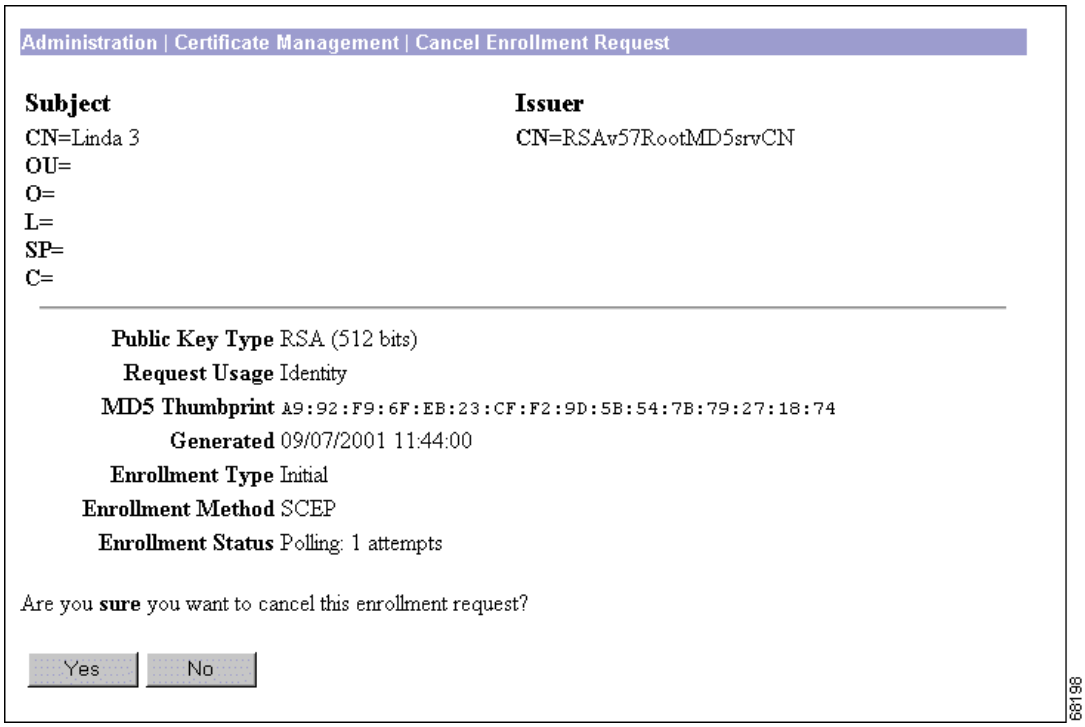
Click **Back** to display the Administration | Certificate Management screen.

Administration | Certificate Management | Cancel Enrollment Request

This screen shows you the details of the enrollment request and allows you to cancel it.

You can cancel only a SCEP enrollment request, and you can do so only when the request is in polling mode. Once a request is cancelled, you can then remove it, re-submit it, or view its details.

Figure 10-54 Administration | Certificate Management | Cancel Enrollment Request Screen



Fields

For a description of the fields in this enrollment request, see "Enrollment Request Fields".

Yes / No

To cancel this enrollment request, click **Yes**. There is no undo.

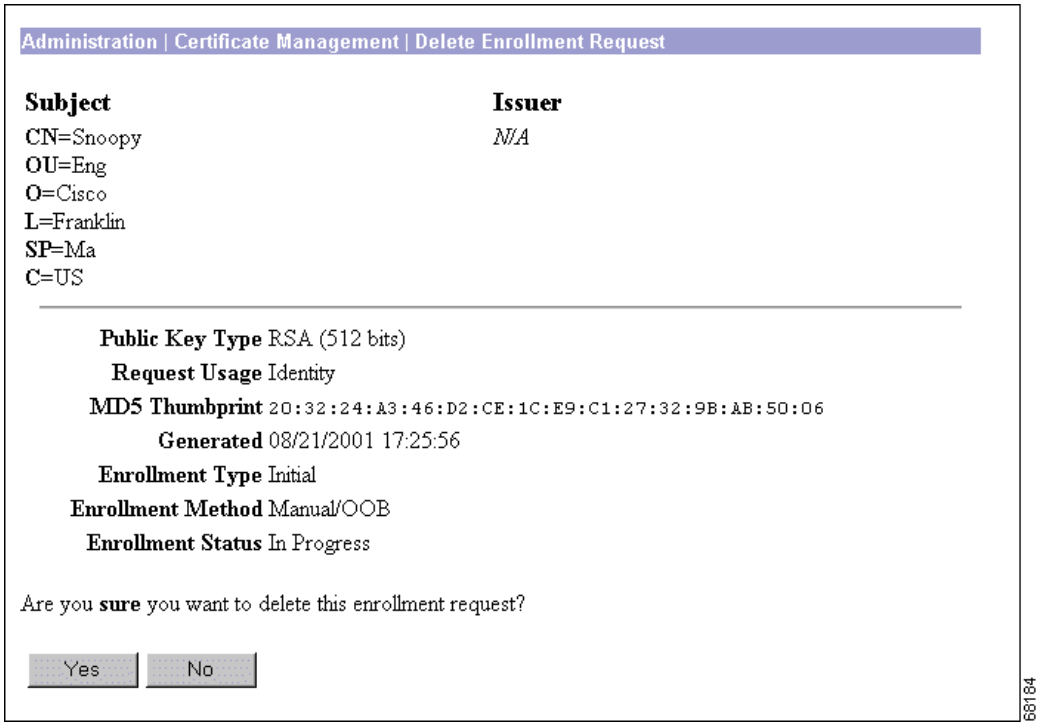
The Manager returns to the Administration | Certificate Management screen.

To retain this enrollment request, click **No**. The Manager returns to the Administration | Certificate Management screen, and the enrollment requests are unchanged.

Administration | Certificate Management | Delete Enrollment Request

This screen shows you details of the enrollment request and allows you to delete it. Deleting an enrollment request removes it from the Enrollment Request table (on the Administration | Certificate Management page) and destroys all record of it.

Figure 10-55 Administration | Certificate Management | Delete Enrollment Request



Fields

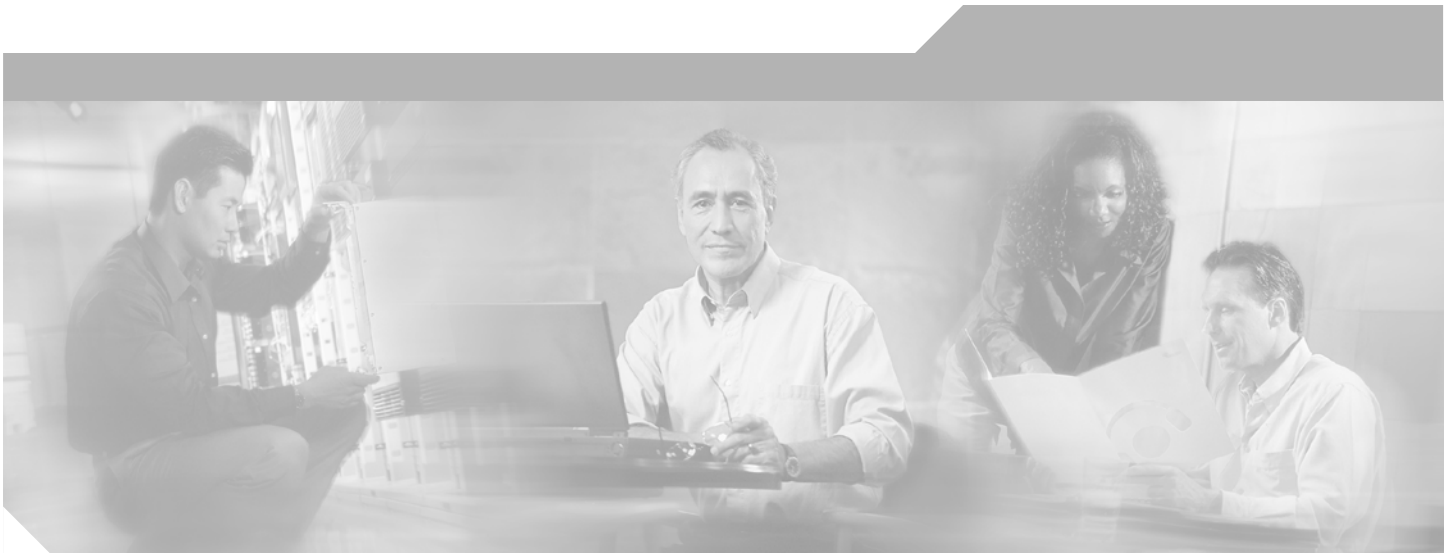
For a description of the fields in this enrollment request, see "Enrollment Request Fields".

Yes / No

To delete this enrollment request, click **Yes**. There is no undo.

The Manager returns to the Administration | Certificate Management screen and shows the remaining enrollment requests.

To retain this enrollment request, click **No**. The Manager returns to the Administration | Certificate Management screen, and the enrollment requests are unchanged.



PART 2

Monitoring

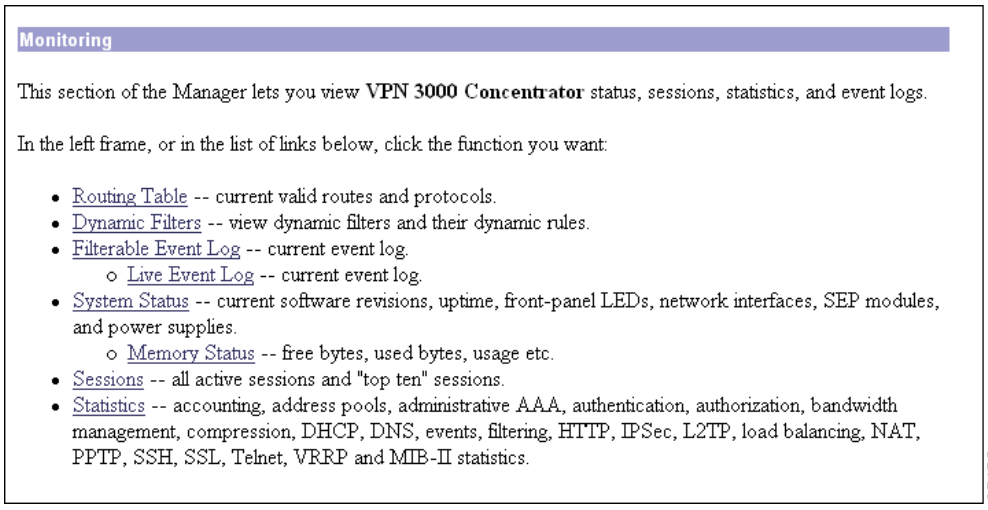
Monitoring

The VPN 3000 Concentrator tracks many statistics and the status of many items essential to system administration and management. Use the VPN Concentrator Manager Monitoring windows to 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

Step 1 In the Concentrator Manager table of contents, click **Monitoring**. The Monitoring screen opens.

Figure 11-1 Monitoring Screen



This section of the Manager lets you view VPN Concentrator status, sessions, statistics, and event logs.

- Routing Table: Current valid routes, protocols, and metrics.
- Dynamic Filters:
- 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, SEP modules, system power supplies, Ethernet interfaces, front-panel LEDs, memory status, and hardware sensors.
  - LED Status: Current status of the VPN Concentrator front-panel LED indicators.
  - Memory Status: Current status of the VPN Concentrator memory use, measured in block size, free blocks and used blocks.
- Sessions: Currently active sessions sorted by protocol, SEP, and encryption. “Top ten” sessions sorted by data, duration, and throughput.
- Statistics: PPTP, L2TP, IPSec, HTTP, events, Telnet, DNS, authentication, accounting, filtering, VRRP, SSL, DHCP, address pools, SSH, load balancing, and data compression. MIB-II statistics for interfaces, TCP/UDP, IP, RIP, OSPF, 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.

You can also configure the Manager to automatically refresh all the screens in this section except the Event Log. See Administration | Monitoring Refresh.

CHAPTER 12

Routing Table

Monitoring | Routing Table

This screen shows the VPN Concentrator routing table at the time the screen displays. The IP routing subsystem examines the destination IP address of packets coming through the VPN Concentrator and forwards or drops them in accordance with configured parameters. The routing table shows the valid forwarding paths that the IP routing subsystem knows about, from whatever source: static routes, learned via routing protocols, interface addresses, etc. However, the table lists only the best routes—based on metric and type—with duplicates removed.

To configure routing, see the Configuration | System | IP Routing and Configuration | Interfaces screens.

Figure 12-1 Monitoring | Routing Table Screen

Monitoring | Routing Table — Wednesday, 12 March 2003 11:52:51

Refresh

Clear Routes

Valid Routes: 16

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	80.124.1.1	2	Default	0	1
5.0.0.0	255.0.0.0	90.124.100.100	1	Static	0	1
73.2.3.0	255.255.255.252	80.124.10.240	2	Static	0	1
73.6.1.0	255.255.255.248	80.124.10.240	2	Static	0	1
73.7.1.0	255.255.255.248	80.124.10.240	2	Static	0	1
73.9.1.0	255.255.255.248	80.124.10.240	2	Static	0	1
73.83.93.0	255.255.255.252	80.124.10.240	2	Static	0	1
73.84.87.80	255.255.255.240	80.124.10.240	2	Static	0	1
73.88.31.0	255.255.255.192	80.124.10.240	2	Static	0	1
75.0.0.0	255.0.0.0	80.124.0.1	2	Static	0	1
80.124.0.0	255.252.0.0	0.0.0.0	2	Local	0	1
83.0.0.0	255.0.0.0	90.124.0.1	1	Static	0	1
90.0.0.0	255.0.0.0	90.124.1.1	1	Static	0	1
90.124.0.0	255.252.0.0	0.0.0.0	1	Local	0	1
93.4.2.0	255.255.255.248	80.124.10.240	2	Static	0	1
100.0.0.0	255.0.0.0	90.124.1.1	1	Static	0	1

87660

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Clear Routes

Click the **Clear Routes** button to clear the dynamic routing entries, such as RIP and OSPF, 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 Concentrator 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 to which this route applies. 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. There is no next hop.

Interface

The VPN Concentrator network interface through which traffic moves on this route:

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.

Protocol

The protocol or source of this routing table entry:

- RIP = Learned via Routing Information Protocol.
- OSPF = Learned via Open Shortest Path First protocol.
- Static = Configured static route.
- Local = Local VPN Concentrator 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, for example: 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. One is the lowest value; sixteen is the highest value.

CHAPTER 13

Dynamic Filters

Monitoring | Dynamic Filters

The VPN Concentrator allows you to define remote access user filters on an external RADIUS server, such as Cisco Secure ACS, rather than on the VPN Concentrator. Using an external RADIUS server allows centralized filter management and greater scaleability. Also, configuring filters in this way allows you to assign filters to a particular tunnel group or a particular user.

These filters are called *dynamic filters* because they remain in place only for the duration of the session to which they apply. When a user authenticates via RADIUS, the VPN Concentrator downloads the filter associated with the user and applies it for the duration of the connection. When the connection finishes, the filter drops.

You configure this feature on the RADIUS server, not on the VPN Concentrator. (The filters you configure on the VPN Concentrator are *static*.) For guidelines on configuring your external RADIUS server to inter operate with the VPN Concentrator, see Configuring Dynamic Filters on a RADIUS Server, page 13-4.

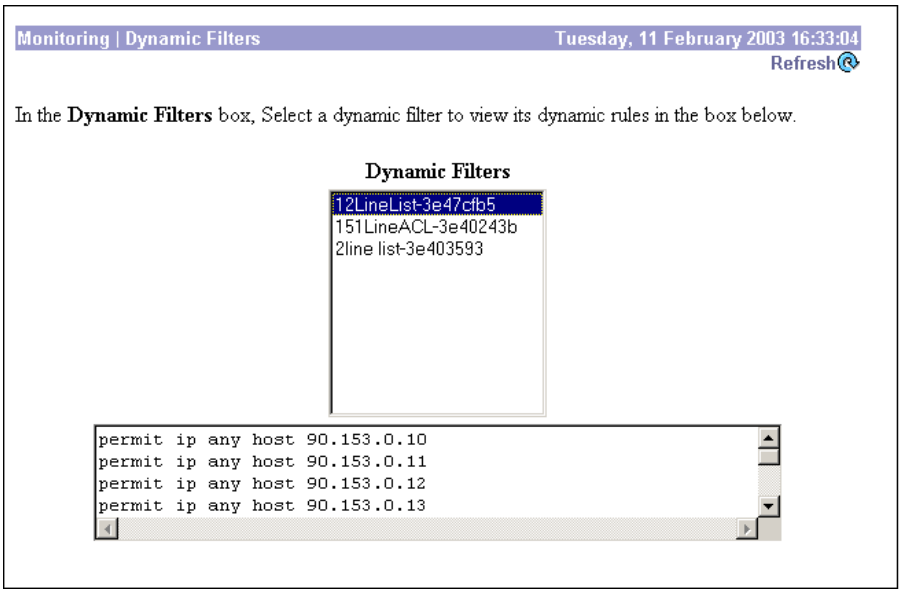
You can configure a dynamic filter on either a user or a group. If both user dynamic filters and group dynamic filters apply to a single connection, the user filters take precedence. If both dynamic filters and static filters apply to the same connection, the dynamic filters take precedence. The order of precedence is:

1. A dynamic user filter
2. A dynamic group filter
3. A static user filter
4. A static group filter

Tip If you encounter problems using this feature, debug by tracking the FILTERDBG event class. Track events with severity level 6 if you are concerned about filter syntax errors; the error log shows how the VPN Concentrator parses the filter. To view the actual filtering, track events with severity level nine; in this case, be sure to define the filter using the keyword “log.”

This screen displays the dynamic filters currently in use governing remote access sessions on the VPN Concentrator.

Figure 13-1 Monitoring | Dynamic Filters Screen



Dynamic Filters

This list shows the unique dynamic filters currently in use on the VPN Concentrator. Select a filter to view its associated rules in the text box below.

The syntax of each rule is as follows:

[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]:

Field	Description
Prefix	An unique identifier for the AV pair. For example: `ip:inacl#1=`. This field only appears when the filter has been sent as an AV pair.
Action	Action to perform if rule matches: deny, permit.
Protocol	Number or name of an IP protocol. Either an integer in the range 0-255 or one of the following keywords: icmp, igmp, ip, tcp, udp.
Source	Network or host from which the packet is sent, specified as an IP address, a hostname, or the keyword “any”. If specified as an IP address, the source wildcard mask must follow.
Source Wildcard Mask	The wildcard mask to be applied to the source address.
Destination	Network or host to which the packet is sent, specified as an IP address, a hostname, or the keyword “any”. If specified as an IP address, the source wildcard mask must follow.
Destination Wildcard Mask	The wildcard mask to be applied to the destination address.
Log	Generates a FILTER log message. You must use this keyword to generate events of severity level 9.
Operator	Logic operators: greater than, less than, equal to, not equal to.
Port	The number of a TCP or UDP port: in the range 0-65535.

Configuring Dynamic Filters on a RADIUS Server

You can configure dynamic filters on any RADIUS server by using the Cisco vendor-specific RADIUS attribute (26/9/1) AV-Pair to define and transmit attribute/value pairs. In configuring the feature, refer to Table 13-1 for a list of tokens the VPN Concentrator supports.

For more information, see the documentation for your particular server.

Table 13-1 VPN Concentrator-Supported Tokens.

Token	Syntax Field	Description
ip:inacl#*Num*=	N/A (Identifier)	(Where *Num* is a unique integer.) Starts all AV pair access control lists.
deny	Action	Denies action. (Default.)
permit	Action	Allows action.
icmp	Protocol	Internet Control Message Protocol (ICMP)
1	Protocol	Internet Control Message Protocol (ICMP)
IP	Protocol	Internet Protocol (IP)
0	Protocol	Internet Protocol (IP)
TCP	Protocol	Transmission Control Protocol (TCP)
6	Protocol	Transmission Control Protocol (TCP)
UDP	Protocol	User Datagram Protocol (UDP)
17	Protocol	User Datagram Protocol (UDP)
any	Hostname	Rule applies to any host.
host	Hostname	Any alpha-numeric string that denotes a hostname.
log	Log	When the event is hit, a filter log message appears. (Same as permit and log or deny and log.)
lt	Operator	Less than value
gt	Operator	Greater than value
eq	Operator	Equal to value
neq	Operator	Not equal to value
range	Operator	Inclusive range. Should be followed by two values.

Cisco Secure ACS

To configure dynamic filters in Cisco Secure ACS, use either of the following screens:

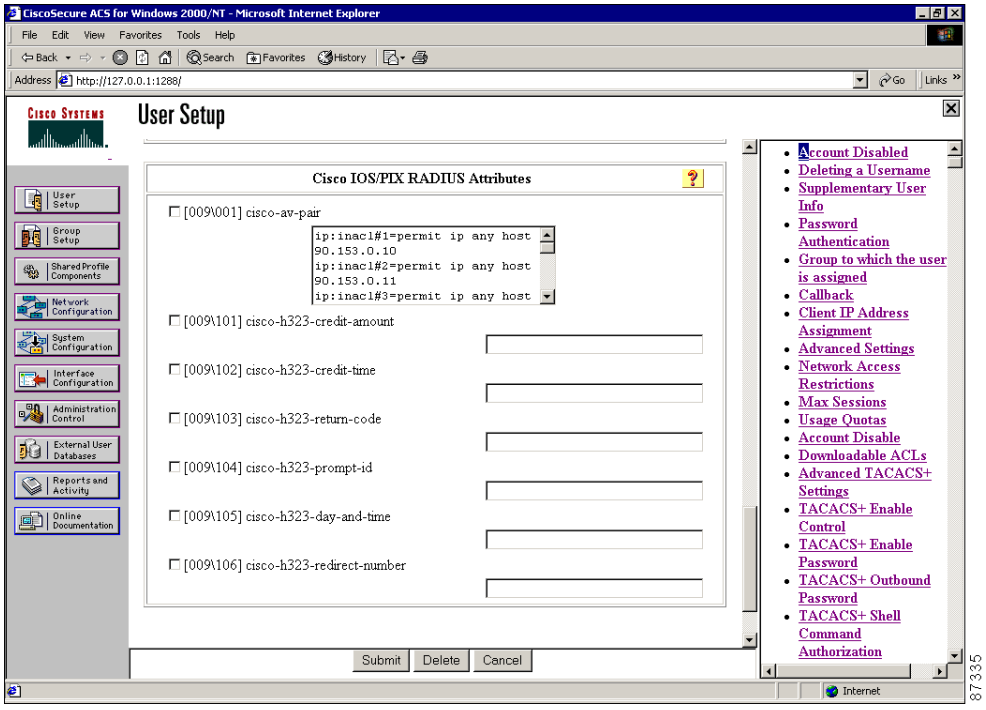
- The Cisco IOS/PIX RADIUS Attributes screen
- The Downloadable PIX ACLs screen

Cisco IOS/PIX RADIUS Attributes Screen

On the Cisco IOS/PIX RADIUS Attributes screen, enter the filter in the **cisco-av-pair** text box. Include the Access List Number. (See Figure 13-2.) For example:

```
ip:inacl#1=permit ip 90.153.0.0 0.0.255.255 host 100.158.9.1
ip:inacl#2=permit ip 90.154.0.0 0.0.255.255 100.158.10.0 0.0.0.255
ip:inacl#3=permit 0 any host 100.159.1.22
ip:inacl#4=deny ip 90.155.10.0 0.0.0.255 100.159.2.0 0.0.0.255 log
ip:inacl#4=permit TCP any host 100.160.0.1 eq 80 log
ip:inacl#5=permit TCP any host 100.160.0.2 eq 23 log
ip:inacl#6=permit TCP any host 100.160.0.3 range 20 30
ip:inacl#7=permit 6 any host HOSTNAME1
ip:inacl#8=permit UDP any host HOSTNAME2 neq 53
ip:inacl#9=deny 17 any host HOSTNAME3 lt 137 log
ip:inacl#10=deny 17 any host HOSTNAME4 gt 138
ip:inacl#11=deny ICMP any 100.161.0.0 0.0.255.255 log
ip:inacl#12=permit TCP any host HOSTNAME5 neq 80
```

Figure 13-2 Cisco IOS/PIX RADIUS Attributes screen

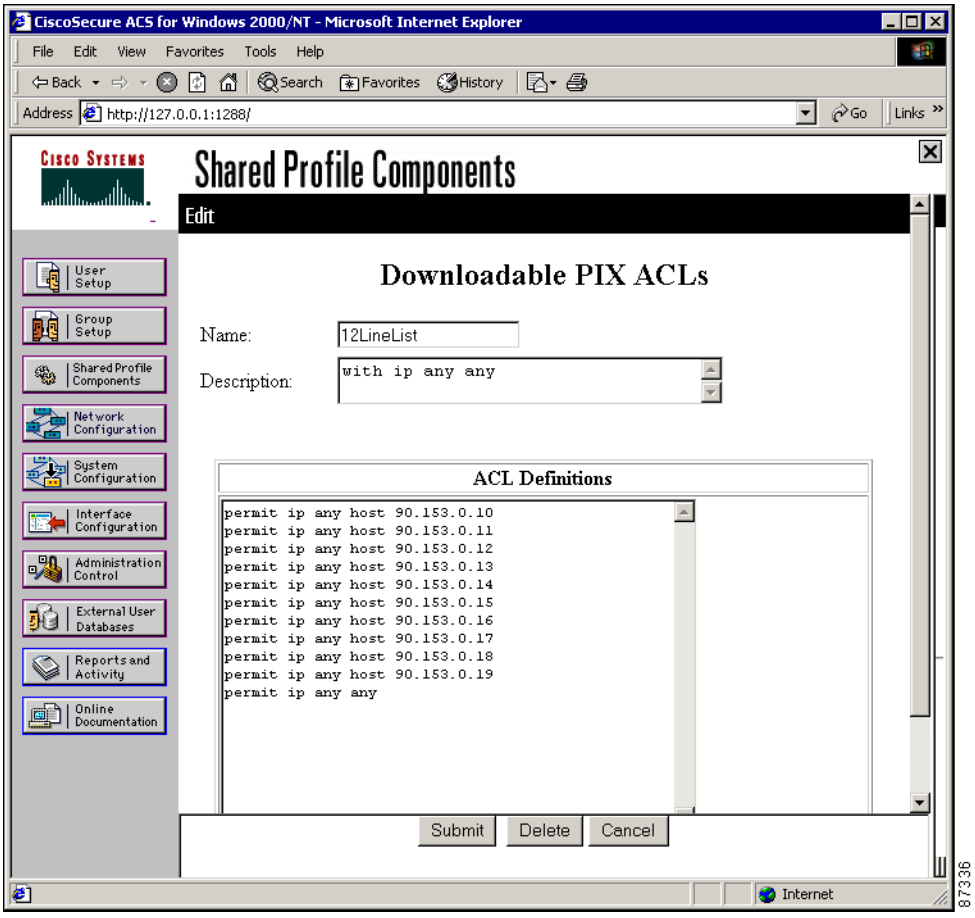


Downloadable PIX ACLs Screen

On the Downloadable PIX ACLs screen, enter the filter in the ACL Definitions box. Omit the Access List Number. (See Figure 13-3.) For example:

```
permit ip 90.153.0.0 0.0.255.255 host 100.158.9.1
permit ip 90.154.0.0 0.0.255.255 100.158.10.0 0.0.0.255
permit 0 any host 100.159.1.22
deny ip 90.155.10.0 0.0.0.255 100.159.2.0 0.0.0.255 log
permit TCP any host 100.160.0.1 eq 80 log
permit TCP any host 100.160.0.2 eq 23 log
permit TCP any host 100.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 100.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

Figure 13-3 Downloadable PIX ACLs Screen



Filterable Event Log

Monitoring | Filterable Event Log

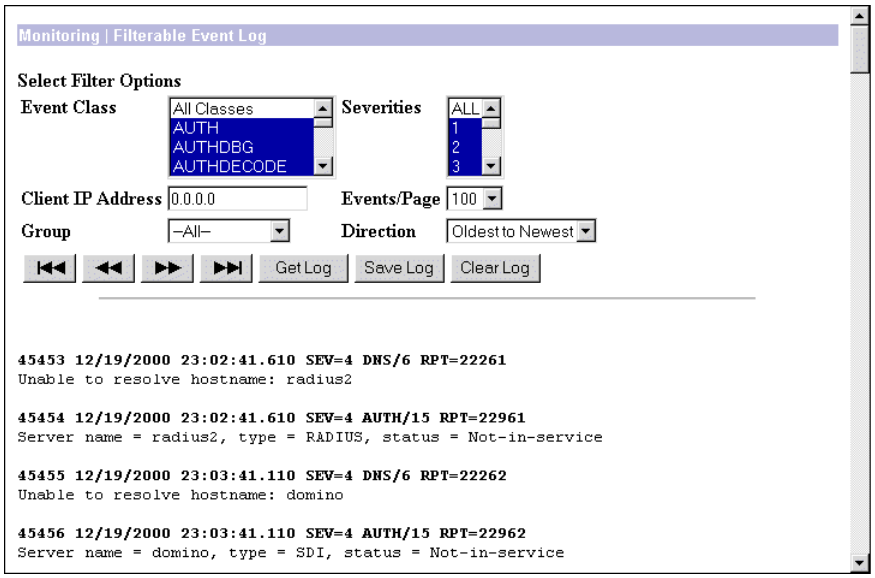
This screen shows the events in the current event log, lets you filter and display events by various criteria, and lets you manage the event log file. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN Concentrator records events in nonvolatile memory, thus the event log persists even if the system is powered off. The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events, and it wraps when it is full; that is, entry 2049 (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 14-1 Monitoring | Filterable Event Log Screen



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 in accordance with 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 **Event Class** drop-down menu button and choose the event class. To choose 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. For a description of event classes, refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

Severities

To display all events of a single severity level, click the **Severities** drop-down menu button and choose the severity level. To choose 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. For an explanation of event severity levels, refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

Client IP Address

To display all events relating to a single IP address, enter the IP address in the field using dotted decimal notation, for example: 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 **Events/Page** drop-down menu button and choose the number. Choices are 10, 25, 50, 100, 250, and ALL. By default, the Manager displays 100 events per screen.

Group

Choose a group from the menu to monitor events for that group only. The default is --All--, which displays events for all groups.

Direction

To display events in a different chronological order, click the **Direction** drop-down menu button and choose 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 the first page 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 the previous page button.

Next Page 

To display the next page (screen) of the event log, click the next page button.

Last Page 

To display the last page (screen) of the event log, click the last page button.

All four Page buttons are also present at the bottom of the screen.

Get Log

To download the event log from VPN Concentrator 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 Concentrator address and log file default filename; for example, `10.10.4.6/LOG/vpn3000log.txt`.

To save a copy of the log file on your PC, click the **File** menu on the *new* browser window and choose **Save As....** The browser opens a dialog box that lets you save the file. The default filename is `vpn3000log.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 of which the 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.
- 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 vpn3000log.txt.

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

Save Log

To save a copy of the current event log as a file *on the VPN Concentrator*, click the **Save Log** button. The browser prompts you for a filename, which must conform to the 8.3 naming convention.

Caution If the filename you enter is the same as an existing file, the browser overwrites the existing file without asking for confirmation.

To list and manage files on the VPN Concentrator, see the Administration | File Management screen.

Clear Log

To clear the current event log from memory, click the **Clear Log** 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 feature for this action.*

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 only appears in 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 number of the logged entry. Event sequence numbers are sequential (they proceed from lower to higher) but not consecutive. For example, a series of events could have the following sequence numbers: 1, 2, 4, 7, 8.

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 2048 entries (Model 3015–3080; 256 entries on Model 3005), numbering continues with event 2049 (or 257) overwriting event 1. The maximum sequence number is 65536.

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. For an explanation of event severity levels, refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

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 Concentrator using HTTP to connect to the Manager. For a description of event classes, refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration*. 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 Concentrator was last booted or reset. For example, RPT=17 indicates that this is the seventeenth 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, 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, "`New administrator login: admin`" describes the event.

Monitoring | Live Event Log

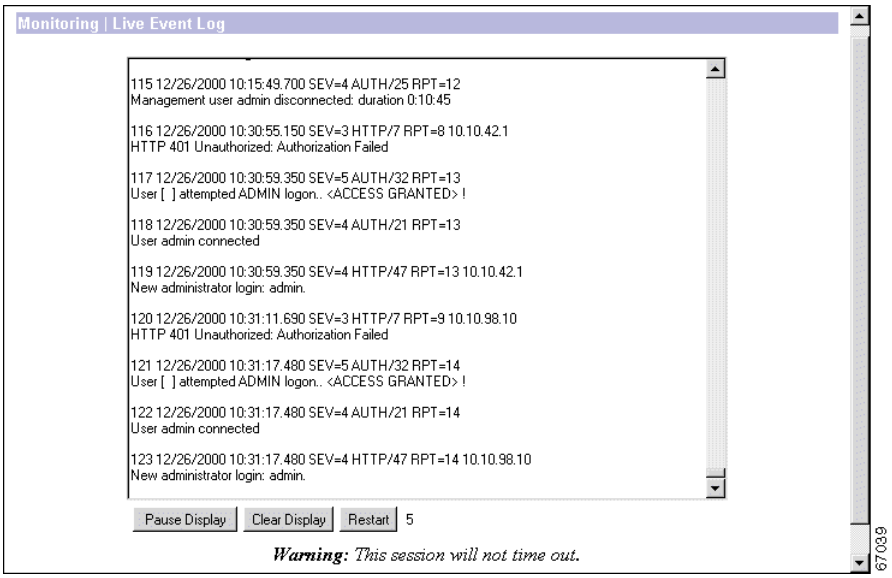
Note The live event log requires Netscape versions 4.5- 4.7 or 6.0. It does not run on other versions of Netscape.

This screen shows events in the current event log and automatically updates the display every 5 seconds. The events might take a few seconds to load when you first open the screen.

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.

Note If you keep this VPN Concentrator 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 14-2 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**. This action *does not* clear the event log, only the display of events on this screen.

Timer

The timer counts `5 – 4 – 3 – 2 – 1` to show where it is in the 5-second refresh cycle. A momentary `Receiving...` indicates receipt of new events. A steady `0` indicates the display has been paused.

CHAPTER 15

System Status

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 and statistics for SEP modules, system power supplies, memory, and network interfaces.

Figure 15-1 Monitoring | System Status Screen (Model 3005)

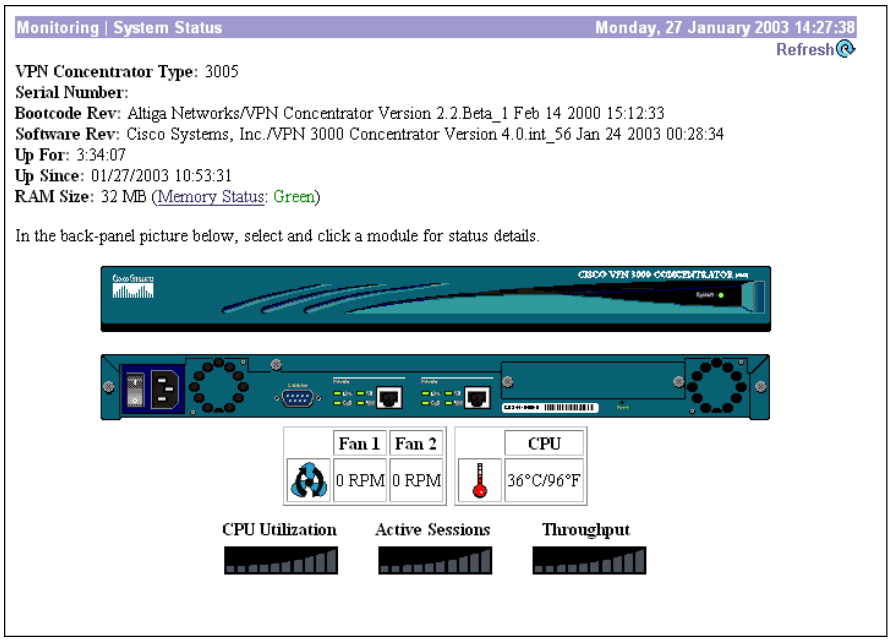
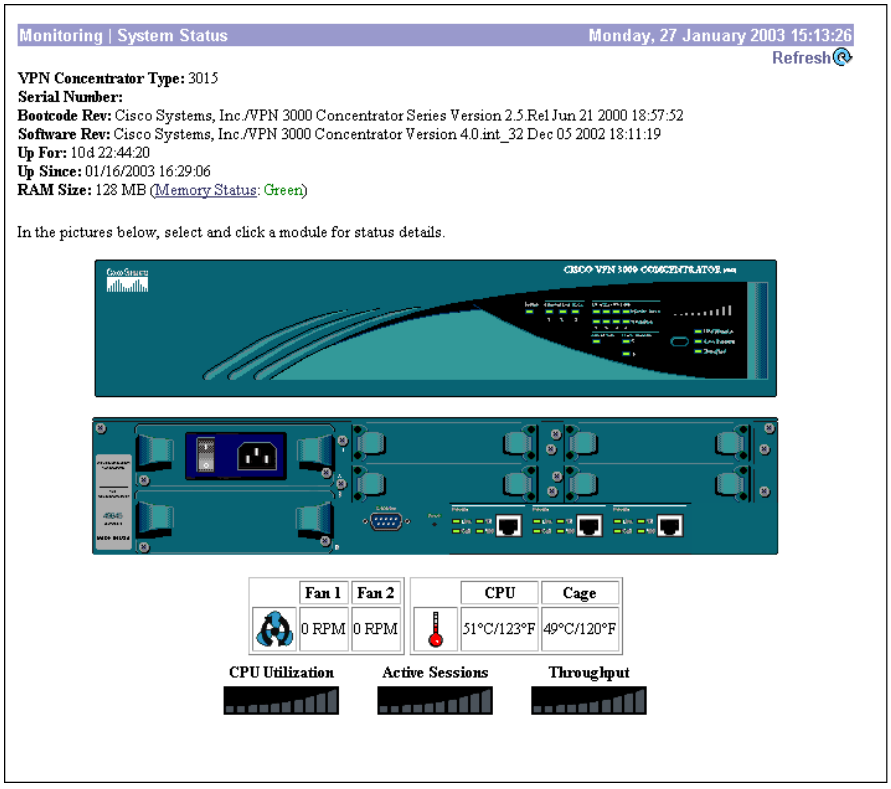


Figure 15-2 Monitoring | System Status Screen (Models 3015-3080)



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

VPN Concentrator Type

The type, or model number, of this VPN Concentrator.

Bootcode Rev

The version name, number, and date of the VPN Concentrator 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.

For instructions on upgrading the bootcode, refer to *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator.*

Software Rev

The version name, number, and date of the VPN Concentrator system software image file. You can update this image file from the Administration | Software Update screen.

Up For

The amount of time since the VPN Concentrator was last booted or reset.

Up Since

The date and time that the VPN Concentrator was last booted or reset.

RAM Size

The total amount of SDRAM memory installed in the VPN Concentrator. *Memory Status* is a link to a table that displays information about memory use on the VPN Concentrator; it includes information about block size, with data about used and free blocks, bytes, and percentages.

Front Panel

On models 3015-3080, the front panel image is an active link. Put the mouse pointer anywhere within the image and click. The Manager displays the Monitoring | System Status | LED Status screen.

Back Panel

The back panel image includes active links for configurable modules installed in the VPN Concentrator: Ethernet interfaces, power supplies, and SEP or SEP-E modules. Use the mouse pointer to select a module on the back-panel image and click anywhere in the highlighted area. The Manager displays the appropriate Monitoring | System Status | Interface, Power, or SEP screen.

Tip To find out if you have a SEP or SEP-E module installed, move the mouse pointer over the module in the back panel image. A pop-up appears that describes the type of module installed.

The VPN Concentrator does not support simultaneous SEP and SEP-E modules. If both are installed, the VPN Concentrator disables the SEP module and uses only the SEP-E. In this case, the back panel image shows the SEP module as "DISABLED."

Fan 1, Fan 2

The VPN Concentrator includes two cooling fans. In the Model 3005, they are on the rear of the chassis, with Fan 1 on the left as you face the rear. In the Model 3015–3080, they are on the right side of the chassis as you face the front, with Fan 1 closest to the front. This table shows the RPM for both fans. The nominal value is 5000 RPM for the Model 3005 and 3800 RPM for the Model 3015–3080, with an acceptable minimum of 3000 RPM for both. Values below this minimum trigger a hardware event.

CPU, Cage

The VPN Concentrator Model 3015–3080 includes two temperature sensors on the main printed circuit board: one near the CPU and one near the power supply cage. The Model 3005 has one sensor near the CPU. This table shows the temperature at the sensor(s). Temperatures between 0° and 50°C (32° and 122°F) are acceptable. Values outside this range trigger a hardware event.

CPU Utilization

This usage graph shows the CPU load as a percentage of the maximum possible load. Each segment represents ten percent of the maximum possible load.

Active Sessions

This usage graph shows the number of active sessions as a percentage of the maximum possible sessions. For example, if 5000 sessions is the maximum, each segment represents 500 sessions. The first segment lights with the first session, the second segment lights with 10 percent plus one session, etc.

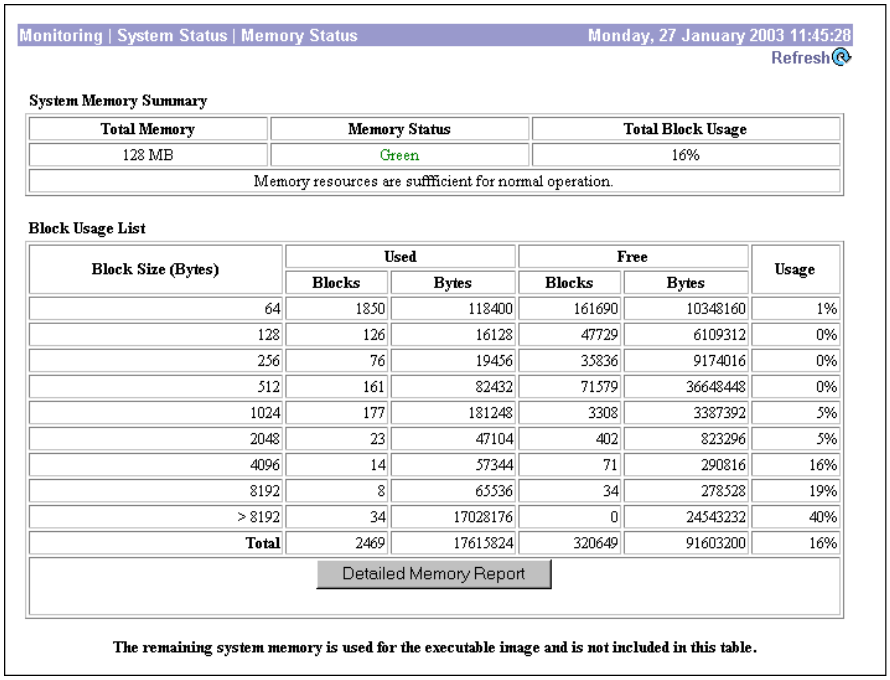
Throughput

This usage graph shows current throughput (measured in LAN packets) as a percentage of the maximum possible system throughput. For example, if two interfaces are set for 100 Mbps, the maximum possible throughput is 200 Mbps and each segment represents 20 Mbps.

Monitoring | System Status | Memory Status

This screen displays status and data for the VPN Concentrator system memory.

Figure 15-3 Monitoring | System Status | Memory Status Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

System Memory Summary

This section summarizes memory use on the VPN Concentrator.

Total Memory

Total amount of system memory, in megabytes, on the VPN Concentrator.

Memory Status

Green: Sufficient memory resources are available for normal VPN Concentrator operations.

Red: Memory resources are critically low; new IPSec, PPTP and L2TP connections are prevented.

Note It is possible for Memory Status to be Red, preventing new connections, even while total memory usage is significantly less than 100%. This is because some VPN Concentrator functions and features require specific block sizes to operate, and those block sizes are critically low. If this occurs, follow the instructions in the section, "Memory Detail Report" that follows.

Total Block Usage

Memory use in total percent of blocks currently in use.

Block Usage List

Provides a list of blocks by size and number, both used and free.

Block Size (Bytes)

The number of blocks by size of block in bytes.

Used/Free Blocks

The number of used blocks and free blocks.

Used/Free Bytes

The number of uesd bytes and free bytes.

Usage

The percentage of blocks in use.

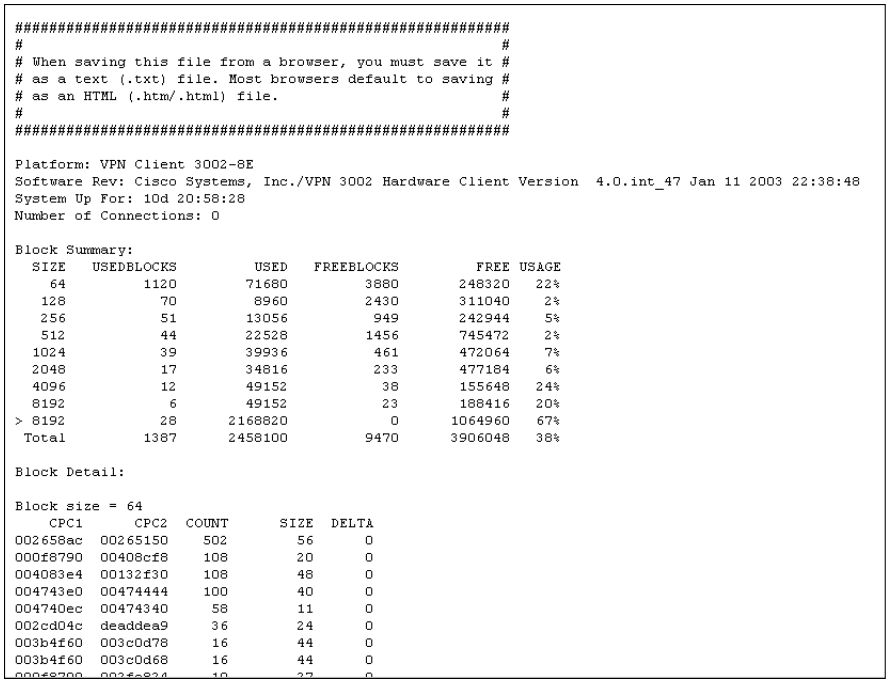
Memory Detail Report

Click this button to generate a text file that displays in a new window.

Memory Detail Report

This screen displays a text file that summarizes memory use on the VPN Concentrator. You can view, copy, save, or delete "Memory.txt" using file management. If necessary, you can send this file to the Cisco TAC by email to help with trouble-shooting.

Figure 15-4 Memory Detail Report



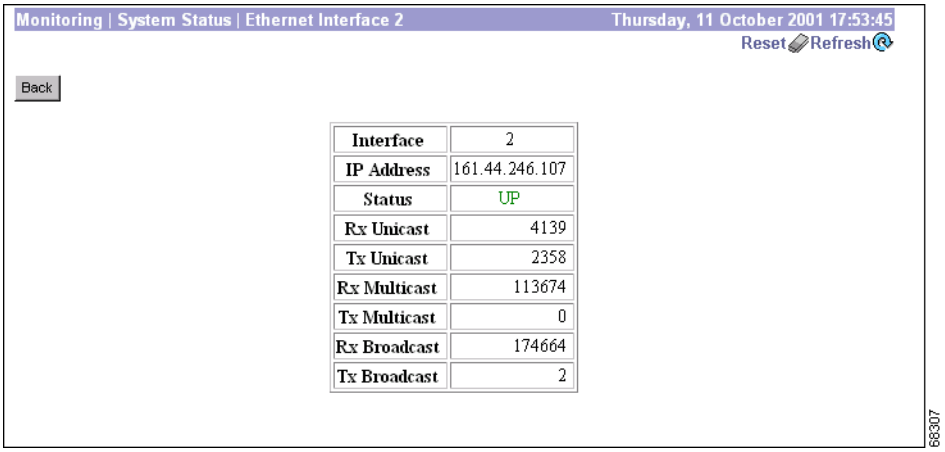
```
############################################################
#                                                          #
# When saving this file from a browser, you must save it #
# as a text (.txt) file. Most browsers default to saving #
# as an HTML (.htm/.html) file.                            #
#                                                          #
############################################################

Platform: VPN Client 3002-8E
Software Rev: Cisco Systems, Inc./VPN 3002 Hardware Client Version  4.0.int_47 Jan 11 2003 22:38:48
System Up For: 10d 20:58:28
Number of Connections: 0

Block Summary:
  SIZE   USEDBLOCKS         USED   FREEBLOCKS         FREE USAGE
    64          1120        71680         3880       248320   22%
   128            70         8960         2430       311040    2%
   256            51        13056          949       242944    5%
   512            44        22528         1456       745472    2%
  1024            39        39936          461       472064    7%
  2048            17        34816          233       477184    6%
  4096            12        49152           38       155648   24%
  8192             6        49152           23       188416   20%
> 8192            28      2168820            0      1064960   67%
 Total          1387      2458100         9470      3906048   38%

Block Detail:

Block size = 64
    CPC1      CPC2  COUNT      SIZE  DELTA
002658ac  00265150    502        56      0
000f8790  00408cf8    108        20      0
004083e4  00132f30    108        48      0
004743e0  00474444    100        40      0
004740ec  00474340     58        11      0
002cd04c  deaddea9     36        24      0
003b4f60  003c0d78     16        44      0
003b4f60  003c0d68     16        44      0
```

90196

Monitoring | System Status | Ethernet Interface

This screen displays status and statistics for a VPN Concentrator Ethernet interface. To configure an interface, see Configuration | Interfaces.

Figure 15-5 Monitoring | System Status | Ethernet Interface Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator Ethernet interface number:

- 1 = Private interface.
- 2 = Public interface.
- 3 = External 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 Concentrator 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 Concentrator 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 Concentrator 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 Concentrator 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 Concentrator 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 Concentrator 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 | System Status | Power

This screen displays status and data for VPN Concentrator power supplies and voltage sensors in the system. To configure alarm thresholds for system voltages, see the Configuration | Interfaces | Power screen.

Figure 15-6 Monitoring | System Status | Power Screen (Model 3005)

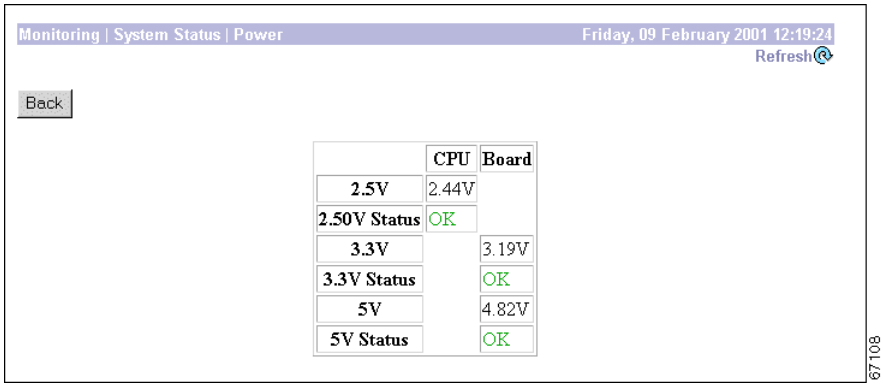
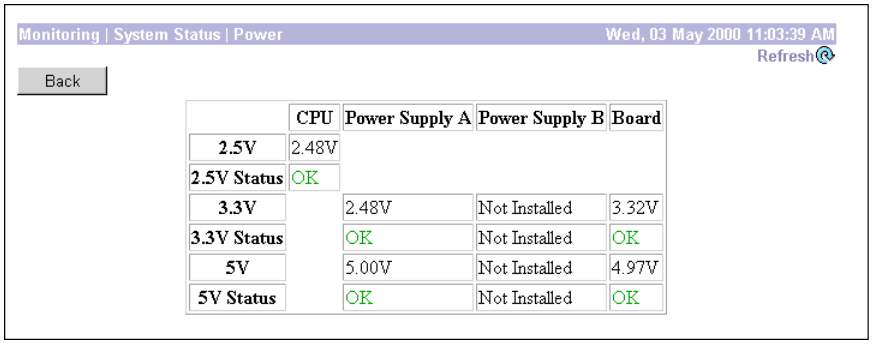


Figure 15-7 Monitoring | System Status | Power Screen (Models 3015-3080)



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**.

CPU

Voltage and status for the voltage sensor on the CPU chip. The screen shows either 1.9 or 2.5 volts, depending on the CPU chip in the system.

Power Supply A, B

Voltages and status of the 3.3- and 5-volt outputs from the power supplies.

Board

Voltages and status of the 3.3- and 5-volt sensors on the main circuit board.

1.9/2.5V Status, 3.3V Status, 5V Status

The status of voltages relative to the configured thresholds:

- OK = within low and high threshold limits.
- ALARM = outside of low or high threshold limit.
- Not Installed = power supply not installed.

Monitoring | System Status | SEP

Note This screen appears on models 3015–3080 only.

This screen displays status and statistics for a VPN Concentrator SEP (Scalable Encryption Processing) or a SEP-E (Enhanced SEP) module, which performs hardware-based cryptographic functions:

- Random-number generation.
- Hash transforms (MD5 and SHA-1) for authentication.
- Encryption and decryption (DES and Triple-DES).

The screen shows cumulative data since the system was last booted or reset.

SEP Redundancy

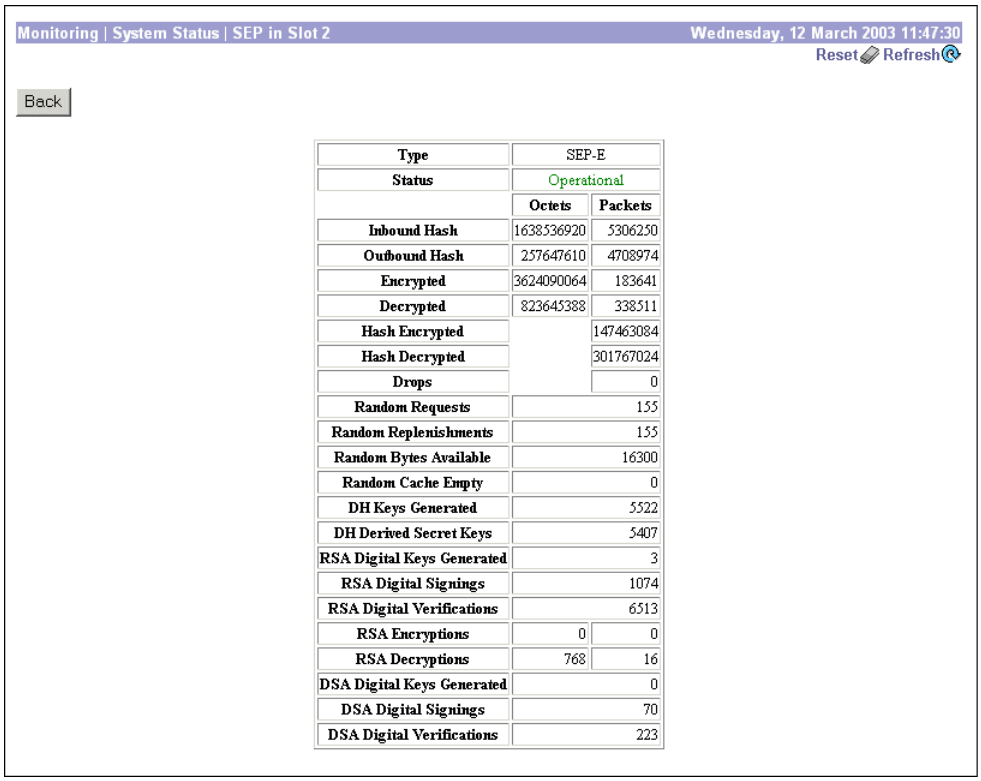
The VPN Concentrator can contain up to four SEP or SEP-E modules for maximum system throughput and redundancy. Two SEP modules provide maximum throughput; additional modules provide redundancy in case of module failure.

SEP redundancy requires no configuration: it is always enabled and completely automatic; no administrator action is required. If a SEP module fails, the VPN Concentrator automatically switches active sessions to another SEP module. If the system has only one SEP module and it fails, the sessions automatically use software cryptographic functions. Even if a SEP module fails, the VPN Concentrator supports the number of sessions for which it is licensed.

Note Only SEPs of the same type provide redundancy. For example, if a SEP fails, the VPN Concentrator can switch sessions only to another SEP, not to a SEP-E.

If a SEP module fails, the system generates an event of severity level 2. It continues to generate an event every 10 minutes until the failed module is removed or replaced and the VPN Concentrator is rebooted. The front- and back-panel Status LEDs also indicate the failed module, as does this screen.

Figure 15-8 Monitoring | System Status | SEP Screen (For SEP-E)



Type	SEP-E	
Status	Operational	
	Octets	Packets
Inbound Hash	1638536920	5306250
Outbound Hash	257647610	4708974
Encrypted	3624090064	183641
Decrypted	823645388	338511
Hash Encrypted		147463084
Hash Decrypted		301767024
Drops		0
Random Requests		155
Random Replenishments		155
Random Bytes Available		16300
Random Cache Empty		0
DH Keys Generated		5522
DH Derived Secret Keys		5407
RSA Digital Keys Generated		3
RSA Digital Signings		1074
RSA Digital Verifications		6513
RSA Encryptions	0	0
RSA Decryptions	768	16
DSA Digital Keys Generated		0
DSA Digital Signings		70
DSA Digital Verifications		223

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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**.

Type

The type of SEP module installed in this slot:

- CryptSet = first-release hardware using a set of integrated circuits.
- CryptIC = second-release hardware using a single integrated circuit.
- SEP-E = third-release hardware using an enhanced single integrated circuit.
- Unknown = hardware could not be determined. *This is an error condition*; please contact Cisco Customer Support.

Status

The functional state of this SEP module:

- Operational = module is operating correctly.
- Not Operational = module has failed during operation. *This is an error condition*; please contact Cisco Customer Support.
- Disabled = SEP module has been disabled because both SEP and SEP-E modules are installed on the VPN Concentrator. The VPN Concentrator does not support simultaneous SEP and SEP-E modules. *This is an error condition*. Remove the SEP module. For instructions on removing the SEP module, refer to *Installing SEP or SEP-E Modules in the VPN 3000 Series Concentrator.*
- Found = module is installed but is not yet operational. If this condition persists after the VPN Concentrator finishes initializing, it is an error. Please contact Cisco Customer Support.
- Not Found = module could not be found. *This is an error condition*; please contact Cisco Customer Support.
- Loading = the system is loading microcode into the SEP module.
- Initializing = the system is initializing the SEP module.
- Diagnostic Failure = module failed during diagnostic testing. *This is an error condition*; please contact Cisco Customer Support.

DSP Code Version

The version of DSP (Digital Signal Processing) microcode running on this SEP module. This information might be useful during troubleshooting.

This field appears for SEP modules only; it does not appear for SEP-E modules.

Inbound Hash: Octets

The number of inbound octets (bytes) to which this SEP applied a hashing algorithm for authentication.

Inbound Hash: Packets

The number of inbound authentication-only hashed packets processed by this SEP. Only hashing algorithms are applied to authentication-only traffic; there is no encryption or decryption.

Outbound Hash: Octets

The number of outbound octets (bytes) to which this SEP applied a hashing algorithm for authentication.

Outbound Hash: Packets

The number of outbound authentication-only hashed packets processed by this SEP. Only hashing algorithms are applied to authentication-only traffic; there is no encryption or decryption.

Encrypted: Octets

The number of octets (bytes) that this SEP encrypted.

Encrypted: Packets

The number of encryption-only packets processed by this SEP. Only encryption algorithms are applied to encryption-only traffic; there is no hashing or authentication.

Decrypted: Octets

The number of octets (bytes) that this SEP decrypted.

Decrypted: Packets

The number of decryption-only packets processed by this SEP. Only encryption algorithms are applied to encryption-only traffic; there is no hashing or authentication.

Hash Encrypted: Packets

The number of packets that this SEP processed using both hashing (authentication) and encryption algorithms. This is typical processing for tunneled traffic.

Hash Decrypted: Packets

The number of packets that this SEP processed using both hashing (authentication) and decryption algorithms.

Drops: Packets

The number of packets intended for processing by this SEP, but dropped due to the SEP being overloaded.

Random Requests

The number of requests to this SEP to generate random numbers. When needed (requested), the SEP generates a 2-KB block of random numbers and caches them on the VPN Concentrator. Various cryptographic functions require random numbers of different sizes, and they get them from the cache.

Random Replenishments

The number of times this SEP fulfilled a request to generate a block of random numbers, to replenish the cache.

Random Bytes Available

The number of bytes currently available in the random-number cache on the VPN Concentrator.

Random Cache Empty

The number of times the VPN Concentrator received a request for random numbers and the random-number cache was empty. Since the VPN Concentrator monitors this cache and communicates with the SEP to replenish it, this number should be zero or very small.

DH Keys Generated

The number of times this SEP generated a new Diffie-Hellman key pair. IPSec Security Associations use the Diffie-Hellman algorithm to generate encryption keys, for example.

DH Derived Secret Keys

The number of times this SEP has derived the Diffie-Hellman secret key. In public-key cryptography, the VPN Concentrator receives a remote public key, and the SEP uses the local private key to generate the secret key.

RSA Digital Keys Generated

The number of times this SEP has generated a new RSA encryption-key pair.

RSA Digital Signings

The number of times this SEP has generated an RSA (Rivest, Shamir, Adelman algorithm) digital signature. The VPN Concentrator generates a digital signature when it creates a digital certificate.

RSA Digital Verifications

The number of times this SEP has verified an RSA digital signature. When the VPN Concentrator receives a signed digital certificate for authentication, it must verify the digital signature by computing a hash of the certificate and comparing it with the received-certificate hash.

RSA Encryptions: Octets / Packets

The number of RSA-encrypted octets (bytes) / packets this SEP has generated.

RSA Decryptions: Octets / Packets

The number of RSA-encrypted octets (bytes) / packets this SEP has received and decrypted.

DSA Digital Keys Generated

The number of times this SEP has generated a new DSA (Digital Signature Algorithm) encryption-key pair.

DSA Digital Signings

The number of times this SEP has generated a DSA digital signature. The VPN Concentrator generates a digital signature when it creates a digital certificate.

DSA Digital Verifications

The number of times this SEP has verified a DSA digital signature. When the VPN Concentrator receives a signed digital certificate for authentication, it must verify the digital signature by computing a hash of the certificate and comparing it with the received-certificate hash.

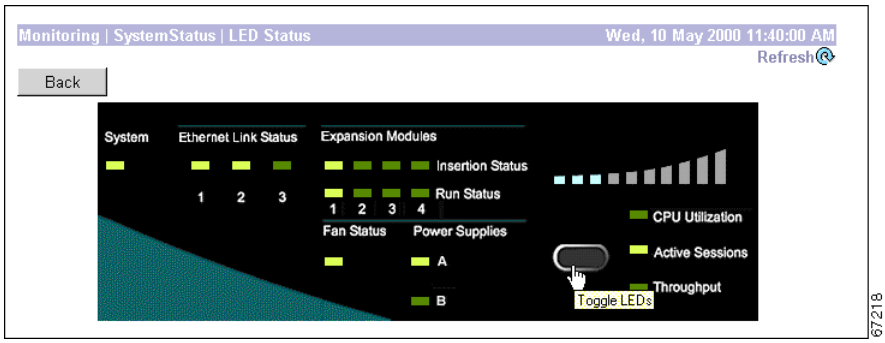
Monitoring | System Status | LED Status

Note This screen appears on models 3015–3080 only.

This screen shows the status of VPN Concentrator front-panel LED indicators, exactly as they appear on the unit itself. LED indicators on the VPN Concentrator are normally green, and the usage graph LEDs are blue. LEDs that are amber, red, or off might indicate an error condition. See Appendix B, "Troubleshooting and System Errors" for descriptions of the LEDs.

The usage graph displays CPU Utilization, Active Sessions, or Throughput, in accordance with the selection you make using the front-panel button. You can "press" the front-panel button either physically—on the unit itself—or logically—on this screen. See Monitoring | System Status for an explanation of usage graph units.

Figure 15-9 Monitoring | System Status | LED Status Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

[LED Selector Button]

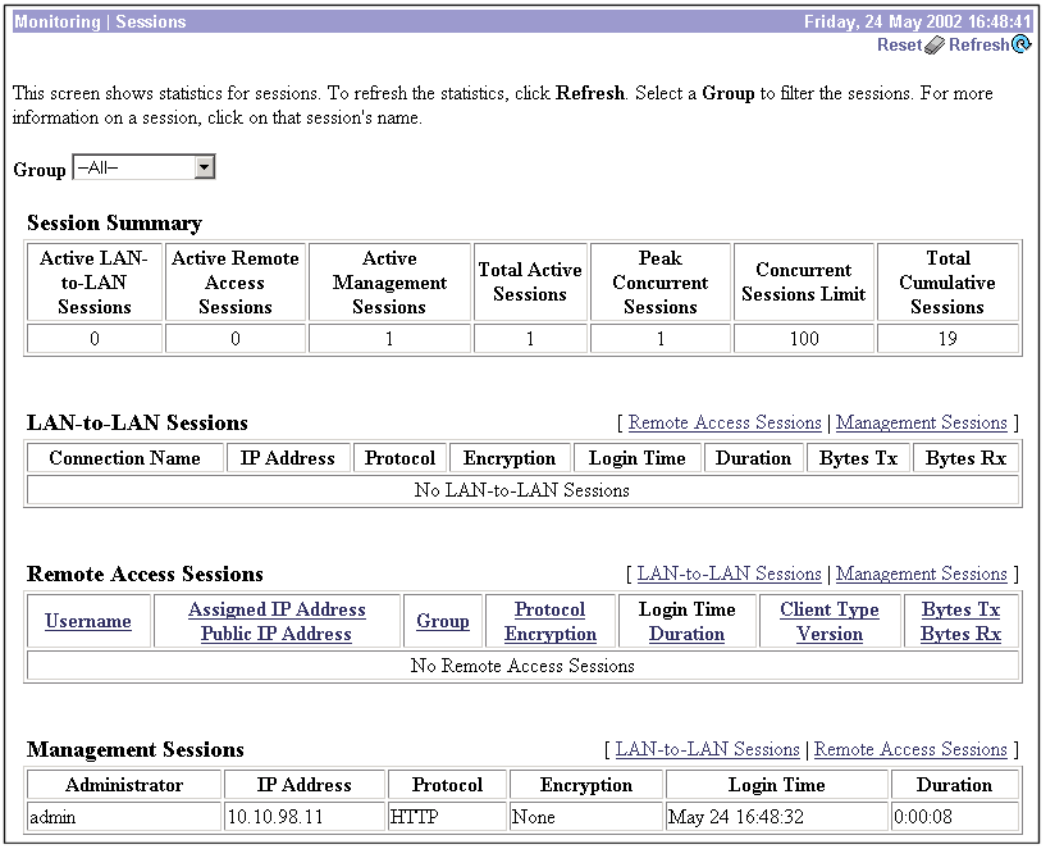
To toggle the usage graph LEDs, click the front-panel button on this screen. Clicking the button here also changes the selection on the VPN Concentrator itself.

Sessions

Monitoring | Sessions

The following screen shows comprehensive data for all active user and administrator sessions on the VPN Concentrator.

Figure 16-1 Monitoring | Sessions Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to monitor sessions for that group only. The default value is --All--, which displays sessions for all groups.

Session Summary Table

This table shows summary totals for LAN-to-LAN, remote access, and management sessions.

A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

Active LAN-to-LAN Sessions

The number of IPSec LAN-to-LAN sessions that are currently active.

Active Remote Access Sessions

The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.

Active Management Sessions

The number of administrator management sessions that are currently active.

Total Active Sessions

The total number of sessions of all types that are currently active.

Peak Concurrent Sessions

The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.

Concurrent Sessions Limit

The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent, for example, model 3060 = 5000 sessions.

Total Cumulative Sessions

The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

LAN-to-LAN Sessions Table

This table shows parameters and statistics for all active IPSec LAN-to-LAN sessions, initially sorted alphanumerically by connection name. Each session here identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

[Remote Access Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Connection Name

The name of the IPSec LAN-to-LAN connection.

To display detailed parameters and statistics for this connection, click this name. See the Monitoring | Sessions | Detail screen.

IP Address

The IP address of the remote peer VPN Concentrator or other secure gateway that initiated this LAN-to-LAN connection.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

Remote Access Sessions Table

This table shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the VPN Concentrator. Remote-access sessions include PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions.

Click a column header in this table to sort the table entries in ascending alphanumeric order, using that column as the sort key field.

[LAN-to-LAN Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Username

The username or login name for the session. The field shows `Authenticating...` if the remote-access client is still negotiating authentication. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

To display detailed parameters and statistics for this session, click this name. See the Monitoring | Sessions | Detail screen.

Public IP Address

The public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.

Assigned IP Address

The private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network.

Group

The group name of the client for this remote-access session. Clicking the column head for Group sorts the table entries in ascending alphanumeric order and also sorts the usernames within each group in ascending alphanumeric order.

Client Type and Operating System

The client type of connected clients, and, when available, the associated operating system, sorted by username. For example:

Client Type	Operating System
VPN 3000 Hardware Client	VPN3002
Windows NT client	Windows NT 4.0, Windows 2000, and Windows XP
Windows 98 client	Windows 98
Windows 95client	Windows 95

Version

The software version number (for example, rel. 3.6,_int 50) for connected clients, sorted by username.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

Management Sessions Table

This table shows parameters and statistics for all active administrator management sessions on the VPN Concentrator.

[LAN-to-LAN Sessions | Remote Access Sessions]

Click these active links to go to the other session tables on this Manager screen.

Administrator

The administrator username or login name for the session.

IP Address

The IP address of the manager workstation that is accessing the system. Local indicates a direct connection through the Console port on the system.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

Table 16-1 Parameter definitions for Monitoring | Sessions Screen

Parameter	Definition
Protocol	The protocol this session is using. `Console` indicates a direct connection through the Console port on the system. See Monitoring | Sessions | Protocols for a graphical representation of sessions by protocol.
Encryption	The data encryption algorithm this session is using, if any. See Monitoring | Sessions | Encryption for a graphical representation of sessions by encryption algorithm used.
Login Time	The date and time (`MMM DD HH:MM:SS`) that the session logged in. Time is displayed in 24-hour notation.
Duration	The elapsed time (`HH:MM:SS`) between the session login time and the last screen refresh.
Bytes Tx	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Bytes Rx	The total number of bytes received from the remote peer or client by the VPN Concentrator.

Monitoring | Sessions | Detail

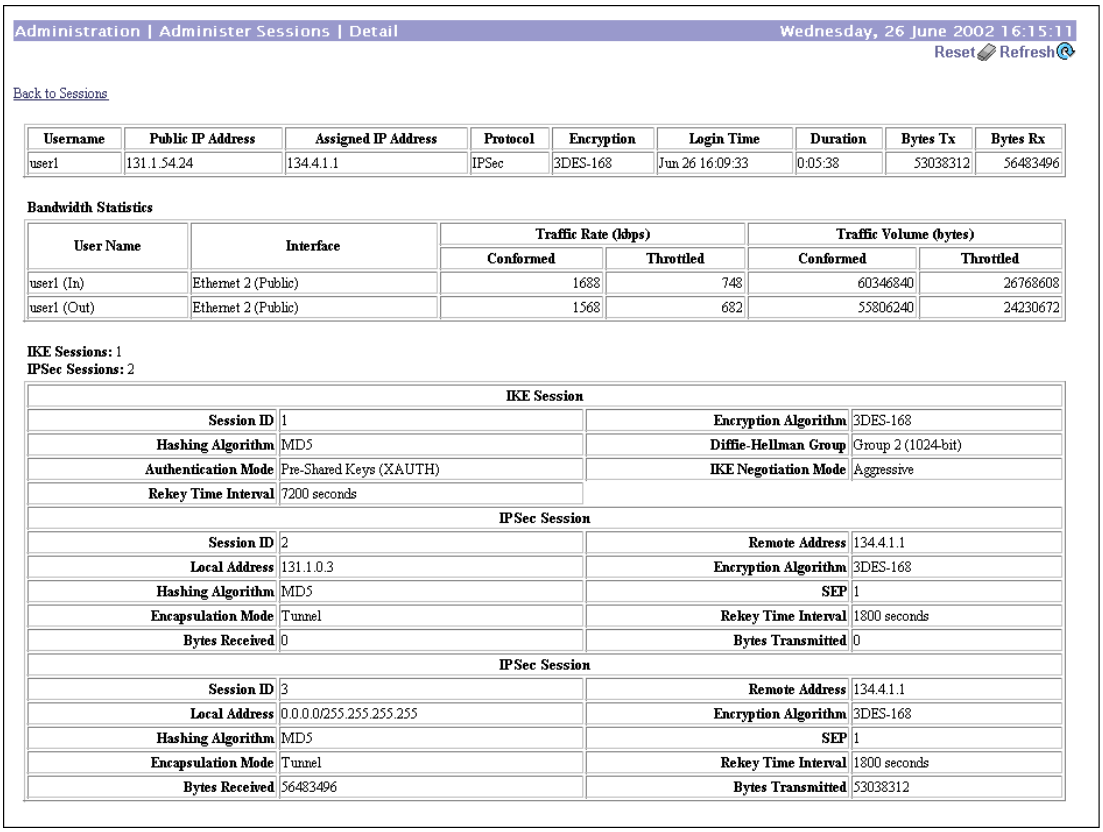
These Manager screens show detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. There are unique screens for:

- IPSec LAN-to-LAN (IPSec/LAN-to-LAN)
- IPSec remote access (IPSec User)
- IPSec through UDP (IPSec/UDP)
- IPSec through TCP (IPSec/TCP)
- L2TP
- L2TP over IPSec (L2TP/IPSec)
- PPTP

The Manager displays the appropriate screen when you click a highlighted connection name or username on the Monitoring | Sessions screen. Figure Figure 16-2 shows an example of one kind of detail screen. Depending on the type of connection you select, your detail screen might look somewhat different from the example shown. But, each session detail screen shows three tables: summary data, bandwidth management information, and detail data. The summary data echoes the session data from the Monitoring | Sessions screen. The Bandwidth Statistics table shows information about the effect of policing on that session. The session detail table shows all the relevant parameters for each session and subsession.

See Table 16-2 for definitions of the possible session detail parameters, in alphabetical order.

Figure 16-2 Example of a Monitoring | Sessions | Detail Screen



Administration | Administer Sessions | Detail — Wednesday, 26 June 2002 16:15:11

Reset Refresh

Back to Sessions

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
user1	131.1.54.24	134.4.1.1	IPSec	3DES-168	Jun 26 16:09:33	0:05:38	53038312	56483496

Bandwidth Statistics

User Name	Interface	Traffic Rate (bps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
user1 (In)	Ethernet 2 (Public)	1688	748	60346840	26768608
user1 (Out)	Ethernet 2 (Public)	1568	682	55806240	24230672

IKE Sessions: 1
IPSec Sessions: 2

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys (XAUTH)	**IKE Negotiation Mode**	Aggressive
Rekey Time Interval	7200 seconds		
IPSec Session			
Session ID	2	**Remote Address**	134.4.1.1
Local Address	131.1.0.3	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	1800 seconds
Bytes Received	0	**Bytes Transmitted**	0
IPSec Session			
Session ID	3	**Remote Address**	134.4.1.1
Local Address	0.0.0.0/255.255.255.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	1800 seconds
Bytes Received	56483496	**Bytes Transmitted**	53038312

78544

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back to Sessions

To return to the Monitoring | Sessions screen, click **Back to Sessions**.

Monitoring | Sessions | Detail Parameters

Table 16-2 Parameter Definitions for Monitoring | Sessions | Detail Screens

Parameter	Definition
Assigned IP Address	The private IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network.
Authentication Mode	The protocol or mode used to authenticate this session.
Bytes Rx Bytes Received	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Bytes Tx Bytes Transmitted	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Compression	The data compression algorithm this session is using. LZS is the data compression algorithm used by IPComp. MPPC uses LZ.
Connection Name	The name of the IPSec LAN-to-LAN connection.
Diffie-Hellman Group	The algorithm and key size used to generate IPSec SA encryption keys.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Dynamic Filter	RADIUS user filter applied to this session.
Dynamic Rules	The rules that make up the dynamic filter. For the syntax of these rules, see Dynamic Filters, page 13-3.
Encapsulation Mode	The mode for applying IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication, in other words, what part of the original IP packet has ESP applied.
Encryption Encryption Algorithm	The data encryption algorithm this session is using, if any.
Hashing Algorithm	The algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Idle Time	The elapsed time (HH:MM:SS) between the last communication activity on this session and the last screen refresh.
IKE Negotiation Mode	The IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	The total number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
IP Address	The IP address of the remote peer VPN Concentrator or other secure gateway that initiated the IPSec LAN-to-LAN connection.
IPSec Sessions	The total number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session may have two IPSec sessions: one showing the tunnel endpoints, and one showing the private networks reachable through the tunnel.
L2TP Sessions	The total number of user sessions through this L2TP or L2TP / IPSec tunnel; usually `1`.

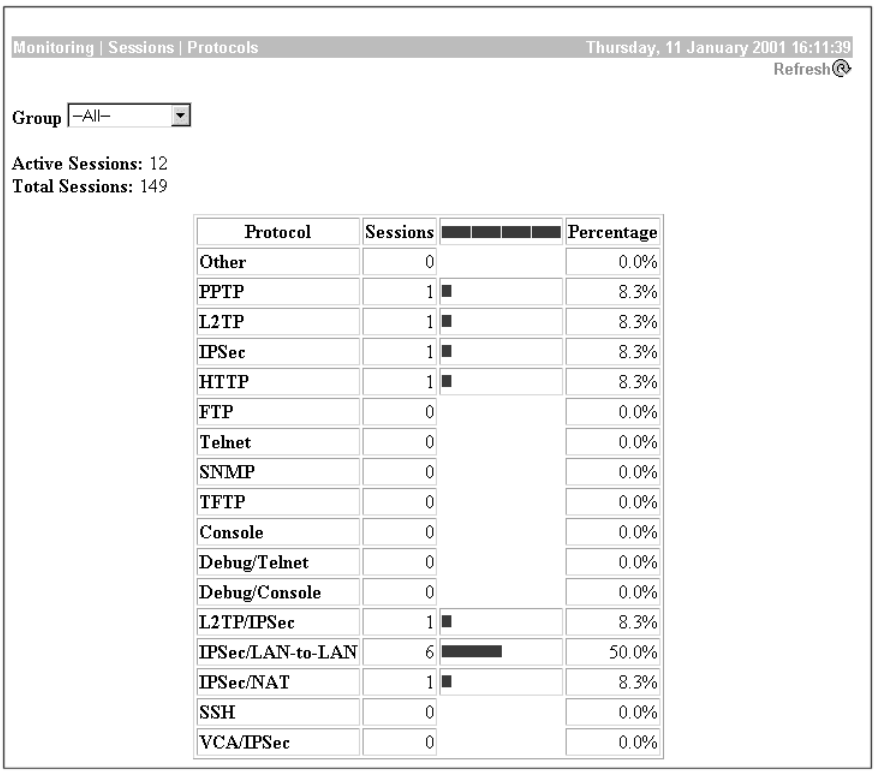
Table 16-2 Parameter Definitions for Monitoring | Sessions | Detail Screens (continued)

Parameter	Definition
Local Address	The IP address (and wildcard mask) of the destination host (or network) for this session.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Perfect Forward Secrecy Group	The Diffie-Hellman algorithm and key size used to generate IPSec SA encryption keys using Perfect Forward Secrecy.
PFS Group	The Perfect Forward Secrecy group: 1, 2, 3, 4, or 7.
PPTP Sessions:	The total number of user sessions through this PPTP tunnel; usually 1.
Protocol	The tunneling protocol that this session is using.
Public IP Address	The public IP address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
Rekey Data Interval	The lifetime in kilobytes of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	The lifetime in seconds of the IPSec (IKE) SA encryption keys.
Remote Address	The IP address (and wildcard mask) of the remote peer (or network) that initiated this session.
SEP	The Scalable Encryption Module that is handling cryptographic processing for this session.
Session ID	An identifier for session components (subsessions) on this screen. With IPSec, there is one identifier for each SA.
UDP Port	The UDP port number used in an IPSec through NAT connection.
Username	The username or login name for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

Monitoring | Sessions | Protocols

This screen graphically displays the protocols used by currently active user and administrator sessions on the VPN Concentrator.

Figure 16-3 Monitoring | Sessions | Protocols Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show protocols used by currently active users in that group only. The default value is --All--, which displays protocols for users in all groups.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Protocol

The protocol that the session is using:

- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- L2TP = Layer 2 Tunneling Protocol.
- IPSec = Internet Protocol Security tunneling protocol (remote-access users).
- HTTP = Hypertext Transfer Protocol (web browser).
- FTP = File Transfer Protocol.
- Telnet = Terminal emulation protocol.
- SNMP = Simple Network Management Protocol.
- TFTP = Trivial File Transfer Protocol.
- Console = Directly connected console; no protocol.
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- Debug/Console = Debugging via console (for Cisco use only).
- L2TP/IPSec = L2TP over IPSec.
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/UDP = IPSec through NAT (Network Address Translation) via UDP.
- SSH = Secure SHell protocol.
- VCA/IPSec = Virtual Cluster Agent via IPSec. (For Cisco use only.)
- IPSec/TCP = IPSec through NAT (Network Address Translation) via TCP.
- IPSec/NAT-T = IPSec over NAT Traversal.
- IPSec/LAN-to-LAN/NAT-T = IPSec LAN-to-LAN connection over NAT Traversal.
- L2TP/IPSec/NAT-T = L2TP/IPSec connection over NAT Traversal.

Sessions

The number of active sessions using this protocol. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph 

The percentage of sessions using this protocol relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

Percentage

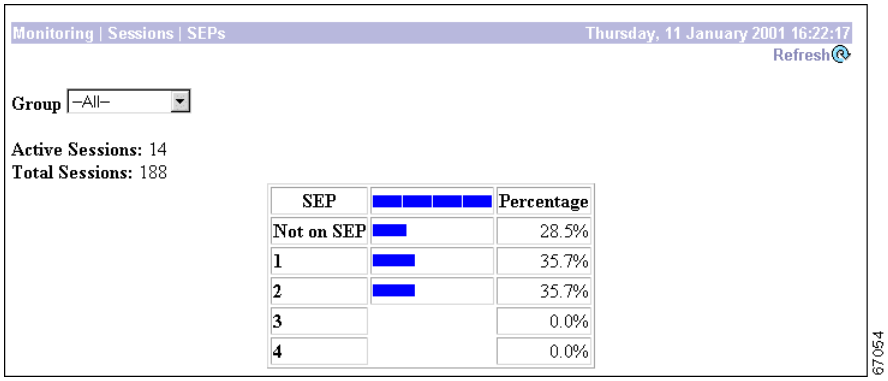
The percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

Monitoring | Sessions | SEPs

Note This screen appears on models 3015–3080 only.

This screen graphically displays the SEP (Scalable Encryption Processing) or SEP-E (Enhanced SEP) modules used by currently active user and administrator sessions on the VPN Concentrator. SEP modules perform data encryption functions in hardware.

Figure 16-4 Monitoring | Sessions | SEPs Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to display SEP modules for that group only. The default value is --All--, which displays SEP modules for all groups.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

SEP

The SEP module that the sessions are using.

- Not on SEP = using software encryption, or not using encryption.
- 1, 2, 3, 4 = SEP module 1, 2, 3, and 4, respectively.

Sessions

The number of active sessions using this SEP module. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph 

The percentage of sessions using this SEP module relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

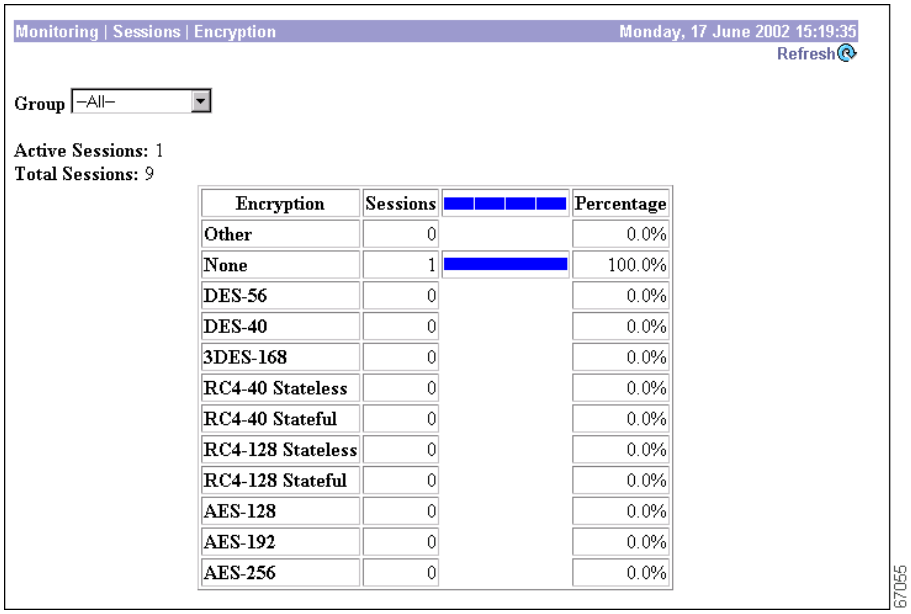
Percentage

The percentage of sessions using this SEP module relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

Monitoring | Sessions | Encryption

This screen graphically displays the data encryption algorithms used by currently active user and administrator sessions on the VPN Concentrator.

Figure 16-5 Monitoring | Sessions | Encryption Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to monitor data encryption algorithms used by currently active users in that group only. The default value is --All--, which displays data encryption algorithms for all groups.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Encryption

The data encryption algorithm that the sessions are using:

- Other = other than listed below.
- None = no data encryption.
- DES-56 = Data Encryption Standard algorithm with a 56-bit key.
- DES-40 = DES encryption with a 56-bit key, 40 bits of which are private.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Sessions

The number of active sessions using this encryption algorithm. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph 

The percentage of sessions using this encryption algorithm relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

Percentage

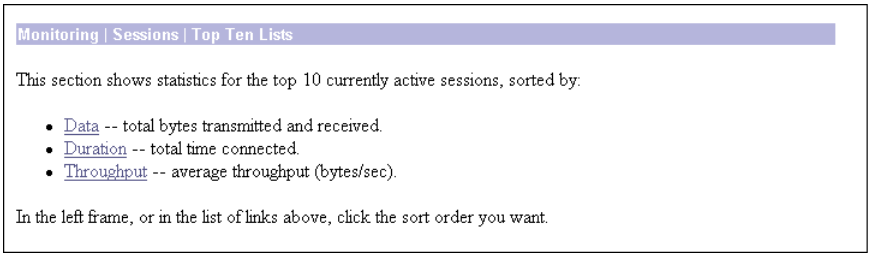
The percentage of sessions using this encryption algorithm relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

Monitoring | Sessions | Top Ten Lists

This section of the Manager shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by:

- Data: total bytes transmitted and received.
- Duration: total time connected.
- Throughput: average throughput (bytes/sec).

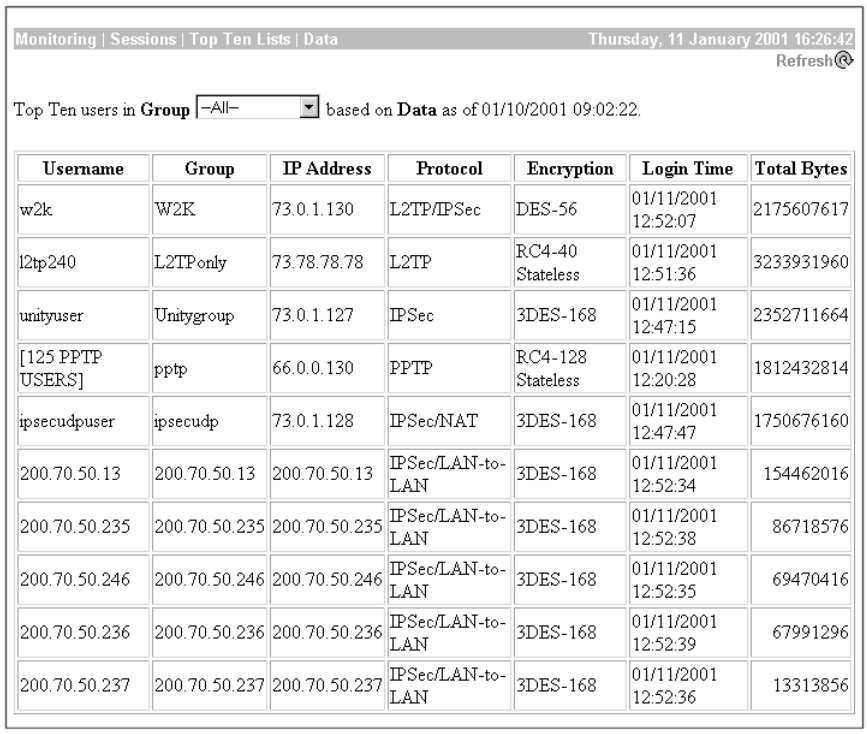
Figure 16-6 Monitoring | Sessions | Top Ten Lists Screen



Monitoring | Sessions | Top Ten Lists | Data

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by data, total bytes transmitted and received.

Figure 16-7 Monitoring | Sessions | Top Ten Lists | Data Screen



Monitoring | Sessions | Top Ten Lists | Data — Thursday, 11 January 2001 16:26:42

Refresh

Top Ten users in **Group** –All– based on **Data** as of 01/10/2001 09:02:22.

Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/11/2001 12:52:07	2175607617
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/11/2001 12:51:36	3233931960
unityuser	Unitygroup	73.0.1.127	IPSec	3DES-168	01/11/2001 12:47:15	2352711664
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/11/2001 12:20:28	1812432814
ipsecudpuser	ipsecudp	73.0.1.128	IPSec/NAT	3DES-168	01/11/2001 12:47:47	1750676160
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:34	154462016
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:38	86718576
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:35	69470416
200.70.50.236	200.70.50.236	200.70.50.236	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:39	67991296
200.70.50.237	200.70.50.237	200.70.50.237	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:36	13313856

67365

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using:

- None = No data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Total Bytes

The total number of bytes transmitted and received by this session. N/A = the session is not passing data, in other words, it is an administrator session.

Monitoring | Sessions | Top Ten Lists | Duration

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by duration: total time connected.

Figure 16-8 Monitoring | Sessions | Top Ten Lists | Duration Screen

Username	Group	IP Address	Protocol	Encryption	Login Time	Duration
200.70.50.230	200.70.50.230	200.70.50.230	IPSec/LAN-to-LAN	3DES-168	01/11/2001 08:48:22	7:46:31
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/11/2001 12:20:28	4:14:25
unityuser	Unitygroup	73.0.1.127	IPSec	3DES-168	01/11/2001 12:47:15	3:47:38
ipsecudpuser	ipsecudp	73.0.1.128	IPSec/NAT	3DES-168	01/11/2001 12:47:47	3:47:06
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/11/2001 12:51:36	3:43:17
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/11/2001 12:52:06	3:42:47
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:34	3:42:19
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:35	3:42:18
200.70.50.237	200.70.50.237	200.70.50.237	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:36	3:42:17
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:37	3:42:16

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using.

- None = no data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

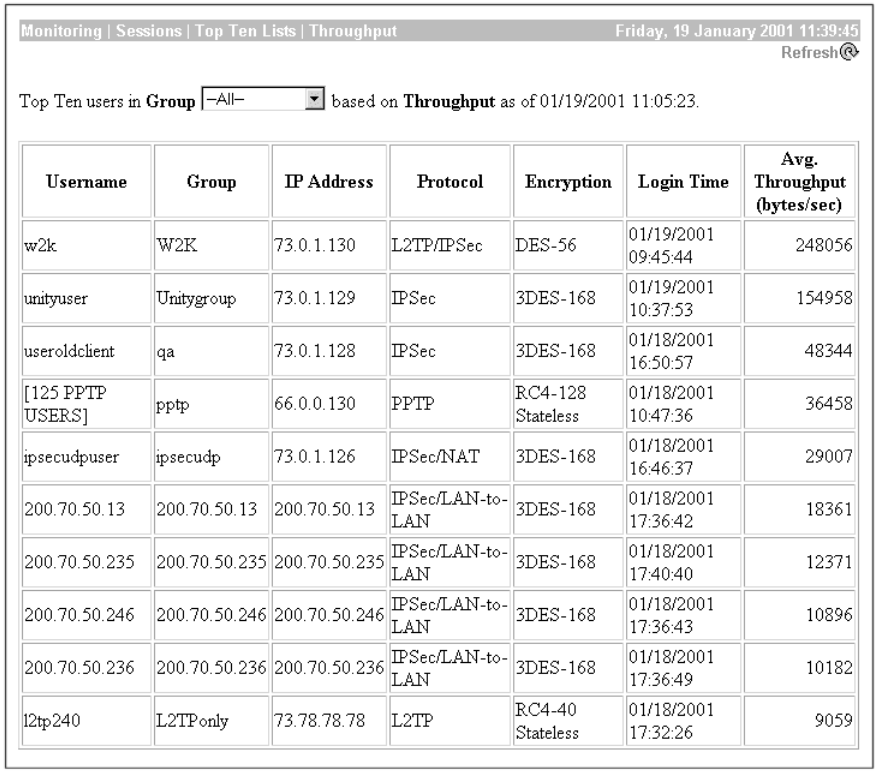
Duration

The total amount of time that this session has been connected: HH:MM:SS.

Monitoring | Sessions | Top Ten Lists | Throughput

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by average throughput (bytes/sec).

Figure 16-9 Monitoring | Sessions | Top Ten Lists | Throughput Screen



Monitoring | Sessions | Top Ten Lists | Throughput — Friday, 19 January 2001 11:39:45

Refresh

Top Ten users in **Group** [–All–] based on **Throughput** as of 01/19/2001 11:05:23.

Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/19/2001 09:45:44	248056
unityuser	Unitygroup	73.0.1.129	IPSec	3DES-168	01/19/2001 10:37:53	154958
useroldclient	qa	73.0.1.128	IPSec	3DES-168	01/18/2001 16:50:57	48344
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/18/2001 10:47:36	36458
ipsecudpuser	ipsecudp	73.0.1.126	IPSec/NAT	3DES-168	01/18/2001 16:46:37	29007
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:42	18361
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:40:40	12371
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:43	10896
200.70.50.236	200.70.50.236	200.70.50.236	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:49	10182
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/18/2001 17:32:26	9059

67363

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using.

- None = No data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Avg. Throughput (bytes/sec)

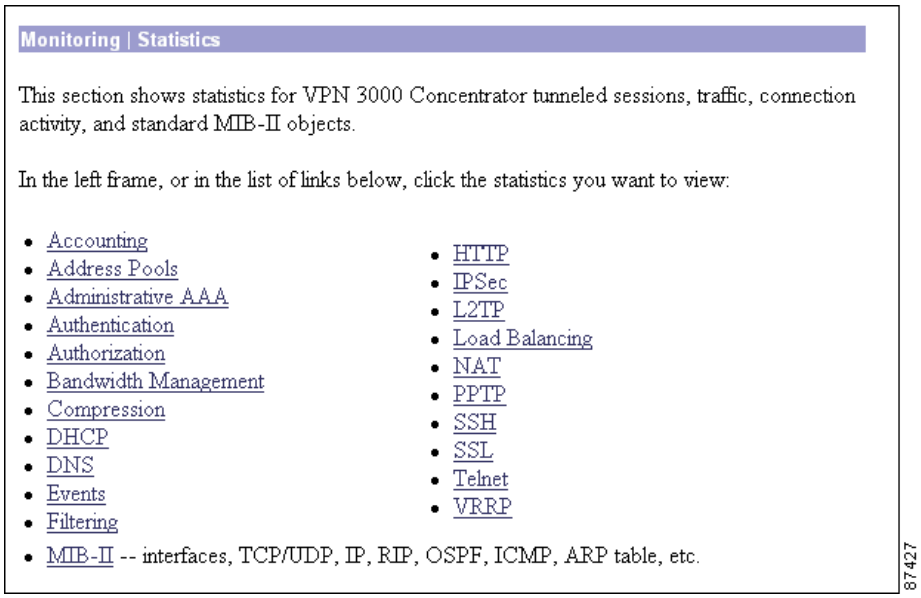
The average throughput of the session, which is [total bytes transmitted and received] divided by total connect time. N/A = the session is not passing data, in other words, it is an administrator session.

Statistics

Monitoring | Statistics

This section of the Manager shows statistics for traffic and activity on the VPN Concentrator 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, and the ARP table.

Figure 17-1 Monitoring | Statistics Screen



Statistics include:

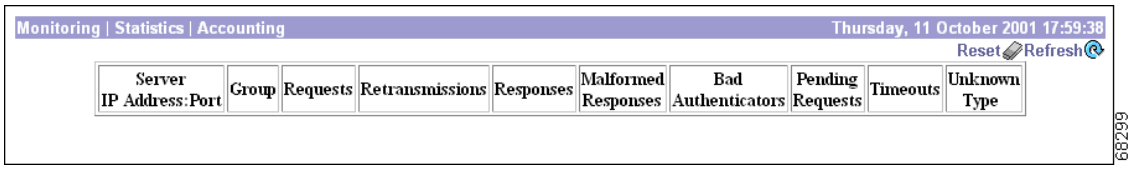
- Accounting: total requests, responses, timeouts, etc.
- Address Pools: configured pools, allocated and available addresses.
- Administrative AAA: requests, accepts, rejects, challenges, timeouts, etc.
- Authentication: total requests, accepts, rejects, challenges, timeouts, etc.
- Authorization: total requests, accepts, rejects, challenges, timeouts, etc.
- Bandwidth Management: volume and rate of traffic managed by bandwidth policies.
- Compression: pre and post-compression byte totals for IPComp and MPPC.
- DHCP: leased addresses, duration, server addresses, etc.
- DNS: total requests, responses, timeouts, etc.
- Events: total events sorted by class, number, and count.
- Filtering: total inbound and outbound filtered traffic by interface.
- HTTP: total data traffic and connection statistics.
- IPSec: total Phase 1 and Phase 2 tunnels, received and transmitted packets, failures, drops, etc.
- L2TP: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- Load Balancing: device role; device load; and cluster peers' sessions, IP addresses, priority, etc.
- NAT: Network Address Translation session data.
- PPTP: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- SSH: total and active sessions, bytes and packets sent and received, etc.
- SSL: total sessions, encrypted vs. unencrypted traffic, etc.
- Telnet: total sessions, and current session inbound and outbound traffic.
- VRRP: total advertisements, Master router roles, errors, etc.
- MIB-II Stats: interfaces, TCP/UDP, IP, RIP, OSPF, ICMP, ARP table, Ethernet, and SNMP.

Monitoring | Statistics | Accounting

This screen shows statistics for RADIUS user accounting activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with RADIUS accounting servers, see the Configuration | System | Servers | Accounting screens.

Figure 17-2 Monitoring | Statistics | Accounting Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address: Port

The IP address of the configured RADIUS user accounting server, and the port number that the VPN Concentrator is using to access the server. Each configured accounting server is a row in this table. The well-known port number for RADIUS accounting is 1646.

Group

The group on which the server is configured.

Requests

The number of accounting request packets sent to this RADIUS accounting server. This number does not include retransmissions.

Retransmissions

The number of accounting request packets retransmitted to this RADIUS accounting server.

Responses

The number of accounting response packets received from this RADIUS accounting server.

Malformed Responses

The number of malformed accounting response packets received from this RADIUS accounting server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of accounting response packets received from this server that contained invalid authenticators.

Pending Requests

The number of accounting request packets sent to this RADIUS accounting server that have not yet timed out or received a response.

Timeouts

The number of accounting timeouts to this RADIUS server. After a timeout the system may retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type

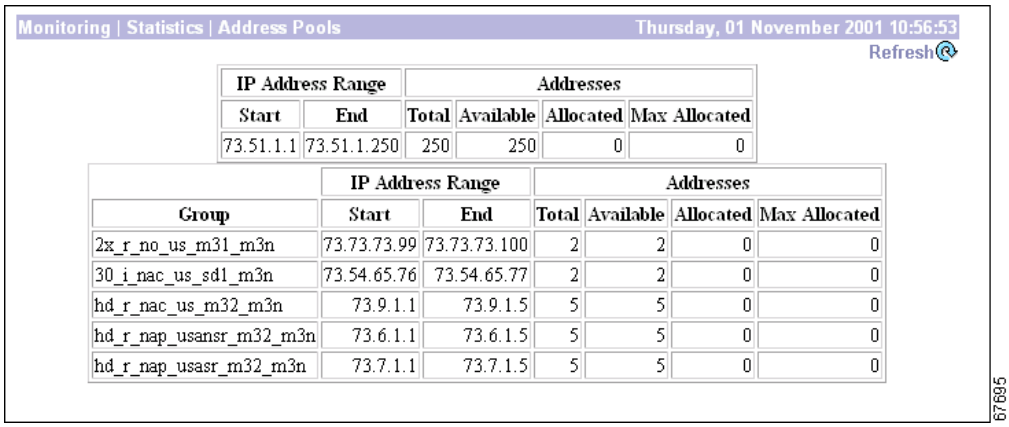
The number of RADIUS packets of unknown type received from this server on the accounting port.

Monitoring | Statistics | Address Pools

This screen shows statistics for address pool activity on the VPN Concentrator since it was last booted or reset. This data appears if the VPN Concentrator is configured to assign IP addresses to clients from an internal address pool.

To configure address pools, see the Configuration | System | Address Management screens.

Figure 17-3 Monitoring | Statistics | Address Pools Screen



IP Address Range		Addresses			
Start	End	Total	Available	Allocated	Max Allocated
73.51.1.1	73.51.1.250	250	250	0	0

	IP Address Range		Addresses			
Group	Start	End	Total	Available	Allocated	Max Allocated
2x_r_no_us_m31_m3n	73.73.73.99	73.73.73.100	2	2	0	0
30_i_nac_us_sd1_m3n	73.54.65.76	73.54.65.77	2	2	0	0
hd_r_nac_us_m32_m3n	73.9.1.1	73.9.1.5	5	5	0	0
hd_r_nap_usansr_m32_m3n	73.6.1.1	73.6.1.5	5	5	0	0
hd_r_nap_usasr_m32_m3n	73.7.1.1	73.7.1.5	5	5	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IP Address Range: Start / End

The starting and ending IP addresses in the configured address pool. Each configured range is a row in the table.

Total Addresses

The total number of IP addresses in this configured pool.

Available Addresses

The number of IP addresses available (unassigned) in this pool.

Allocated Addresses

The number of IP addresses currently assigned from this pool.

Max Allocated Addresses

The maximum number of IP addresses assigned from this pool at any one time.

Group

The names of configured groups.

IP Address Range: Start / End

The starting and ending IP addresses in the group's address pool. Each configured range is a row in the table.

Total Addresses

The total number of IP addresses in the address pool of this group.

Available Addresses

The number of IP addresses available (unassigned) in this group's pool.

Allocated Addresses

The number of IP addresses currently assigned from this group's pool.

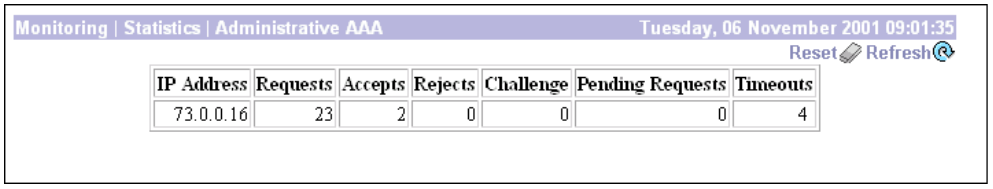
Max Allocated Addresses

The maximum number of IP addresses assigned from this group's pool at any one time.

Monitoring | Statistics | Administrative AAA

If you have configured a TACACS+ server, this screen shows statistics for communications between the VPN Concentrator and the TACACS+ server since the VPN Concentrator was last booted or reset.

Figure 17-4 Monitoring | Statistics | Administrative AAA Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IP Address

The IP address of the TACACS+ server.

Requests

The number of requests for authentication, information, or authorization from the VPN Concentrator to the TACACS+ server.

Accepts

The number of successful authentications.

Rejects

The number of rejected authentications.

Challenge

This field is not used.

Pending Requests

The number of requests that have not yet been answered.

Timeouts

The number of times the VPN Concentrator timed out waiting for a request.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

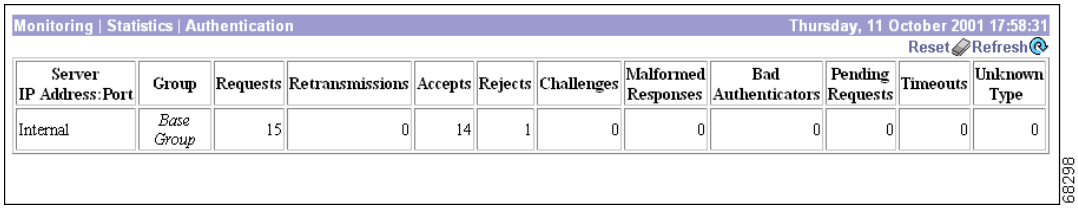
Monitoring | Statistics | Authentication

This screen shows statistics for user authentication activity on the VPN Concentrator since it was last booted or reset.

Note Not all fields apply to all types of authentication servers.

To configure the VPN Concentrator to communicate with authentication servers, see the Configuration | System | Servers | Authentication screens.

Figure 17-5 Monitoring | Statistics | Authentication Screen



Server IP Address:Port	Group	Requests	Retransmissions	Accepts	Rejects	Challenges	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type
Internal	*Base Group*	15	0	14	1	0	0	0	0	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address:Port

The IP address of the configured authentication server, and the port number that the VPN Concentrator is using to access the server. Each configured authentication server is a row in this table. Internal identifies the internal VPN Concentrator authentication server.

When the authentication server is an SDI 5.0 server, this field becomes a link. Click the link to view the Monitoring | Statistics | Authentication | Replicas screen, which displays a list of replicas, and data about them (see the next section).

The default, or well-known, port numbers identify an authentication server type:

- 139 = NT Domain
- 389 = LDAP
- 1645 = RADIUS
- 5500 = SDI

Group

The group on which the server is configured.

Requests

The total number of authentication request packets sent to this server. This number does not include retransmissions.

Retransmissions

The number of authentication request packets retransmitted to this server.

Accepts

The number of authentication acceptance packets received from this server.

Rejects

The number of authentication rejection packets received from this server.

Challenges

The number of authentication challenge packets received from this server.

Malformed Responses

The number of malformed authentication response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of bad authentication response packets received from this server. Bad authenticators contain invalid authenticators or signature attributes.

Pending Requests

The number of authentication request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authentication timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

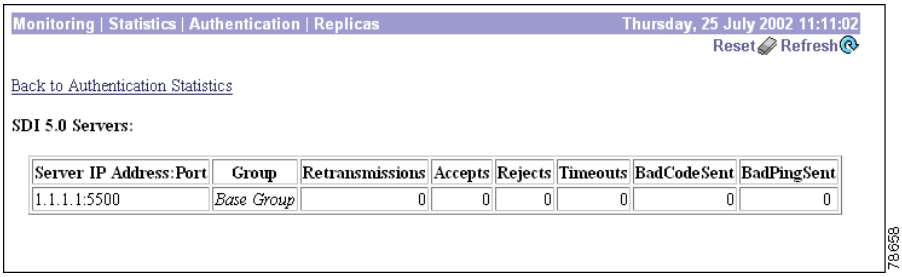
Unknown Type

The number of authentication packets of unknown type received from this server.

Monitoring | Statistics | Authentication | Replicas

This screen shows statistics for SDI 5.0 user authentication activity on the VPN Concentrator since it was last booted or reset.

Figure 17-6 Monitoring | Statistics | Authentication | Replicas Screen



Server IP Address:Port

The IP address of the configured SDI authentication server, and the port number that the VPN Concentrator is using to access the server.

The default, or well-known, port numbers for an SDI 5.0 authentication server is 5500.

Group

The group on which the server is configured.

Retransmissions

The number of authentication request packets retransmitted to this server.

Accepts

The number of authentication acceptance packets received from this server.

Rejects

The number of authentication rejection packets received from this server.

Timeouts

The number of authentication timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

BadCodeSent

The number of bad code packets received from this server. Bad code packets indicate invalid SecurID token code.

BadPinSent

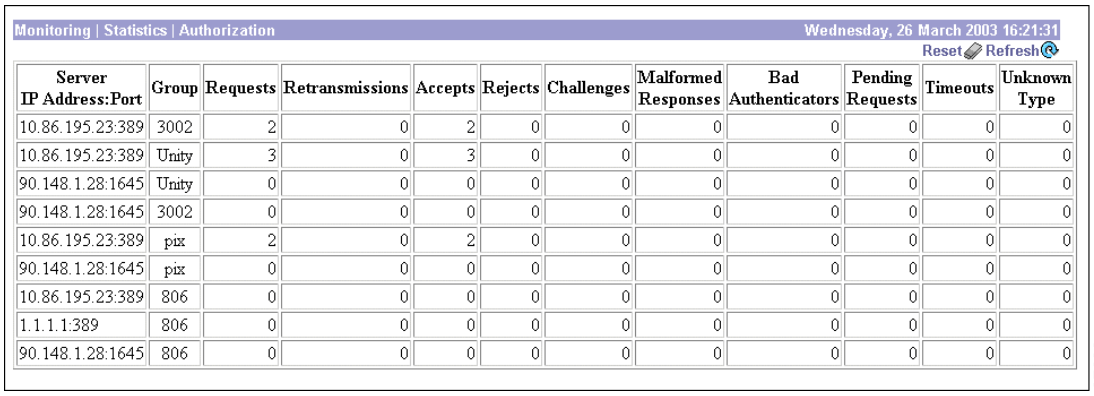
The number of bad pin packets received from this server. Bad pin packets indicate invalid user identification.

Monitoring | Statistics | Authorization

This screen shows statistics for user authorization activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with authorization servers, see the Configuration | System | Servers | Authorization screens.

Figure 17-7 Monitoring | Statistics | Authorization Screen



Server IP Address:Port	Group	Requests	Retransmissions	Accepts	Rejects	Challenges	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type
10.86.195.23:389	3002	2	0	2	0	0	0	0	0	0	0
10.86.195.23:389	Unity	3	0	3	0	0	0	0	0	0	0
90.148.1.28:1645	Unity	0	0	0	0	0	0	0	0	0	0
90.148.1.28:1645	3002	0	0	0	0	0	0	0	0	0	0
10.86.195.23:389	pix	2	0	2	0	0	0	0	0	0	0
90.148.1.28:1645	pix	0	0	0	0	0	0	0	0	0	0
10.86.195.23:389	806	0	0	0	0	0	0	0	0	0	0
1.1.1.1:389	806	0	0	0	0	0	0	0	0	0	0
90.148.1.28:1645	806	0	0	0	0	0	0	0	0	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address:Port

The IP address of the configured authorization server, and the port number that the VPN Concentrator is using to access the server. Each configured authorization server is a row in this table. Internal identifies the internal VPN Concentrator authorization server.

The default, or well-known, port numbers identify an authorization server type:

- 389 = LDAP
- 1645 = RADIUS

Group

The group on which the server is configured.

Requests

The total number of authorization request packets sent to this server. This number does not include retransmissions.

Retransmissions

The number of authorization request packets retransmitted to this server.

Accepts

The number of authorization acceptance packets received from this server.

Rejects

The number of authorization rejection packets received from this server.

Challenges

The number of authorization challenge packets received from this server.

Malformed Responses

The number of malformed authorization response packets received from this server. Malformed packets include packets with an invalid length. Bad authorizations are not included in this number.

Bad Authenticators

The number of bad authorization response packets received from this server. Bad authenticators contain invalid authenticators or signature attributes.

Pending Requests

The number of authorization request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authorization timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

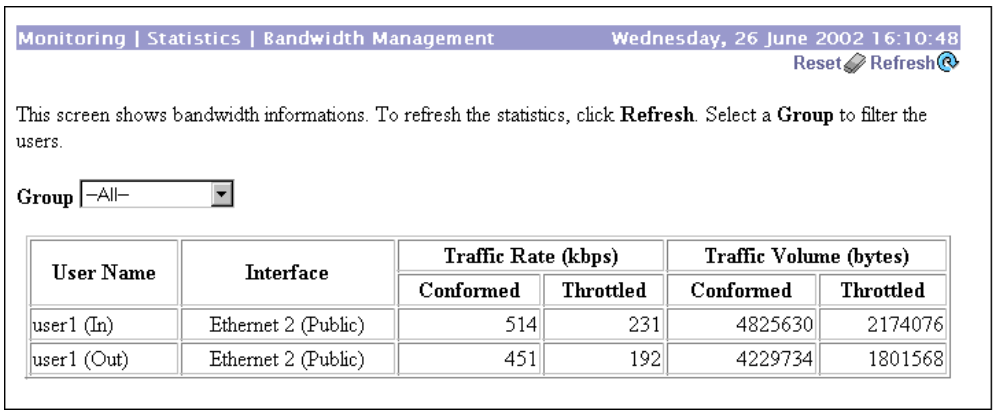
Unknown Type

The number of authorization packets of unknown type received from this server.

Monitoring | Statistics | Bandwidth Management

This screen shows details of the effects of bandwidth management policies on each tunnel. Only tunnels on which bandwidth management policies are enabled appear on this screen.

Figure 17-8 Monitoring | Statistics | Bandwidth Management Screen



Group

Choose a group from the **Group** menu to show bandwidth statistics for users in that group only. The default value is --All--, which displays bandwidth statistics for users in all groups.

User Name

The user name identifying a tunnel using a bandwidth management policy.

Traffic Rate (kbps)

Conformed

The current rate of session traffic (as set by the bandwidth management policy).

Throttled

The rate at which packets are being throttled to maintain the conformed rate.

Traffic Volume (bytes)

Conformed

The number of bytes of session traffic (as set by the bandwidth management policy).

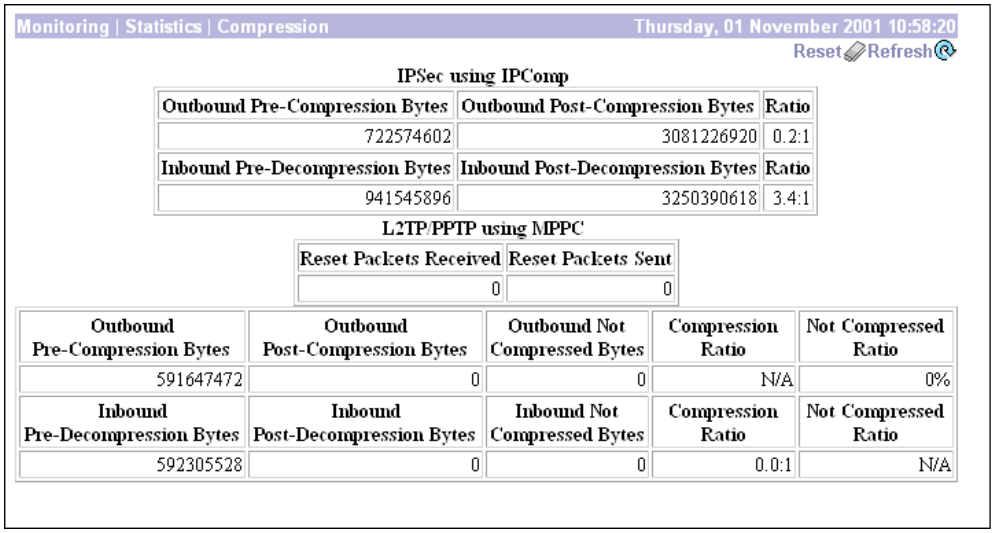
Throttled

The number of bytes being throttled to maintain the conformed rate.

Monitoring | Statistics | Compression

If you have enabled data compression, this screen shows statistics for data compression on the VPN Concentrator since it was last booted or reset.

Figure 17-9 Monitoring | Statistics | Compression Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IPSec Using IPComp

This screen shows statistics for IPSec data compression using the IPComp compression protocol.

Note The following IPComp statistics measure the results of compression on *all* incoming and outgoing data, including data not intended for compression and data that is not compressible.

Outbound Pre-Compression

The total number of bytes of all outbound data before compression.

Outbound Post-Compression

The total number of bytes of all outbound data after compression.

Ratio

The ratio of Outbound Pre-Compression to Outbound Post-Compression.

Inbound Pre-Decompression

The total number of bytes of all incoming data before any of it is decompressed.

Inbound Post-Decompression

The total number of bytes of all incoming data after decompression.

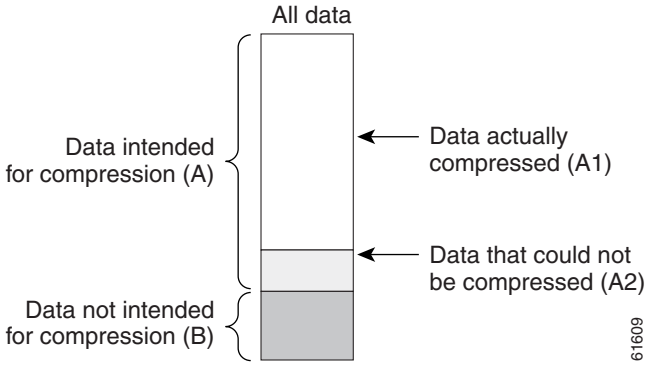
Ratio

The ratio of Inbound Post-Decompression to Inbound Pre-Decompression.

L2TP/PPTP Using MPPC

This table shows statistics for L2TP and PPTP data compression using the MPPC compression protocol. These MPPC statistics use the following distinctions. (See Figure 17-10.) All data transmitted can be divided into two groups: data intended for compression (A) and data that is not intended for compression (B). Of the data intended for compression, some of it actually compresses (A1) and some does not (A2). (The compression process would actually cause certain data to expand, so this data is left uncompressed.)

Figure 17-10 Distinctions Used for Data Compression Statistics



Resets Received

The total number of reset requests received from the remote peer.

Resets Sent

The total number of reset requests sent to the remote peer.

Outbound Pre-Compression

The total number of bytes of outbound data intended for compression. (“A” in Figure 17-10.)

Outbound Post-Compression

The total number of bytes of outbound data actually compressed. (“A1” in Figure 17-10.)

Outbound Not Compressed

The total number of bytes of data intended for compression that were not compressed. The compression process would actually cause certain data to expand, so this data is left uncompressed. (“A2” in Figure 17-10.)

Compression Ratio

The ratio of Outbound Pre-Compression to (Outbound Post-Compression + Outbound Not Compressed).

Not Compressed Ratio

The ratio of Outbound Pre-Compressed to Outbound Not Compressed.

Inbound Pre-Decompression

The total number of bytes of incoming data intended for decompression. (“A” in Figure 17-10.)

Inbound Post-Decompression

The total number of bytes of incoming data actually decompressed. (“A1” in Figure 17-10.)

Inbound Not Compressed

The total number of uncompressed inbound data bytes of the data. (“A2” in Figure 17-10.)

Compression Ratio

The ratio of (Inbound Post-Decompression + Inbound Not Compressed) to Inbound Pre-Decompression.

Not Compressed Ratio

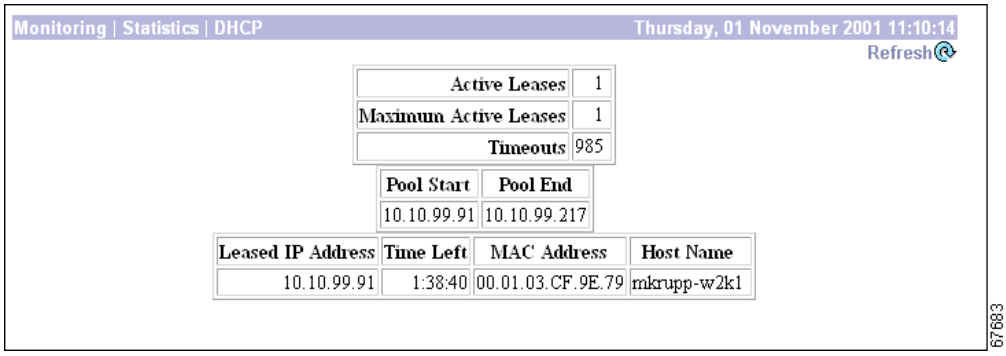
The ratio of Inbound Pre-Decompression to Inbound Not Compressed.

Monitoring | Statistics | DHCP

This screen shows statistics for DHCP (Dynamic Host Configuration Protocol) activity on the VPN Concentrator since it was last booted or reset. Each row of the table shows data for each session using an IP address via DHCP.

To identify DHCP servers to the VPN Concentrator, see Configuration | System | Servers | DHCP. To configure system-wide DHCP functions within the VPN Concentrator, see Configuration | System | IP Routing | DHCP. To use DHCP to assign addresses to clients, see the Configuration | System | Address Management | Assignment screen.

Figure 17-11 Monitoring | Statistics | DHCP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 duration of the current IP address lease, shown as HH:MM:SS.

Time Used

The total length of time that this session has had an active 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

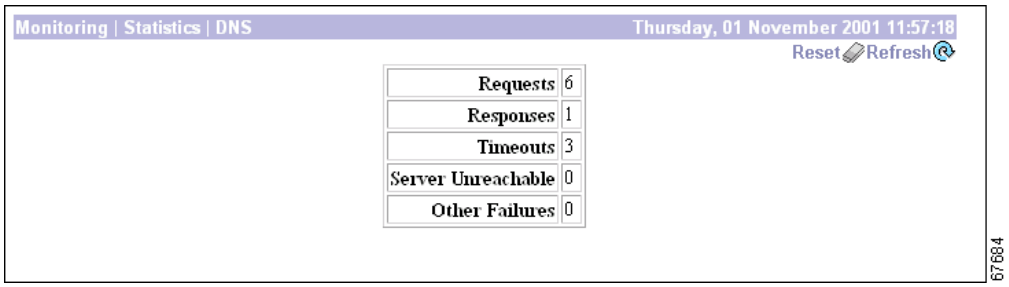
The IP address of the DHCP server that leased this IP address.

Monitoring | Statistics | DNS

This screen shows statistics for DNS (Domain Name System) activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with DNS servers, see the Configuration | System | Servers | DNS screen.

Figure 17-12 Monitoring | Statistics | DNS Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator 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 Concentrator's routing table.

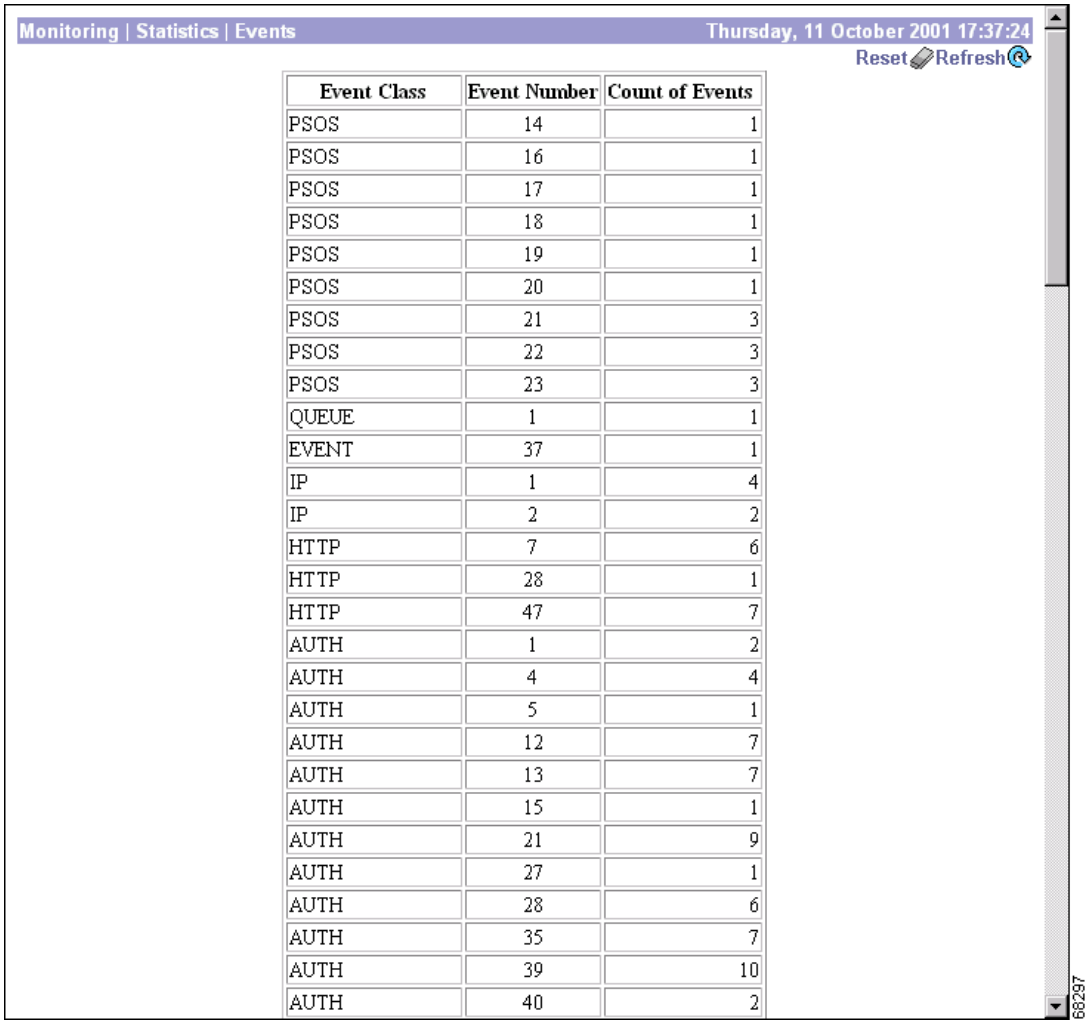
Other Failures

The number of DNS queries that failed for an unspecified reason.

Monitoring | Statistics | Events

This screen shows statistics for all events on the VPN Concentrator since it was last booted or reset. To configure event handling, see the Configuration | System | Events screens.

Figure 17-13 Monitoring | Statistics | Events Screen



Event Class	Event Number	Count of Events
PSOS	14	1
PSOS	16	1
PSOS	17	1
PSOS	18	1
PSOS	19	1
PSOS	20	1
PSOS	21	3
PSOS	22	3
PSOS	23	3
QUEUE	1	1
EVENT	37	1
IP	1	4
IP	2	2
HTTP	7	6
HTTP	28	1
HTTP	47	7
AUTH	1	2
AUTH	4	4
AUTH	5	1
AUTH	12	7
AUTH	13	7
AUTH	15	1
AUTH	21	9
AUTH	27	1
AUTH	28	6
AUTH	35	7
AUTH	39	10
AUTH	40	2

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Event Class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. For a description of event classes, see *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

Event Number

Event number is an Cisco-assigned reference number that denotes a specific event within the event class. For example, CONFIG event number 2 is "Reading configuration file." This reference number assists Cisco support personnel if they need to examine event statistics.

Count of Events

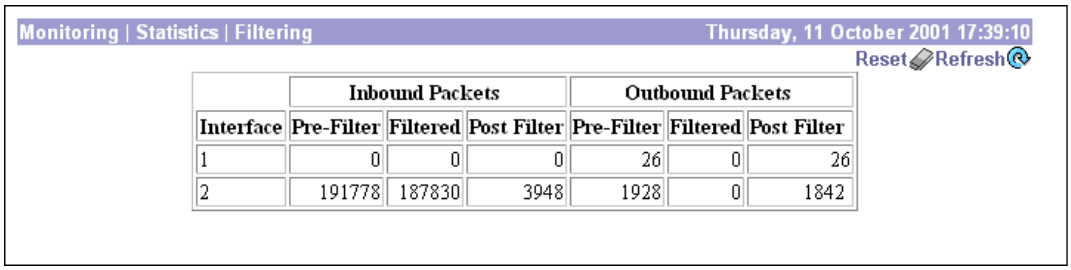
The number of times that specific event has occurred on the VPN Concentrator since it was last booted or reset.

Monitoring | Statistics | Filtering

This screen shows statistics for filtering of traffic that has passed through the interfaces on the VPN Concentrator since it was last booted or reset.

To configure filters, see the Configuration | Policy Management | Traffic Management screens. To apply filters to interfaces, see the Configuration | Interfaces screens. To apply filters to users and groups, see the Configuration | User Management screens.

Figure 17-14 Monitoring | Statistics | Filtering Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator network interface through which the filtered traffic has passed.

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.

Inbound Packets Pre-Filter

The total number of inbound packets received on this interface.

Inbound Packets Filtered

The number of inbound packets that have been filtered and dropped on this interface.

Inbound Packets Post Filter

The number of inbound packets that have been filtered and forwarded on this interface. This number equals Inbound Packets Pre-Filter minus Inbound Packets Filtered.

Outbound Packets Pre-Filter

The total number of outbound packets received on this interface.

Outbound Packets Filtered

The number of outbound packets that have been filtered and dropped on this interface.

Outbound Packets Post Filter

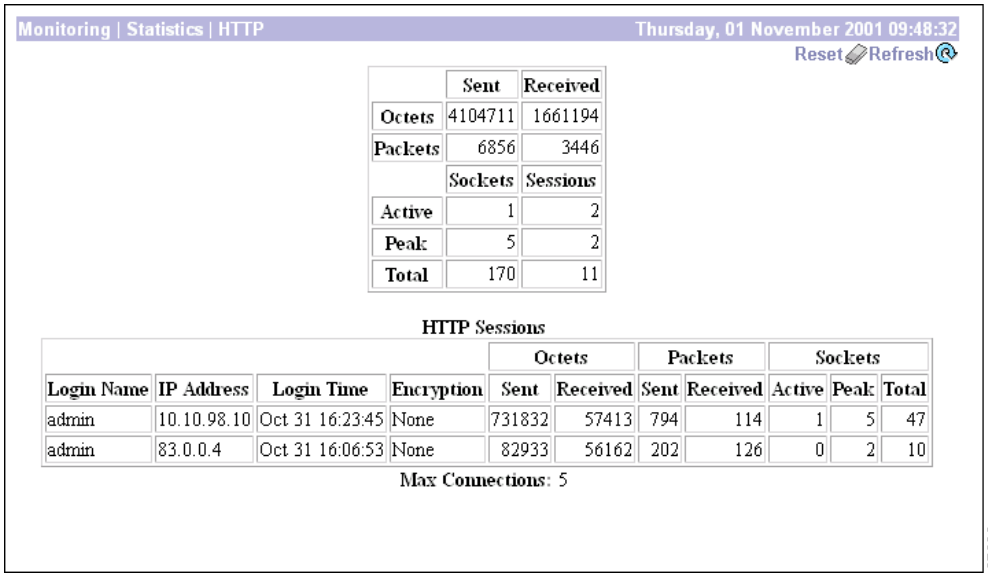
The number of outbound packets that have been filtered and forwarded on this interface. This number equals Outbound Packets Pre-Filter minus Outbound Packets Filtered.

Monitoring | Statistics | HTTP

This screen shows statistics for HTTP activity on the VPN Concentrator since it was last booted or reset.

To configure system-wide HTTP server parameters, see the Configuration | System | Management Protocols | HTTP screen.

Figure 17-15 Monitoring | Statistics | HTTP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset 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 HTTP octets (bytes) sent or received since the VPN Concentrator was last booted or reset.

Packets Sent/Received

The total number of HTTP packets sent or received since the VPN Concentrator was last booted or reset.

Packets Sent Sockets/Sessions

The number of HTTP sessions on the VPN Concentrator.

Active

The number of currently active HTTP connections on the VPN Concentrator.

Peak

The maximum number of HTTP connections that were simultaneously active on the VPN Concentrator since it was last booted or reset.

Total

The total number of HTTP connections on the VPN Concentrator since it was last booted or reset.

HTTP Sessions

This section provides information about HTTP sessions on the VPN Concentrator since it was last booted or reset.

Login Name

The name of the administrative user for the HTTP session.

IP Address

The IP address of the HTTP session.

Login Time

The time when the HTTP session began.

Encryption

The encryption method used in the HTTP session.

Octets Sent/Received

Number of octets sent or received during the HTTP session.

Packets Sent/Received

Number of packets sent or received during the HTTP session.

Sockets Active

The number of currently active sockets for the HTTP session.

Sockets Peak

The maximum number of sockets simultaneously active during the HTTP session.

Sockets Total

The total number of sockets active during the HTTP session.

Max Connections

The maximum number of concurrent HTTP connections for the VPN Concentrator since it was last rebooted or reset.

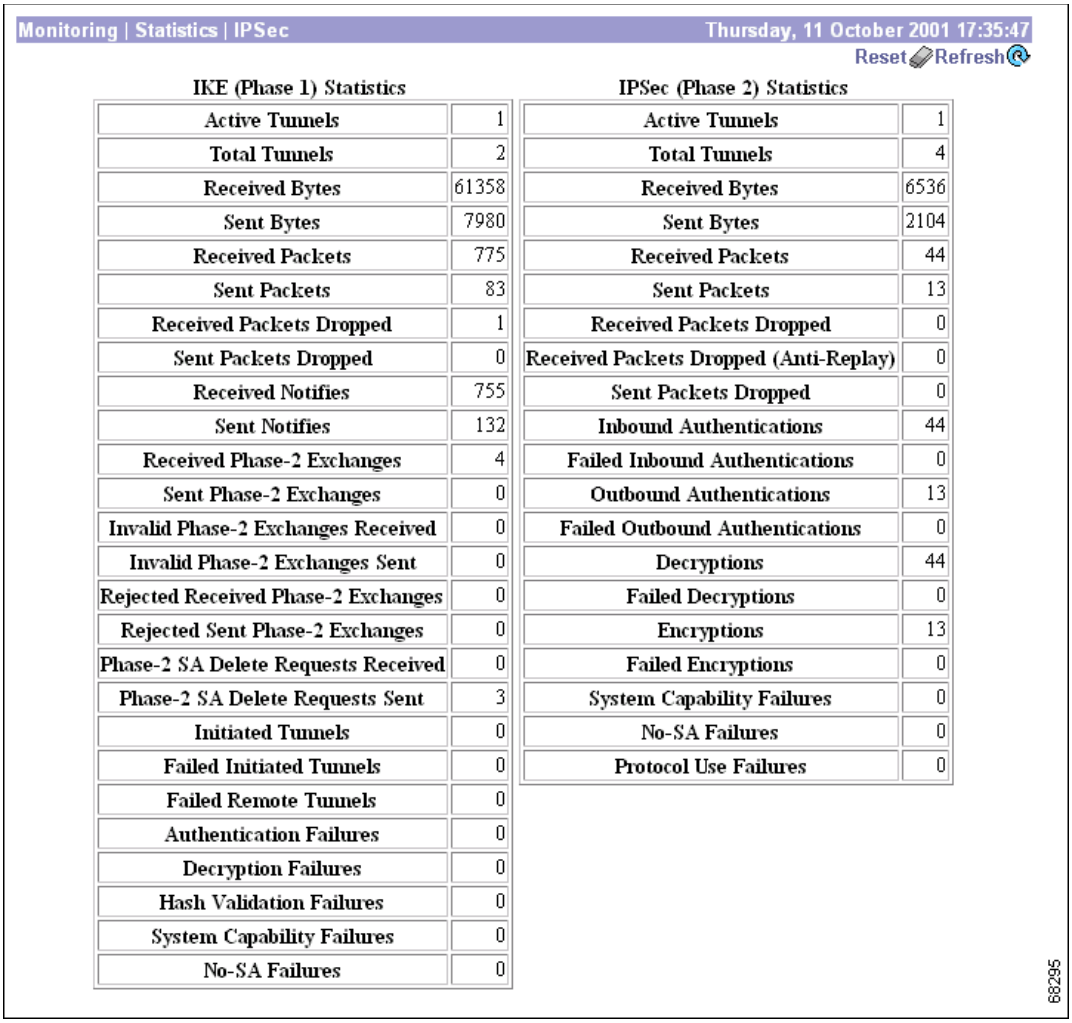
Monitoring | Statistics | IPSec

This screen shows statistics for IPSec activity—including current IPSec tunnels—on the VPN Concentrator since it was last booted or reset. These statistics conform to the IETF draft for the IPSec Flow Monitoring MIB.

The Monitoring | Sessions | Detail screens also show IPSec data.

To configure system-wide IPSec parameters and LAN-to-LAN connections, see the Configuration | System | Tunneling Protocols | IPSec screens. To configure IPSec parameters for users and groups, see Configuration | User Management. To configure IPSec parameters and SAs on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-16 Monitoring | Statistics | IPSec Screen



IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	2
Received Bytes	61358
Sent Bytes	7980
Received Packets	775
Sent Packets	83
Received Packets Dropped	1
Sent Packets Dropped	0
Received Notifies	755
Sent Notifies	132
Received Phase-2 Exchanges	4
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	3
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	0
Authentication Failures	0
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0
No-SA Failures	0

IPSec (Phase 2) Statistics

Active Tunnels	1
Total Tunnels	4
Received Bytes	6536
Sent Bytes	2104
Received Packets	44
Sent Packets	13
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	44
Failed Inbound Authentications	0
Outbound Authentications	13
Failed Outbound Authentications	0
Decryptions	44
Failed Decryptions	0
Encryptions	13
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IKE control tunnels, both for LAN-to-LAN connections and remote access.

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 Notifies

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, for example: error packets, keepalive packets, etc.

Sent Notifies

The cumulative total of notify packets sent by all currently and previously active IKE tunnels. See comments for Received Notifies.

Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges received by all currently and previously active IKE tunnels, in other words, 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, in other words, the total of Phase-2 negotiations initiated by this VPN Concentrator.

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 Concentrator 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 Concentrator, sent, and rejected, by all currently and previously active IKE tunnels. See the previous comment.

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 Concentrator initiated. The VPN Concentrator initiates tunnels only for LAN-to-LAN connections.

Failed Initiated Tunnels

The cumulative total of IKE tunnels that this VPN Concentrator 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. This number should be at or near zero; if not, check for misconfiguration or SEP module problems.

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 might 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, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IPSec Phase-2 tunnels, both for LAN-to-LAN connections and remote access.

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 might 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 or SEP module problems.

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 for IPSec subsystem or SEP module problems.

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 might 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.

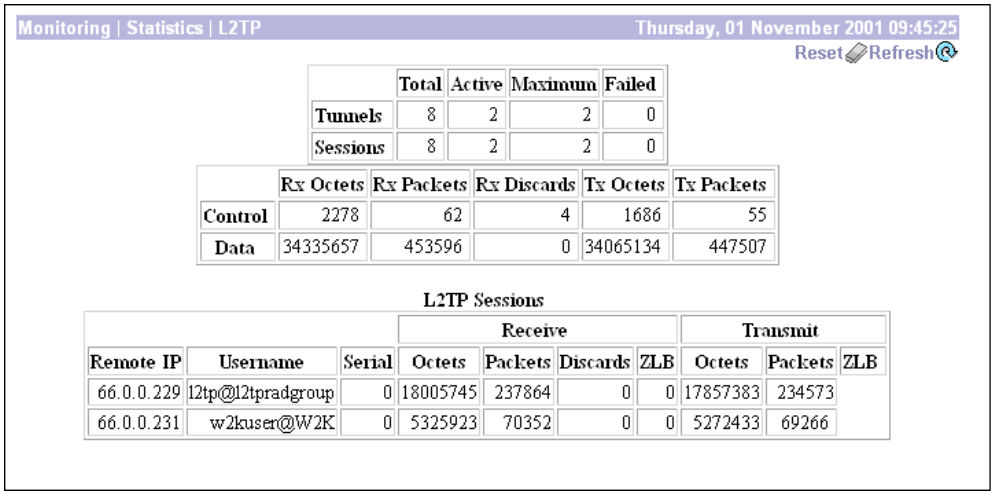
Monitoring | Statistics | L2TP

This screen shows statistics for L2TP activity on the VPN Concentrator since it was last booted or reset, and for current L2TP sessions.

The Monitoring | Sessions | Detail screens also show L2TP data.

To configure system-wide L2TP parameters, see the Configuration | System | Tunneling Protocols | L2TP screen. To configure L2TP parameters for users and groups, see Configuration | User Management. To configure L2TP on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-17 Monitoring | Statistics | L2TP Screen



	Total	Active	Maximum	Failed
Tunnels	8	2	2	0
Sessions	8	2	2	0

	Rx Octets	Rx Packets	Rx Discards	Tx Octets	Tx Packets
Control	2278	62	4	1686	55
Data	34335657	453596	0	34065134	447507

			Receive				Transmit		
Remote IP	Username	Serial	Octets	Packets	Discards	ZLB	Octets	Packets	ZLB
66.0.0.229	l2tp@l2tpradgroup	0	18005745	237864	0	0	17857383	234573	
66.0.0.231	w2kuser@W2K	0	5325923	70352	0	0	5272433	69266	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Tunnels

The total number of L2TP tunnels successfully established since the VPN Concentrator was last booted or reset.

Active Tunnels

The number of L2TP tunnels that are currently active.

Maximum Tunnels

The maximum number of L2TP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Failed Tunnels

The number of L2TP tunnels that failed to become established since the VPN Concentrator was last booted or reset.

Total Sessions

The total number of user sessions successfully established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The L2TP Sessions table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through L2TP tunnels on the VPN Concentrator since it was last booted or reset.

Failed Sessions

The number of sessions that failed to become established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Rx Octets Control / Data

The number of L2TP control / data channel octets (bytes) received by the VPN Concentrator since it was last booted or reset.

Rx Packets Control / Data

The number of L2TP control / data channel packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of L2TP control / data channel packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of L2TP control/data channel octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of L2TP control/data channel packets transmitted by the VPN Concentrator since it was last booted or reset.

L2TP Sessions

This table shows statistics for active L2TP sessions on the VPN Concentrator. Each active session is a row.

Remote IP

The IP address of the remote host that established the L2TP tunnel for this session, in other words, the tunnel endpoint IP address. The Monitoring | Sessions screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within an L2TP tunnel. This is typically the login name of the remote user.

Serial

The serial number of the session within an L2TP tunnel. If there are multiple sessions using a tunnel, each session has a unique serial number.

Receive Octets

The total number L2TP data octets (bytes) received by this session.

Receive Packets

The total number of L2TP data packets received by this session.

Receive Discards

The total number of L2TP data packets received and discarded by this session.

Receive ZLB

The total number of L2TP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of L2TP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of L2TP data packets transmitted by this session.

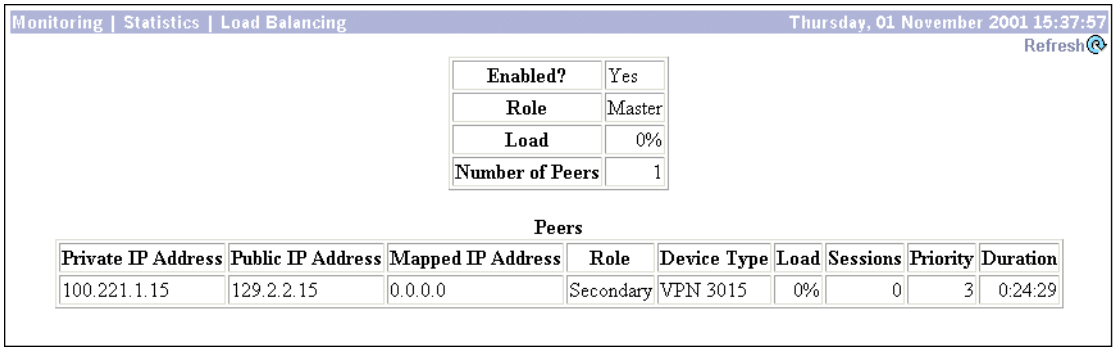
Transmit ZLB

The total number of L2TP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Monitoring | Statistics | Load Balancing

This screen shows statistics for load balancing on the VPN Concentrator since it was last booted or reset.

Figure 17-18 Monitoring | Statistics | Load Balancing Screen



Enabled?

Indicates whether load balancing has been enabled on this VPN Concentrator.

Role

The role of this VPN Concentrator within the virtual cluster. It is either a virtual cluster master or a secondary device.

Load

The percentage of the cluster's total session load that this VPN Concentrator is carrying.

Number of Peers

The number of other VPN Concentrators in the virtual cluster.

Peers

The peers chart shows configuration details and session statistics of the other VPN Concentrators in the virtual cluster.

Private IP Address

The private IP address of the peer.

Public IP Address

The public IP address of the peer.

Mapped IP Address

The NAT address of the peer, if it has one.

Role

The role of the peer within the virtual cluster. It is either a virtual cluster master or a secondary device.

Device Type

The VPN Concentrator model (such as 3005 or 3015) of the peer.

Load

The percentage of the cluster's total session load that the peer is carrying. You can view this information only from the virtual cluster master device. If you are viewing this field from a secondary device, its value is N/A.

Sessions

The number of currently active sessions on the peer. You can view this information only from the virtual cluster master device. If you are viewing this field from a secondary device, its value is N/A.

Priority

The likelihood that this peer will become the master at power-up or if the current master fails. For more information on priorities, see the Configuration | System | Load Balancing section.

Duration

The length of time this device has been connected to the virtual cluster.

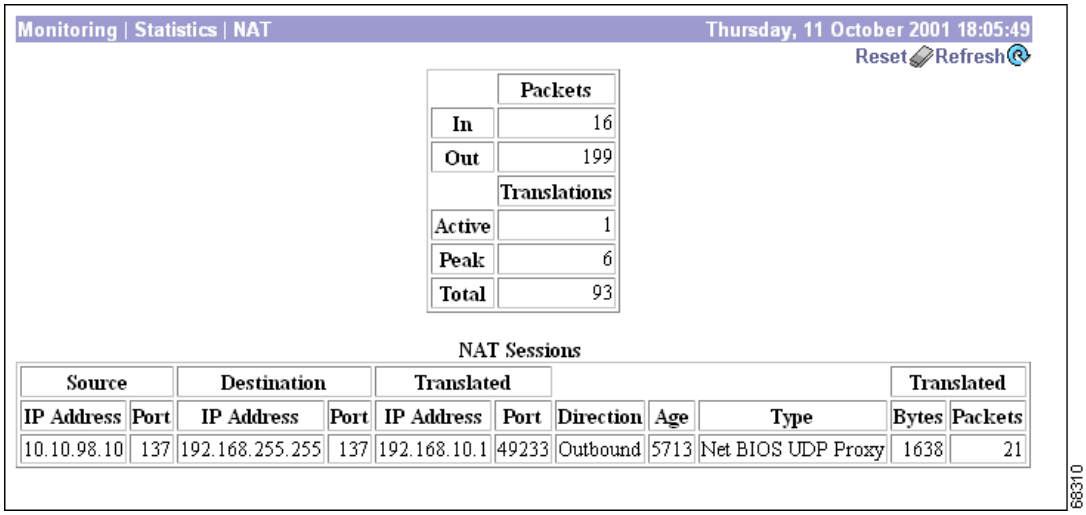
Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Monitoring | Statistics | NAT

This screen shows statistics for NAT (Network Address Translation) activity on the VPN Concentrator since it was last booted or reset.

Figure 17-19 Monitoring | Statistics | NAT screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets In/Out

The total of NAT packets inbound and outbound since the last time the VPN Concentrator was rebooted or reset.

Translations Active

The number of currently active NAT sessions.

Translations Peak

The maximum number of NAT sessions that were simultaneously active on the VPN Concentrator since it was last booted or reset.

Translations Total

The total number of NAT sessions on the VPN Concentrator since it was last booted or reset.

NAT Sessions

The following sections provide detailed information about active NAT sessions on the VPN Concentrator.

Source IP Address/Port

The source IP address and port for the NAT session.

Destination IP Address/Port

The destination IP address and port for the NAT session.

Translated IP Address/Port

The translated IP address and port for the NAT session. The VPN Concentrator uses this port number to keep track of which devices initiate data transfer; by keeping this record, the VPN Concentrator is able to correctly route responses.

Direction

The direction, inbound or outbound, of the data transferred for the NAT session.

Age

The number of half seconds remaining until the NAT session times out.

Type

The type of packets for the NAT session. The possible types are:

- TCP NAT session
- UDP NAT session
- FTP session
- TFTP session
- NetBIOS over TCP Proxy
- NetBIOS over UDP Proxy
- NetBIOS Datagram Service

Translated Bytes/Packets

The total number of translated bytes and packets for the NAT session.

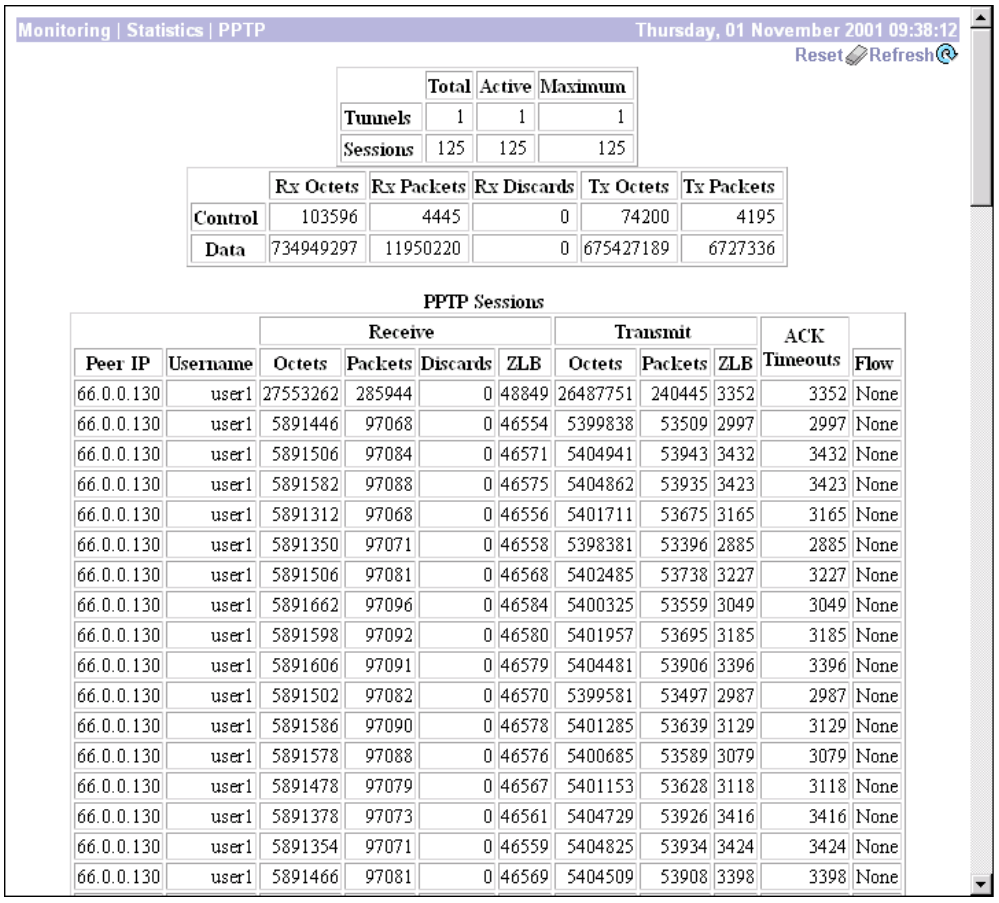
Monitoring | Statistics | PPTP

This screen shows statistics for PPTP activity on the VPN Concentrator since it was last booted or reset, and for current PPTP sessions.

The Monitoring | Sessions | Detail screens also show PPTP data.

To configure system-wide PPTP parameters, see the Configuration | System | Tunneling Protocols | PPTP screen. To configure PPTP parameters for users and groups, see Configuration | User Management. To configure PPTP on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-20 Monitoring | Statistics | PPTP Screen



	Total	Active	Maximum
Tunnels	1	1	1
Sessions	125	125	125

	Rx Octets	Rx Packets	Rx Discards	Tx Octets	Tx Packets
Control	103596	4445	0	74200	4195
Data	734949297	11950220	0	675427189	6727336

PPTP Sessions

		Receive				Transmit			ACK	
Peer IP	Username	Octets	Packets	Discards	ZLB	Octets	Packets	ZLB	Timeouts	Flow
66.0.0.130	user1	27553262	285944	0	48849	26487751	240445	3352	3352	None
66.0.0.130	user1	5891446	97068	0	46554	5399838	53509	2997	2997	None
66.0.0.130	user1	5891506	97084	0	46571	5404941	53943	3432	3432	None
66.0.0.130	user1	5891582	97088	0	46575	5404862	53935	3423	3423	None
66.0.0.130	user1	5891312	97068	0	46556	5401711	53675	3165	3165	None
66.0.0.130	user1	5891350	97071	0	46558	5398381	53396	2885	2885	None
66.0.0.130	user1	5891506	97081	0	46568	5402485	53738	3227	3227	None
66.0.0.130	user1	5891662	97096	0	46584	5400325	53559	3049	3049	None
66.0.0.130	user1	5891598	97092	0	46580	5401957	53695	3185	3185	None
66.0.0.130	user1	5891606	97091	0	46579	5404481	53906	3396	3396	None
66.0.0.130	user1	5891502	97082	0	46570	5399581	53497	2987	2987	None
66.0.0.130	user1	5891586	97090	0	46578	5401285	53639	3129	3129	None
66.0.0.130	user1	5891578	97088	0	46576	5400685	53589	3079	3079	None
66.0.0.130	user1	5891478	97079	0	46567	5401153	53628	3118	3118	None
66.0.0.130	user1	5891378	97073	0	46561	5404729	53926	3416	3416	None
66.0.0.130	user1	5891354	97071	0	46559	5404825	53934	3424	3424	None
66.0.0.130	user1	5891466	97081	0	46569	5404509	53908	3398	3398	None

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Tunnels

The total number of PPTP tunnels created since the VPN Concentrator was last booted or reset, including those tunnels that failed to be established.

Active Tunnels

The number of PPTP tunnels that are currently active.

Maximum Tunnels

The maximum number of PPTP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Total Sessions

The total number of user sessions through PPTP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The PPTP Sessions table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through PPTP tunnels on the VPN Concentrator since it was last booted or reset.

Rx Octets Control / Data

The number of PPTP control/data octets (bytes) received by the VPN Concentrator since it was last booted or reset.

Rx Packets Control / Data

The number of PPTP control/data packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of PPTP control/data packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of PPTP control/data octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of PPTP control/data packets transmitted by the VPN Concentrator since it was last booted or reset.

PPTP Sessions

This table shows statistics for active PPTP sessions on the VPN Concentrator. Each active session is a row.

Peer IP

The IP address of the peer host that established the PPTP tunnel for this session, in other words, the tunnel endpoint IP address. The Monitoring | Sessions screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within a PPTP tunnel. This is typically the login name of the remote user.

Receive Octets

The total number of PPTP data octets (bytes) received by this session.

Receive Packets

The total number of PPTP data packets received by this session.

Receive Discards

The total number of PPTP data packets received and discarded by this session.

Receive ZLB

The total number of PPTP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of PPTP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of PPTP data packets transmitted by this session.

Transmit ZLB

The total number of PPTP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

ACK Timeouts

The total number of acknowledgement timeouts seen on PPTP data packets for this session. When the system times out waiting for a data packet on which to piggyback an acknowledgement, it sends a ZLB instead. Therefore, this number should equal the Transmit ZLB number.

Flow

The state of packet flow control for this PPTP session:

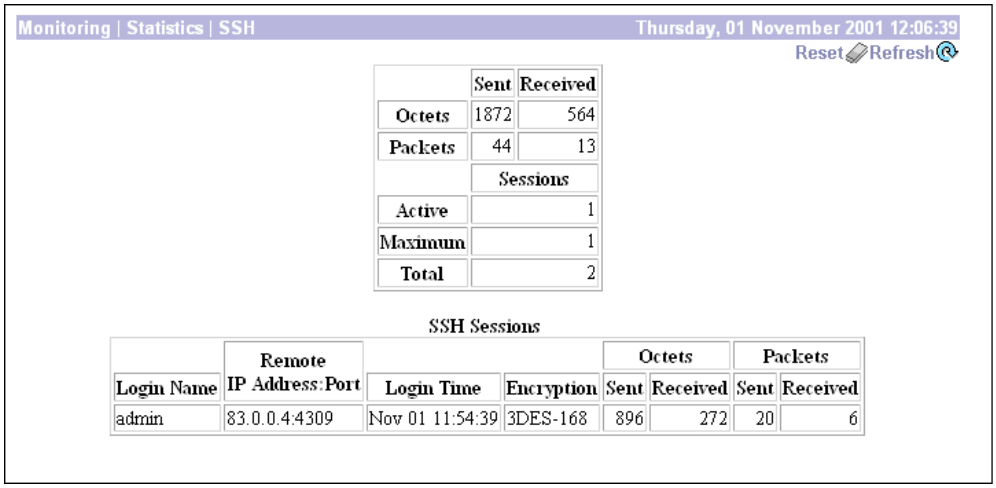
- Local = The local buffer is full. Packet flow for the local end of the session is OFF because the number of outstanding unacknowledged packets received from the peer is equal to the local window size.
- Peer = The peer buffer is full. Packet flow for the peer end of the session is OFF because the number of outstanding unacknowledged packets sent to the peer is equal to the peer's window size.
- Both = Both buffers are full. Packet flow for both ends of the session is OFF because the number of outstanding unacknowledged packets is equal to the window size on both ends.
- None = Neither end of the session has a full buffer. Packet flow for the session is ON. This is the normal operating state.

Monitoring | Statistics | SSH

This screen shows statistics for SSH (Secure Shell) protocol traffic on the VPN Concentrator since it was last booted or reset.

To configure SSH, see Configuration | System | Management Protocols | SSH.

Figure 17-21 Monitoring | Statistics | SSH Screen



Octets Sent / Received

The total number of SSH octets (bytes) sent / received since the VPN Concentrator was last booted or reset.

Packets Sent / Received

The total number of SSH packets sent / received since the VPN Concentrator was last booted or reset.

Total Sessions

The total number of SSH sessions since the VPN Concentrator was last booted or reset.

Active Sessions

The number of currently active SSH sessions.

Max Sessions

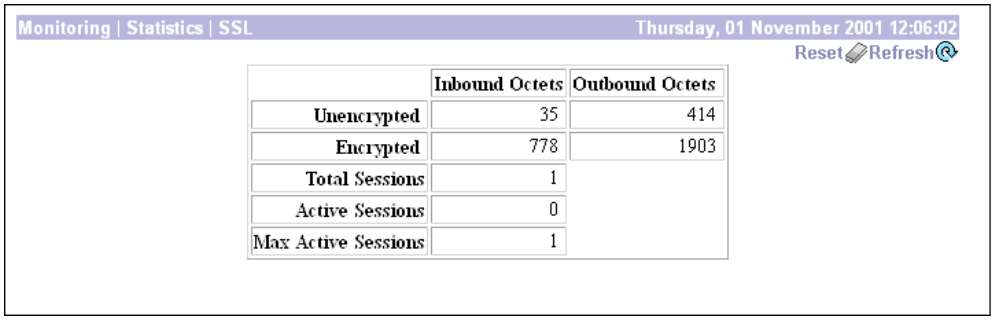
The maximum number of simultaneously active SSH sessions on the VPN Concentrator.

Monitoring | Statistics | SSL

This screen shows statistics for SSL (Secure Sockets Layer) protocol traffic on the VPN Concentrator since it was last booted or reset.

To configure SSL, see Configuration | System | Management Protocols | SSL.

Figure 17-22 Monitoring | Statistics | SSL Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset 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

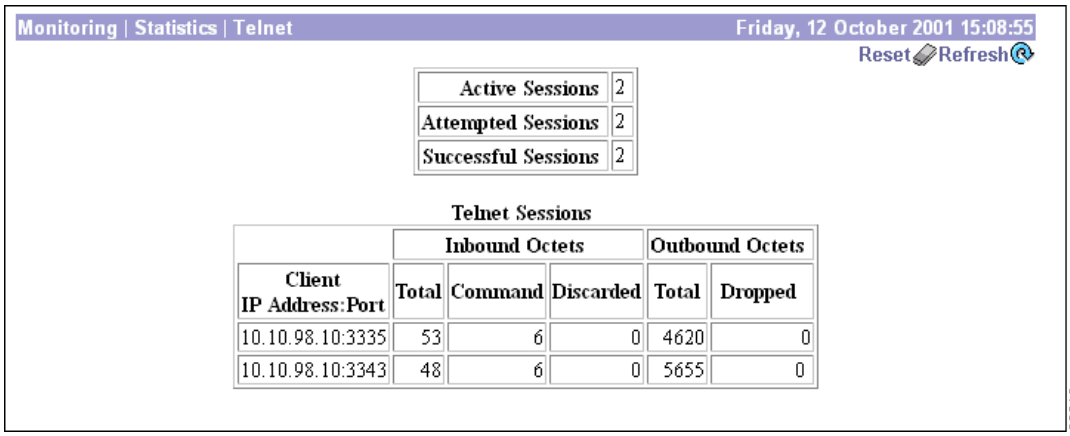
The maximum number of SSL sessions simultaneously active at any one time.

Monitoring | Statistics | Telnet

This screen shows statistics for Telnet activity on the VPN Concentrator since it was last booted or reset, and for current Telnet sessions.

To configure the VPN Concentrator's Telnet server, see the Configuration | System | Management Protocols | Telnet screen.

Figure 17-23 Monitoring | Statistics | Telnet Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator since it was last booted or reset.

Successful Sessions

The total number of Telnet sessions successfully established on the VPN Concentrator since it was last booted or reset.

Telnet Sessions

This table shows statistics for active Telnet sessions on the VPN Concentrator. 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

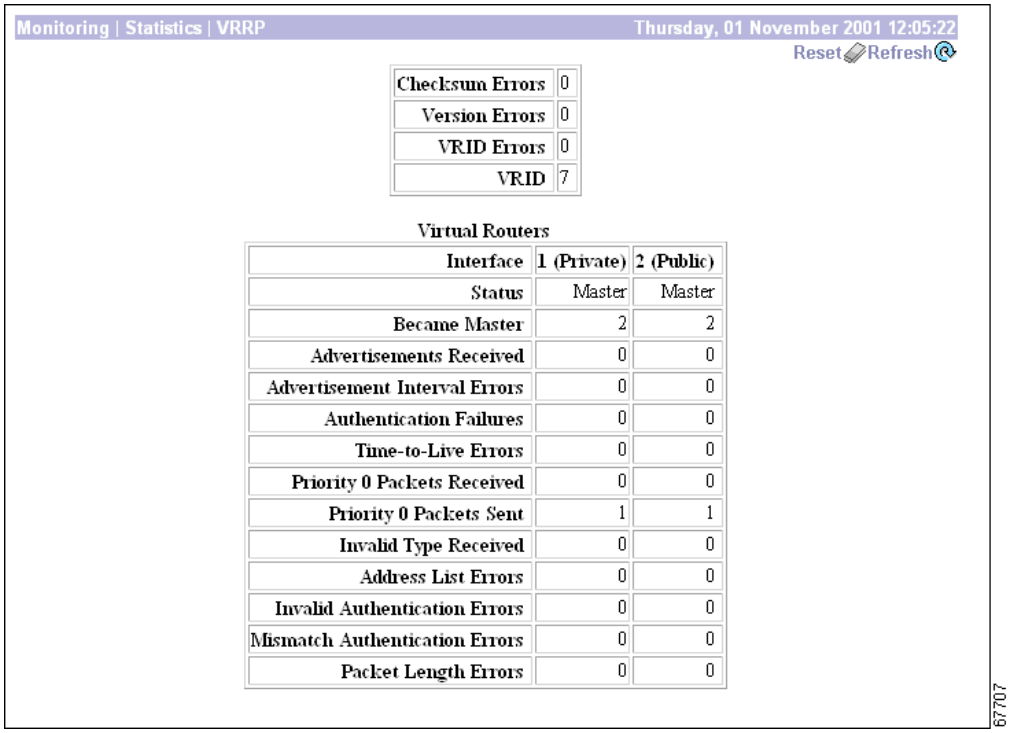
The number of outbound Telnet octets dropped during output processing by this session.

Monitoring | Statistics | VRRP

This screen shows status and statistics for VRRP (Virtual Router Redundancy Protocol) activity on the VPN Concentrator since it was last booted or reset.

To configure VRRP, see the Configuration | System | IP Routing | Redundancy screen.

Figure 17-24 Monitoring | Statistics | VRRP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Checksum Errors

The total number of VRRP packets received with an invalid VRRP checksum value.

Version Errors

The total number of VRRP packets received with an unknown or unsupported version number. The VPN Concentrator supports VRRP version 2 as defined in RFC 2338.

VRID Errors

The total number of VRRP packets received with an invalid VRRP Group ID number.

VRID

The identification number that uniquely identifies the group of virtual routers to which this VPN Concentrator belongs.

- Not Configured = VRRP has not been configured or enabled.

Virtual Routers

This table shows statistics for the virtual router on each configured VRRP interface on this VPN Concentrator.

Interface: 1 (Private), 2 (Public), 3 (External)

The Ethernet interface configured for VRRP.

Status

The status of the VRRP router in this VPN Concentrator:

- Master = VRRP is enabled and the router is functioning as the Master router.
- Backup = VRRP is enabled and the router is functioning as a Backup router, monitoring the status of the Master router.
- Init = VRRP has been configured but is disabled. The router is waiting to be enabled (initialized).

Became Master

The total number of times that this VPN Concentrator has become a VRRP Master router after having a different role. This number should be the same in all columns.

Advertisements Received

The total number of VRRP advertisements received by this interface.

Advertisement Interval Errors

The total number of VRRP advertisement packets received by this interface, in which the advertisement interval differs from the interval configured on this VPN Concentrator.

Authentication Failures

The total number of VRRP packets received by this interface that do not pass the authentication check.

Time-to-Live Errors

The total number of VRRP packets received by this interface with IP TTL (Time-To-Live) not equal to 255. All VRRP packets must have TTL = 255.

Priority 0 Packets Received

The total number of VRRP packets received by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Priority 0 Packets Sent

The total number of VRRP packets sent by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Invalid Type Received

The number of VRRP packets received by this interface with an invalid value in the Type field. For VRRP version 2, the only valid Type value is 1, which indicates an advertisement packet.

Address List Errors

The total number of packets received for which the address list does not match the list configured on this VPN Concentrator.

Invalid Authentication Errors

The total number of packets received by this interface with an unknown authentication type.

Mismatch Authentication Errors

The total number of packets received by this interface with an authentication type that differs from the configured authentication type.

Packet Length Errors

The total number of packets received by this interface with a packet length less than the length of the VRRP header.

Monitoring | Statistics | MIB-II

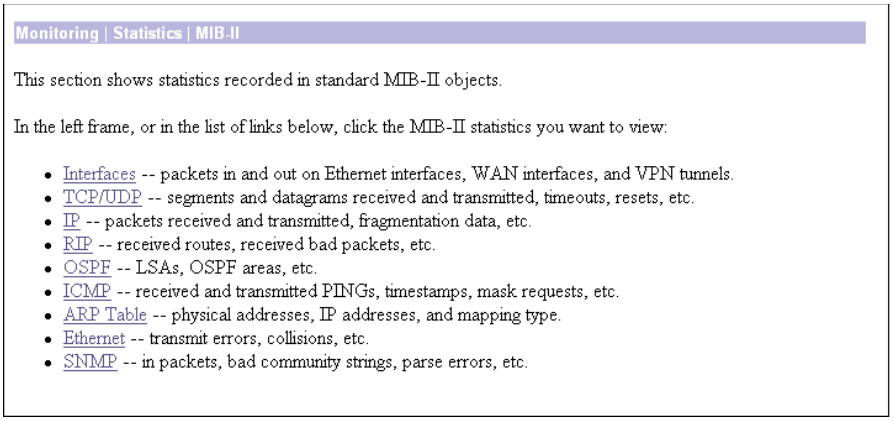
This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN Concentrator. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN Concentrator 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.
- RIP: Routing Information Protocol global route changes, bad packets and bad routes received, etc.
- OSPF: Open Shortest Path First protocol LSA data, Area 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 Concentrator's SNMP server, see the Configuration | System | Management Protocols | SNMP screen.

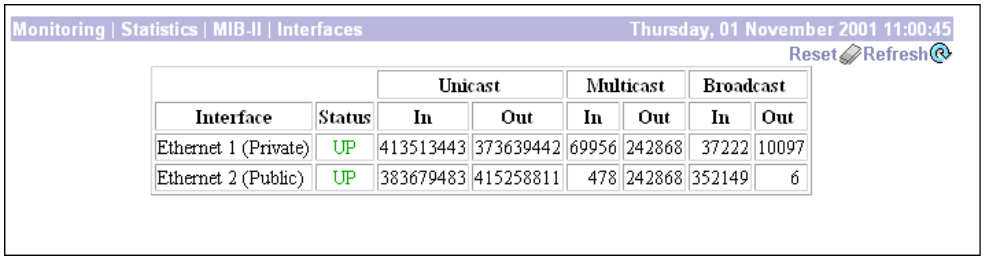
Figure 17-25 Monitoring | Statistics | MIB-II Screen



Monitoring | Statistics | MIB-II | Interfaces

This screen shows statistics in MIB-II objects for VPN Concentrator interfaces since the system was last booted or reset. This screen also shows statistics for VPN tunnels as logical interfaces. RFC 2233 defines interface MIB objects.

Figure 17-26 Monitoring | Statistics | MIB-II | Interfaces Screen



		Unicast		Multicast		Broadcast	
Interface	Status	In	Out	In	Out	In	Out
Ethernet 1 (Private)	UP	413513443	373639442	69956	242868	37222	10097
Ethernet 2 (Public)	UP	383679483	415258811	478	242868	352149	6

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator interface:

- Ethernet 1 (Private) = Ethernet 1 (Private) interface.
- Ethernet 2 (Public) = Ethernet 2 (Public) interface.
- Ethernet 3 (External) = Ethernet 3 (External) interface.
- 1000 and up = VPN tunnels, which are treated as logical interfaces.

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.

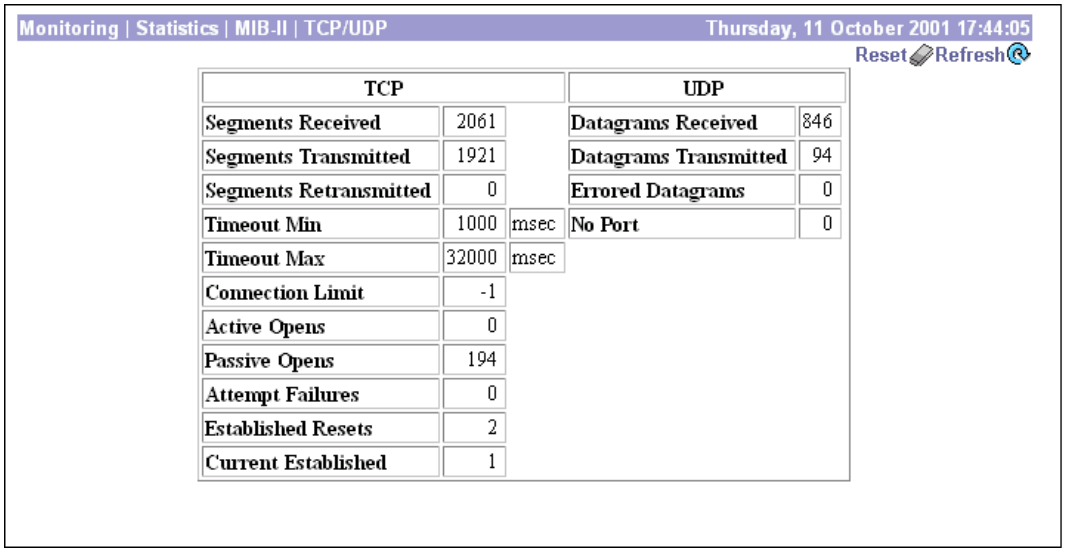
Broadcast Out

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 Concentrator since it was last booted or reset. RFC 2012 defines TCP MIB objects, and RFC 2013 defines UDP MIB objects.

Figure 17-27 Monitoring | Statistics | MIB-II | TCP/UDP Screen



TCP			UDP	
Segments Received	2061		Datagrams Received	846
Segments Transmitted	1921		Datagrams Transmitted	94
Segments Retransmitted	0		Errored Datagrams	0
Timeout Min	1000	msec	No Port	0
Timeout Max	32000	msec		
Connection Limit	-1			
Active Opens	0			
Passive Opens	194			
Attempt Failures	0			
Established Resets	2			
Current Established	1			

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 often 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

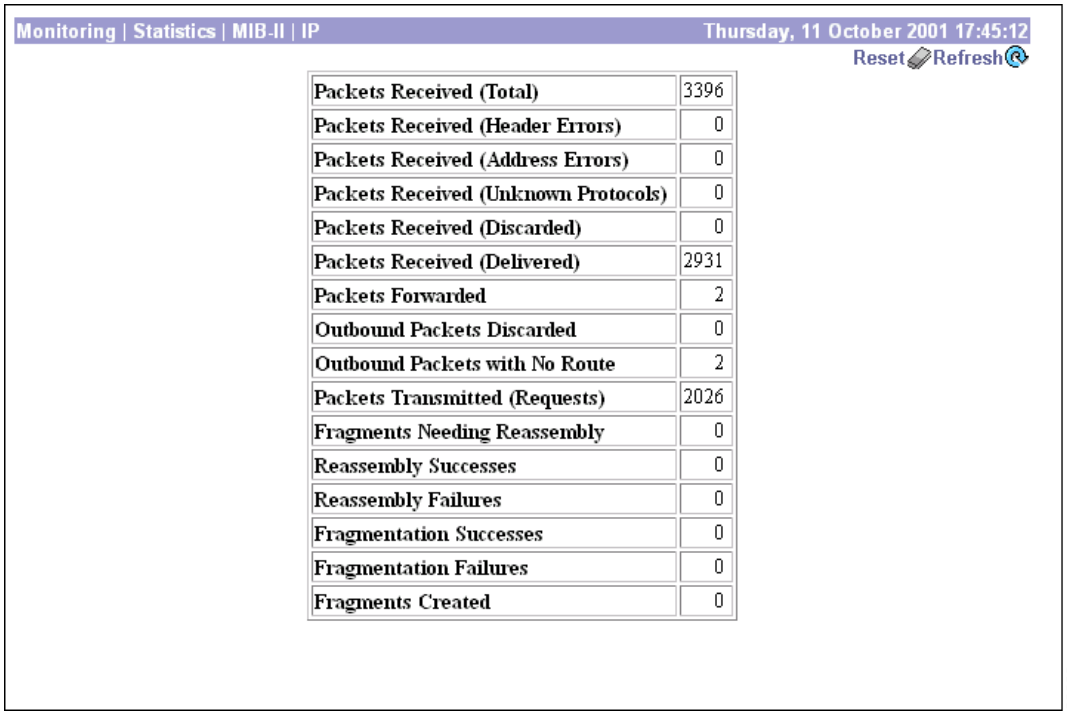
The total number of received UDP datagrams that could not be delivered because there was no application at the destination port. Datagram is the official UDP name for what is casually called a data packet.

Go to top of help page.

Monitoring | Statistics | MIB-II | IP

This screen shows statistics in MIB-II objects for IP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines IP MIB objects.

Figure 17-28 Monitoring | Statistics | MIB-II | IP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator, 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 check sums, 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 Concentrator. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, 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 (for example, 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 Concentrator; i.e., the VPN Concentrator was the final destination.

Packets Forwarded

The number of IP data packets received and forwarded to destinations other than the VPN Concentrator.

Outbound Packets Discarded

The number of outbound IP data packets that had no problems preventing their transmission to a destination, but that were discarded (for example, 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 Concentrator 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 Concentrator 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 Concentrator.

Fragmentation Failures

The number of IP data packets that have been discarded because they needed to be fragmented but could not be fragmented (for example, because the Don’t Fragment flag was set).

Fragments Created

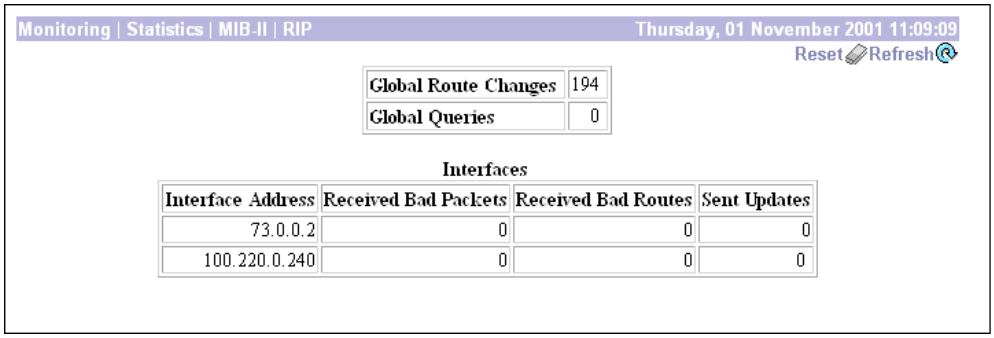
The number of IP data packet fragments that have been generated by the VPN Concentrator.

Monitoring | Statistics | MIB-II | RIP

This screen shows statistics in MIB-II objects for RIP version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1724 defines RIP version 2 MIB objects.

To configure RIP on interfaces, see Configuration | Interfaces.

Figure 17-29 Monitoring | Statistics | MIB-II | RIP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Global Route Changes

The total number of route changes made to the IP route database by RIP. This number does not include changes that only refresh the age route of a route.

Global Queries

The total number of responses sent to RIP queries from other systems.

Interfaces

This table shows a row of statistics for each configured interface.

Interface Address

The IP address configured on the interface.

Received Bad Packets

The number of RIP response packets received by this interface that were subsequently discarded for any reason (such as wrong version or unknown command type).

Received Bad Routes

The number of routes in valid RIP packets received by this interface that were ignored for any reason (such as unknown address family or invalid metric).

Sent Updates

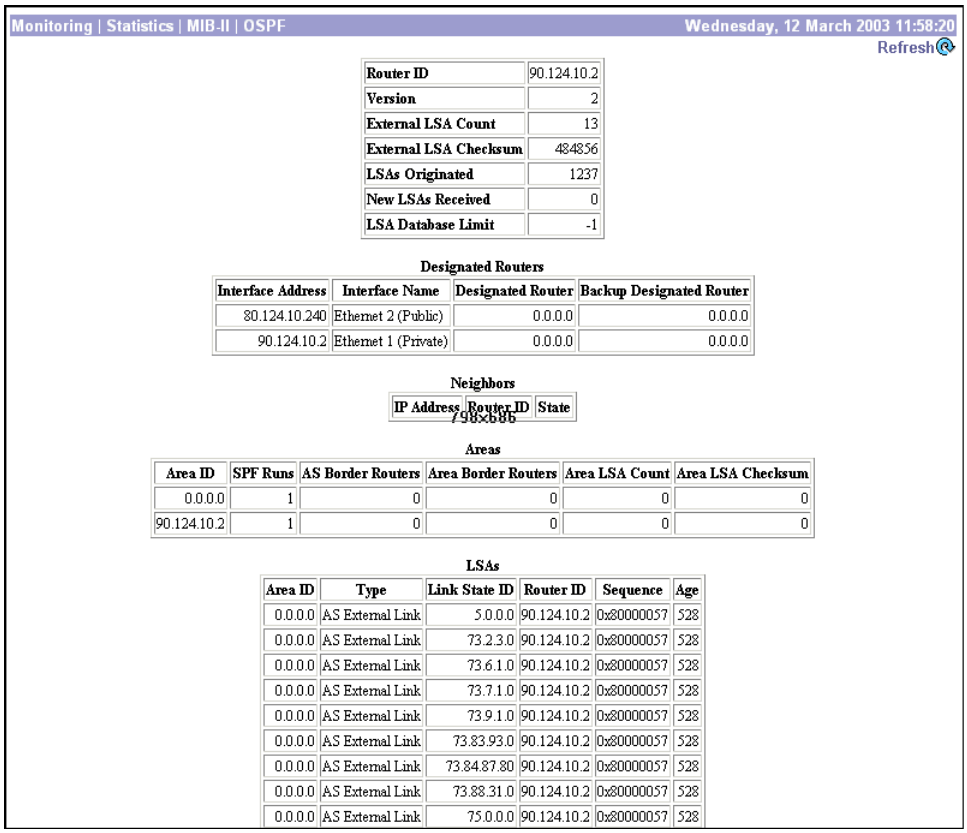
The number of triggered RIP updates actually sent by this interface. This number does not include full updates sent containing new information.

Monitoring | Statistics | MIB-II | OSPF

This screen shows statistics in MIB-II objects for OSPF version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1850a defines OSPF version 2 MIB objects.

To configure OSPF on interfaces, see Configuration | Interfaces. To configure system-wide OSPF parameters, see Configuration | System | IP Routing.

Figure 17-30 Monitoring | Statistics | MIB-II | OSPF Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Router ID

The VPN Concentrator OSPF router ID. This ID uniquely identifies the VPN Concentrator to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network. 0.0.0.0 means no router is configured.

Version

The current version number of the OSPF protocol running on the VPN Concentrator.

External LSA Count

The number of external Link-State Advertisements (LSAs) in the link-state database. LSAs from neighboring OSPF Autonomous Systems (AS) describe the state of the AS router's interfaces and routing paths.

External LSA Checksum

The sum of the check sums of the external Link-State Advertisements in the link-state database. You can use this sum to determine if there has been a change in the OSPF router link-state database of the system, and to compare its database with other routers.

LSAs Originated

The number of new Link-State Advertisements that the system has originated. This number increments each time the OSPF router originates a new LSA.

New LSAs Received

The number of Link-State Advertisements received that are completely new LSAs. This number does not include newer instances of self-originated LSAs.

LSA Database Limit

The maximum number of external LSAs that can be stored in the link-state database. A value of -1 means there is no limit.

Designated Routers

This table shows a row of statistics for each enabled VPN Concentrator interface. When OSPF routing is enabled on an interface, that interface communicates with other OSPF routers in its area, and each area elects one OSPF router to be the Designated Router.

Interface Address

The IP address of the VPN Concentrator interface that communicates with its area.

Interface Name

The VPN Concentrator interface that communicates with its area:

- Ethernet 1 (Private) = Ethernet 1 (Private) interface.
- Ethernet 2 (Public) = Ethernet 2 (Public) interface.
- Ethernet 3 (External) = Ethernet 3 (External) interface.

Designated Router

The IP address of the Designated Router in this OSPF area.

Backup Designated Router

The IP address of the backup Designated Router in this OSPF area.

Neighbors

This table shows a row of statistics for each OSPF neighbor, for all areas in which the VPN Concentrator participates. A neighbor is another OSPF router in an OSPF area, and this table includes all such areas for the VPN Concentrator.

IP Address

The IP address of the neighboring OSPF router.

Router ID

The router ID of the neighboring OSPF router, which uniquely identifies it to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier. By convention, however, it is the same as the IP address of the interface that is connected to the OSPF router network.

State

The state of the relationship with this neighboring OSPF router:

- Down = (Red) The VPN Concentrator has received no recent information from this neighbor. The neighbor might be out of service, or it might not have been in service long enough to establish its presence (at startup).
- Initializing = The VPN Concentrator has received a Hello packet from this neighbor, but it has not yet established bidirectional communication.
- Attempting = This state applies only to neighbors in an NBMA (Non-Broadcast Multi-Access) OSPF network. It indicates that the VPN Concentrator has received no recent information from this neighbor, but it is trying to establish contact by sending Hello packets at the Hello Interval.
- Two Way = The VPN Concentrator has established bidirectional communication with this neighbor, but has not established adjacency, in other words, they are not exchanging routing information.
- Exchange Start = The VPN Concentrator and this neighbor are in the first step of establishing an adjacency relationship.
- Exchanging = The VPN Concentrator is describing its entire link state database by sending Database Description packets to this neighbor, to establish an adjacency relationship.
- Loading = The VPN Concentrator is sending Link State Request packets to this neighbor asking for the more recent LSAs that have been discovered but not yet received in the Exchange state.
- Full = (Green) The VPN Concentrator is in a fully adjacent relationship with this neighbor. This adjacency now appears in router LSAs and network LSAs.

Areas

This table shows a row of statistics for each OSPF Area.

Area ID

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. 0.0.0.0 identifies a special area—the backbone—that contains all area border routers.

SPF Runs

The number of times that the system has calculated the intra-area route table (SPF, or Shortest Path First table) using the link-state database of this area.

AS Border Routers

The total number of Autonomous System border routers reachable within this area.

Area Border Routers

The total number of area border routers reachable within this area.

Area LSA Count

The total number of Link-State Advertisements in the link-state database of this area, excluding AS external LSAs.

Area LSA Checksum

The sum of the check sums of the Link-State Advertisements in the link-state database of this area. This sum excludes external LSAs. You can use this sum to determine if there has been a change in the link-state database of the area, and to compare its database with other routers.

External LSAs

This table shows a row for each external Link-State Advertisement in the link-state database.

Area ID

The Area ID identifies the Area from which the LSA was received.

Type

The LSA type. Each LSA type has a different format:

- Router Link = Describes the states of the router's interfaces (LS Type 1).
- Network Link = Describes the set of routers attached to the network (LS Type 2).
- Summary Link = Describes routes to networks (LS Type 3).
- AS Summary Link = Describes routes to AS boundary routers (LS Type 4).
- AS External Link = Describes routes to destinations external to the AS (LS Type 5).
- Multicast Link = Describes group membership for multicast OSPF routing (LS Type 6).
- NSSA External Link = Describes routing for NSSAs: Not-So-Stubby-Areas (LS Type 7).

Link State ID

Either a router ID or an IP address that identifies the piece of the routing domain being described by the LSA.

Router ID

The identifier of the router in the Autonomous System that originated this LSA.

Sequence

The sequence number of this LSA. Sequence numbers are linear. They are used to detect old and duplicate LSAs. The larger the number, the more recent the LSA.

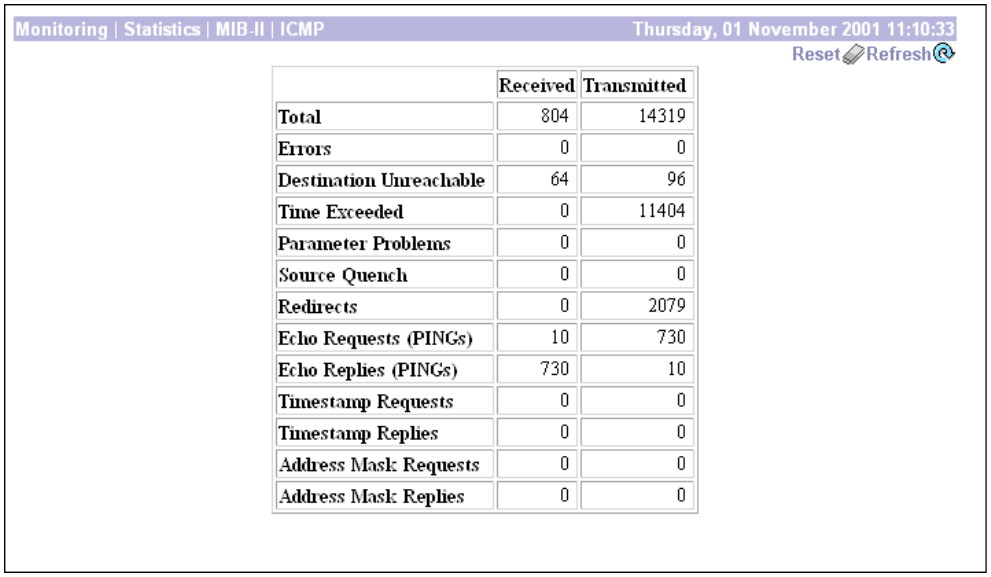
Age

The age of the LSA in seconds.

Monitoring | Statistics | MIB-II | ICMP

This screen shows statistics in MIB-II objects for ICMP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines ICMP MIB objects.

Figure 17-31 Monitoring | Statistics | MIB-II | ICMP Screen



	Received	Transmitted
Total	804	14319
Errors	0	0
Destination Unreachable	64	96
Time Exceeded	0	11404
Parameter Problems	0	0
Source Quench	0	0
Redirects	0	2079
Echo Requests (PINGs)	10	730
Echo Replies (PINGs)	730	10
Timestamp Requests	0	0
Timestamp Replies	0	0
Address Mask Requests	0	0
Address Mask Replies	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator 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 Concentrator received but determined to have ICMP-specific errors (bad ICMP check sums, bad length, etc.).

The number of ICMP messages that the VPN Concentrator 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.

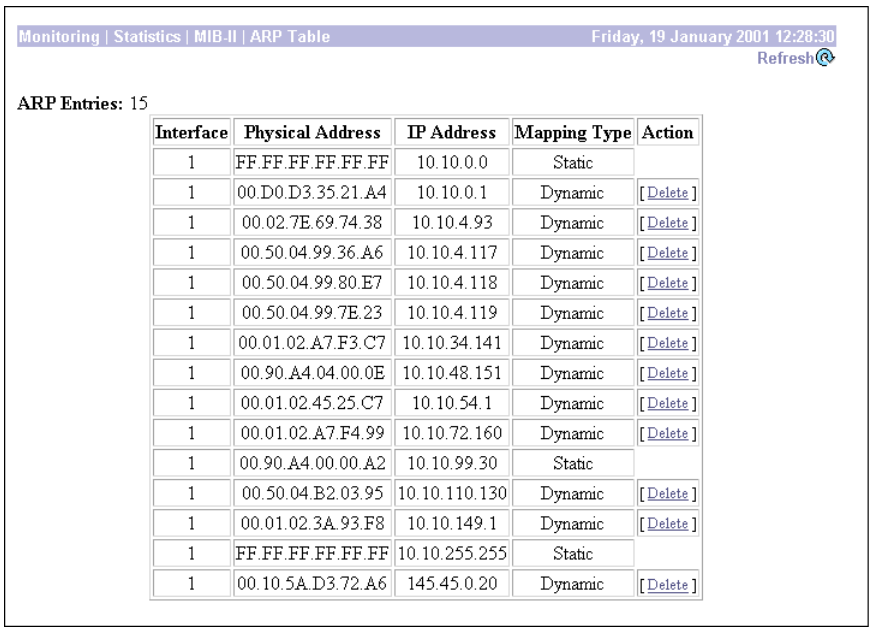
Monitoring | Statistics | MIB-II | ARP Table

This screen shows entries in the Address Resolution Protocol mapping table since the VPN Concentrator 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 might 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 17-32 Monitoring | Statistics | MIB-II | ARP Table Screen



Interface	Physical Address	IP Address	Mapping Type	Action
1	FF.FF.FF.FF.FF.FF	10.10.0.0	Static	
1	00.D0.D3.35.21.A4	10.10.0.1	Dynamic	[Delete]
1	00.02.7E.69.74.38	10.10.4.93	Dynamic	[Delete]
1	00.50.04.99.36.A6	10.10.4.117	Dynamic	[Delete]
1	00.50.04.99.80.E7	10.10.4.118	Dynamic	[Delete]
1	00.50.04.99.7E.23	10.10.4.119	Dynamic	[Delete]
1	00.01.02.A7.F3.C7	10.10.34.141	Dynamic	[Delete]
1	00.90.A4.04.00.0E	10.10.48.151	Dynamic	[Delete]
1	00.01.02.45.25.C7	10.10.54.1	Dynamic	[Delete]
1	00.01.02.A7.F4.99	10.10.72.160	Dynamic	[Delete]
1	00.90.A4.00.00.A2	10.10.99.30	Static	
1	00.50.04.B2.03.95	10.10.110.130	Dynamic	[Delete]
1	00.01.02.3A.93.F8	10.10.149.1	Dynamic	[Delete]
1	FF.FF.FF.FF.FF.FF	10.10.255.255	Static	
1	00.10.5A.D3.72.A6	145.45.0.20	Dynamic	[Delete]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Arp Entries

The total number of entries in the ARP table.

Interface

The VPN Concentrator network interface on which this mapping applies:

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.
- 1000 and up = VPN tunnels, which are treated as logical interfaces.

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 Concentrator.

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.

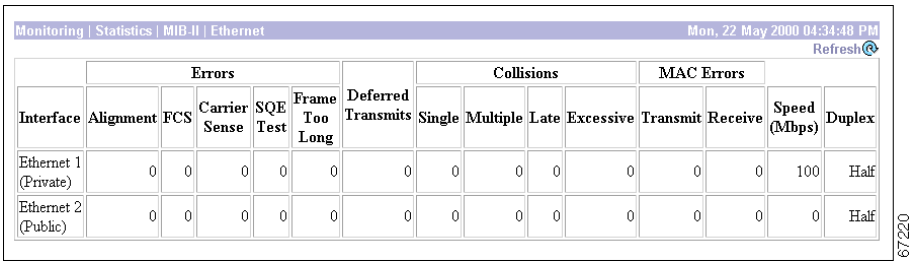
You cannot delete static mappings.

Monitoring | Statistics | MIB-II | Ethernet

This screen shows statistics in MIB-II objects for Ethernet interface traffic on the VPN Concentrator 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 17-33 Monitoring | Statistics | MIB-II | Ethernet Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The Ethernet interface to which the data in this row applies. Only configured interfaces are shown.

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:

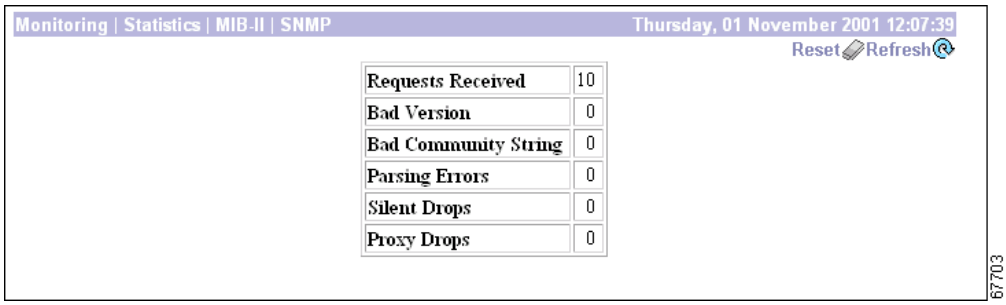
- Full = Full-Duplex: transmission in both directions at the same time.
- Half = Half-Duplex: transmission in only one direction at a time.

Monitoring | Statistics | MIB-II | SNMP

This screen shows statistics in MIB-II objects for SNMP traffic on the VPN Concentrator since it was last booted or reset. RFC 1907 defines SNMP version 2 MIB objects.

To configure the VPN Concentrator SNMP server, see Configuration | System | Management Protocols | SNMP.

Figure 17-34 Monitoring | Statistics | MIB-II | SNMP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

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 Concentrator.

Bad Version

The total number of SNMP messages received that were for an unsupported SNMP version. The VPN Concentrator supports SNMP version 2.

Bad Community String

The total number of SNMP messages received that used an SNMP community string the VPN Concentrator did not recognize. See Configuration | System | Management Protocols | SNMP Communities to configure permitted community strings. To protect security, the VPN Concentrator does not include the usual default public community string.

Parsing Errors

The total number of syntax or transmission errors encountered by the VPN Concentrator 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).

Using the Command-Line Interface

The VPN 3000 Concentrator Series Command-Line Interface (CLI) is a menu- and command-line-based configuration, administration, and monitoring system built into the VPN Concentrator. You use it via the system console, an SSH session, or Telnet (including SSL Telnet).

You can use the CLI to completely manage the system. You can access and configure the same parameters as the HTML-based VPN 3000 Concentrator Series Manager, except for IPSec LAN-to-LAN configuration.

Note LAN-to-LAN configuration is not supported via the CLI.

Note Certificate upload is available only via SSH.

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 VPN Concentrator Manager in the *VPN 3000 Series Concentrator Reference*. For example, to understand Ethernet interface configuration parameters and choices, see Configuration | Interfaces | Ethernet 1 2 3 in the "Interfaces" chapter of *VPN 3000 Series Concentrator Reference Volume I: Configuration.*

Accessing the CLI

You can access the CLI in three ways:

- Via the system console.
- Via a Telnet (or Telnet over SSL) client.
- Via SSH.

Console access

To access the CLI via console:

Step 1 Connect a PC to the VPN Concentrator via a straight-through RS-232 serial cable (which Cisco supplies with the system) between the Console port on the VPN Concentrator and the serial port on the PC. For more information, see the *VPN Concentrator Getting Started* manual.

Step 2 Start a terminal emulator (e.g., HyperTerminal) on the PC. Configure a connection to COM1 with port settings of:

- Bits per second = 9600.
- Data bits= 8.
- Parity = None.
- Stop bit = 1.
- Flow control = None.

Step 3 Set the emulator for VT100 emulation, or let it auto-detect the emulation type.

Step 4 Press **Enter** on the PC keyboard until you see the login prompt. (You might 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:

Step 1 Enable the Telnet or Telnet/SSL server on the VPN Concentrator. (They are both enabled by default.) See the Configuration | System | Management Protocols | Telnet screen on the VPN Concentrator Manager.

Step 2 Start the Telnet or Telnet/SSL client, and connect to the remote system using these parameters:

- Host Name or Session Name = The IP address on the VPN Concentrator Ethernet 1 (Private) interface; e.g., 10.10.147.2
- Port = Telnet (The default Telnet port is 23; the default Telnet/SSL port is 992.)
- Terminal Type = VT100 or ANSI
- Telnet/SSL only: If the client offers it, enable *both* SSL and SSL Only.

Step 3 The VPN Concentrator displays a login prompt:

```
Login: _
```

SSH Access

To access the CLI via an SSH client:

Step 1 Enable the SSH server on the VPN Concentrator. (It is enabled by default.) See the Configuration | System | Management Protocols | SSH screen on the VPN Concentrator Manager.

Step 2 Start the SSH client, and connect to the remote system using these parameters:

- Host Name or Session Name = The IP address on the VPN Concentrator Ethernet 1 (Private) interface; e.g., 10.10.147.2
- Port = SSH (The default SSH port is 22.)
- Terminal Type = VT100 or ANSI
- User name = **`admin`**

Step 3 A security warning might appear stating: “There is no entry for this server in your list of know hosts.” If this warning appears, continue.

Step 4 Enter your administrative password, and connect to the VPN Concentrator. When your connection is established, you are already logged in.

Starting the CLI

You start the CLI by logging in.

CLI login usernames and passwords for console, Telnet, and SSH 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. (The CLI does not show your password entry.)

```
Login: admin
Password: admin
```

The CLI displays the opening welcome message, the main menu, and the Main -> prompt:

```
                Welcome to
               Cisco Systems
        VPN 3000 Concentrator Series
           Command Line Interface
Copyright (C) 1998-2002 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 Management> General Config> 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.

Specifying Configured Items

Many menus give choices that act on configured items—such as groups, users, filter rules, etc.—and the CLI lists those items with a number and their name. To specify an item, you can usually enter either its number or its name. The CLI indicates when you must use a specific identifier (usually the item's number).

For example, the Configuration > User Management > Groups menu lists configured groups:

```
Current User Groups
----------------------------------------------------------------
| 1. QuickGroup                        | 2. IPSecGroup
----------------------------------------------------------------

1) Add a Group
2) Modify a Group
3) Delete a Group
4) Back

Groups -> _
```

To delete QuickGroup, enter **3** at the prompt. The CLI displays:

```
> Enter the Group to Delete

Groups -> _
```

At the prompt you can enter either its number (**1**) or its name (**QuickGroup**).

However, this next example shows the prompt for a specific identifier. The Configuration > System Management > Servers > Authentication Servers menu lists configured servers:

```
Authentication Server Summary Table

Num |        Server       |        Type         |    Port
-------------------------------------------------------------
  1 |          Internal   |      Internal       |        0
  2 |     192.168.34.56   |        RADIUS       |        0
-------------------------------------------------------------

1) Add Authentication Server
2) Modify Authentication Server
3) Delete Authentication Server
4) Move Server Up
5) Move Server Down
6) Test Server
7) Back

Authentication -> _
```

To delete the RADIUS server, enter **3** at the prompt. The CLI displays:

```
> Delete Server (number)

Authentication -> _
```

At the prompt, you must enter **2** for the RADIUS server.

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

Once you become familiar with the structure of the CLI—which parallels the HTML-based VPN Concentrator Manager—you can quickly access any level by entering a series of numbers separated by periods. For example, suppose you want to change the General Parameters for the Base Group. The series of menus that gets to that level from the main menu is:

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

Main -> 1 (Configuration)

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

Config -> 3 (User Management)

1) Base Group
2) Groups
3) Users
4) Back

User Management -> 1 (Base Group)

1) General Parameters
2) Server Parameters
3) IPSec Parameters
4) VPN Client Firewall Parameters
5) Hardware Client Parameters
6) PPTP/L2TP Parameters
7) Back

Base Group -> 1 (General Parameters)

1) Access Parameters
2) Tunneling Protocols
3) SEP Config
4) Back

Base Group -> _
```

As a shortcut, you can just enter **1.3.1.1** at the Main-> prompt, and move directly to the Base Group General Parameters menu:

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

Main -> 1.3.1.1

1) Access Parameters
2) Tunneling Protocols
3) SEP Config
4) Back

Base Group -> _
```

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 Concentrator without *saving* the active configuration, you lose all 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 redisplays 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 the designation "-)" (rather than a number) in menus.

For example, here is the main menu for the default User administrator:

```
-) Configuration
-) Administration
3) Monitoring
-) Save changes to Config file
5) Help Information
6) Exit

Main -> _
```

The default user administrator can only monitor the VPN Concentrator, not configure system parameters or administer the system.

See the "Administration | Access Rights | Administrators" section for more information.

CLI Menu Reference

This section of the documentation 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 > User Management> Base Group menu.

Note 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.

Note Models 3015–3080 have more interfaces than the Model 3005. They also have additional SEP capacity. Therefore, CLI menu shortcuts differ by model where they involve interface and expansion card selections. We note some differences here, but please note carefully the system you are using.

Main Menu

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

Main -> _
```

1 Configuration

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

Config -> _
```

1.1 Configuration > Interface Configuration

```
This table shows current IP addresses.
.
.
.
```

Note The following menu appears on models 3015–3080 only.

```
1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Ethernet #3 (External)
4) Configure Power Supplies
5) Back

Interfaces -> _
```

Note The following menu appears on model 3005 only.

```
1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

Interfaces -> _
```

1.1.1, 1.1.2, or 1.1.3 Configuration > Interface Configuration > Configure Ethernet #1 or #2 or #3

Note The Configuration > Interface Configuration > Configure Ethernet #3 menu appears only on models 3015-3080. It does not appear on model 3005.

```
1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Select IP Filter
4) Select Ethernet Speed
5) Select Duplex
6) Set MTU
7) Set Port Routing Config
8) Set Bandwidth Management
9) Set Public Interface IPSec Fragmentation Policy
10) Back

Ethernet Interface 1 -> _
```

1.1.4 Configuration > Interface Configuration > Configure Power Supplies

Note The following menu appears on models 3015–3080 only.

```
Alarm Thresholds in centivolts (e.g. 361 = 3.61V)
Voltages will be adjusted to conform to the hardware.

1) Configure CPU voltage thresholds
2) Configure Power Supply 1 voltage thresholds
3) Configure Power Supply 2 voltage thresholds
4) Configure Board voltage thresholds
5) Back

Interfaces -> _
```

1.1.3 Configuration > Interface Configuration > Configure Power Supplies

Note The following menu appears on model 3005 only.

```
Alarm Thresholds in centivolts (e.g. 361 = 3.61V)
Voltages will be adjusted to conform to the hardware.

1) Configure CPU voltage thresholds
2) Configure Power Supply voltage thresholds
3) Configure Board voltage thresholds
4) Back

Interfaces -> _
```

1.2 Configuration > System Management

```
1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) Tunneling Protocols (PPTP, L2TP, etc.)
4) IP Routing (static routes, OSPF, etc.)
5) Management Protocols (Telnet, TFTP, FTP, etc.)
6) Event Configuration
7) General Config (system name, time, etc.)
8) Client Update
9) Load Balancing Configuration
10) Back

System -> _
```

1.2.1 Configuration > System Management > Servers

```
1) Authentication Servers
2) Authorization Servers
3) Accounting Servers
4) DNS Servers
5) DHCP Servers
6) Firewall Server
7) NTP Servers
8) Back

Servers -> _
```

1.2.2 Configuration > System Management > Address Management

```
1) Address Assignment
2) Address Pools
3) Back

Address -> _
```

1.2.3 Configuration > System Management > Tunneling Protocols

```
1) PPTP
2) L2TP
3) IPSec
4) Back

Tunnel -> _
```

Note The CLI does not include IPSec LAN-to-LAN configuration.

1.2.4 Configuration > System Management > IP Routing

```
1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

Routing -> _
```

1.2.5 Configuration > System Management > Management Protocols

```
1) Configure FTP
2) Configure HTTP/HTTPS
3) Configure TFTP
4) Configure Telnet
5) Configure SNMP
6) Configure SNMP Community Strings
7) Configure SSL
8) Configure SSH
9) Configure XML
10) Back

Network -> _
```

1.2.6 Configuration > System Management > Event Configuration

```
1) General
2) FTP Backup
3) Classes
4) Trap Destinations
5) Syslog Servers
6) SMTP Servers
7) Email Recipients
8) Back

Event -> _
```

1.2.7 Configuration > System Management > General Config

```
1) System Identification
2) System Time and Date
3) Session Configuration
4) Global Authentication Parameters
5) Back

General -> _
```

1.2.8 Configuration > System Management > Client Update

```
1) Client Update Enable
2) Client Update Entries
3) Back

Client Update -> _
```

1.2.9 Configuration > System Management > Load Balancing

```
1) Cluster Configuration
2) Device Configuration
3) Back

Load Balancing -> _
```

1.3 Configuration > User Management

```
1) Base Group
2) Groups
3) Users
4) Back

User Management -> _
```

1.3.1 Configuration > User Management > Base Group

```
1) General Parameters
2) Server Parameters
3) IPSec Parameters
4) VPN Client Firewall Parameters
5) Hardware Client Parameters
6) PPTP/L2TP Parameters
7) Back

Base Group -> _
```

1.3.2 Configuration > User Management > Groups

```
Current User Groups
.
.
.
1) Add a Group
2) Modify a Group
3) Delete a Group
4) Back

Groups -> _
```

1.3.3 Configuration > User Management > Users

```
Current Users
.
.
.
1) Add a User
2) Modify a User
3) Delete a User
4) Back

Users -> _
```

1.4 Configuration > Policy Management

```
1) Access Hours
2) Traffic Management
3) Group Matching
4) Back

Policy -> _
```

1.4.1 Configuration > Policy Management > Access Hours

```
Current Access Hours
.
.
.
1) Add Access Hours
2) Modify Access Hours
3) Delete Access Hours
4) Back

Access Hours -> _
```

1.4.2 Configuration > Policy Management > Traffic Management

```
1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back

Traffic -> _
```

2 Administration

```
1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Access Rights
7) File Management
8) Certificate Management
9) Back

Admin -> _
```

2.1 Administration > Administer Sessions

```
Active Sessions
.
.
.
1) Refresh Session Statistics
2) Reset Session Statistics
3) Restore Session Statistics
4) Logoff Sessions
5) Session Details
6) Filter Sessions on Group
7) Back

Admin -> _
```

2.2 Administration > Software Update

```
1) Concentrator
2) Clients
3) Bootloader
4) Back

Admin -> _
```

2.3 Administration > System Reboot

```
1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back

Admin -> _
```

2.3.2 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 -> _
```

2.3.3 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 -> _
```

2.4 Administration > Reboot Status

```
Reboot Status
-------------
No reboot is scheduled.

1) Refresh Reboot Status
2) Skip Notifications/Reboot Now
3) Logout
4) Back

Admin -->
```

2.6 Administration > Access Rights

```
1) Administrators
2) Access Control List
3) Access Settings
4) Admin AAA Servers
5) Back

Admin -> _
```

2.6.1 Administration > Access Rights > Administrators

```
Administrative Users
.
.
.
1) Modify Administrator
2) Back

Admin -> _
```

2.6.2 Administration > Access Rights > Access Control List

```
This is the Current Access List
.
.
.
1) Add Manager Workstation
2) Modify Manager Workstation
3) Delete Manager Workstation
4) Move Manager Workstation Up
5) Move Manager Workstation Down
6) Back

Admin -> _
```

2.6.3 Administration > Access Rights > Access Settings

```
1) Set Session Timeout
2) Set Session Limit
3) Set Config File Encryption
4) Zeroize/Regenerate DES Config File Encryption Key
5) Back

Admin -> _
```

2.6.4 Administration > Access Rights > Admin AAA Servers

```
1) Authentication Servers
2) Back

Admin -> _
```

2.7 Administration > File Management

```
List of Files
.
.
.
1) Delete File
2) Copy File
3) View File
4) Put File via TFTP
5) Get File via TFTP
6) Swap Config Files
7) Export XML File
8) Import XML File
9) Back

File -> _
```

2.7.6 Administration > File Management > Swap Configuration File

```
Every time the active configuration is saved,...
.
.
.

1) Swap
2) Back

Admin -> _
```

2.8 Administration > Certificate Management

```
1) Enrollment
2) Installation
3) Certificate Authorities
4) Identity Certificates
5) SSL Certificate
6) Enrollment Status
7) Back

Certificates -> _
```

2.8.1 Administration > Certificate Management > Enrollment

```
1) Identity Certificate Enrollment
2) SSL Certificate Enrollment
3) Back

Certificates ->
```

2.8.2 Administration > Certificate Management > Installation

```
1) Install CA Certificate
2) Install SSL Certificate with private key
3) Install Certificate obtained via enrollment
4) Back

Certificates -> _
```

2.8.3 Administration > Certificate Management > Certificate Authorities

```
Certificate Authorities
.
.
.
1) View Certificate
2) Delete Certificate
3) Configure Certificate
4) View CRL Cache
5) Clear CRL Cache
6) Back

Certificates -> _
```

2.8.4 Administration > Certificate Management > Identity Certificates

```
Identity Certificates
.
.
.
1) View Certificate
2) Delete Certificate
3) Renew Certificate
4) Back

Certificates -> _
```

2.8.5 Administration > Certificate Management > SSL Certificate

```
Subject
.
.
.

1) Delete Certificate
2) Generate Certificate
3) Renew Certificate
4) Back

Certificates ->
```

2.8.6 Administration > Certificate Management > Enrollment Status

```
Enrollment Requests

1) View Enrollment Request
2) Install/Activate Enrollment Request
3) Resubmit Enrollment Request
4) Delete/Cancel Enrollment Request
5) Back

Certificates ->
```

3 Monitoring

```
1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back

Monitor -> _
```

3.1 Monitoring > Routing Table

```
Routing Table
.
.
.
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) Save Log
4) Clear Log
5) 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

Note The following menu appears on models 3015–3080 only.

```
System Status
.
.
.
1) Refresh System Status
2) View Card Status
3) View LED status
4) View Memory Status
5) Back

Status -> _
```

Note The following menu appears on model 3005 only.

```
System Status
.
.
.
1) Refresh System Status
2) View Card Status
3) Back

Status ->
```

3.3.2 Monitoring > System Status > View Card Status

Note The following menu appears on models 3015–3080 only.

```
1) Card in Slot 1
2) Card in Slot 2
3) Card in Slot 3
4) Card in Slot 4
5) Back

Card Status -> _
```

Note The following menu appears on model 3005 only.

```
1) Card in Slot 1
2) Back

Card Status -> _
```

3.4 Monitoring > Sessions

Note The following menu appears on models 3015–3080 only.

```
1) View Session Statistics
2) View Top Ten Lists
3) View Session Protocols
4) View Session SEPs
5) View Session Encryption
6) Filter Sessions on Group
7) Back

Sessions -> _
```

Note The following menu appears on model 3005 only.

```
1) View Session Statistics
2) View Top Ten Lists
3) View Session Protocols
4) View Session Encryption
5) Filter Sessions on Group
6) Back

Sessions -> _
```

3.4.1 Monitoring > Sessions > View Session Statistics

```
Active Sessions
.
.
.
1) Refresh Session Statistics
2) Reset Session Statistics
3) Restore Session Statistics
4) Session Details
5) Back

Sessions -> _
```

3.4.2 Monitoring > Sessions > View Top Ten Lists

```
1) Top 10 Users based on Data
2) Top 10 Users based on Duration
3) Top 10 Users based on Throughput
4) Back

Sessions -> _
```

3.4.3 Monitoring > Sessions > View Session Protocols

```
Session Protocols
.
.
.
1) Refresh Session Protocols
2) Back

Sessions -> _
```

3.4.4 View Session SEPS

Note The following menu appears on models 3015–3080 only.

```
Session SEPs
.
.
.
1) Refresh Session SEPs
2) Back

Session ->
```

3.4.4 (3.4.5 on Models 3015-3080) Monitoring > Sessions > View Session Encryption

```
Session Encryption
.
.
.
1) Refresh Session Encryption
2) Back

Sessions -> _
```

3.4.5 (3.4.6 on Models 3015-3080) Monitoring > Sessions > Filter Sessions on Group

```
Current User Groups
.
.
.
> Group to view (-1 for All Groups, 0 for Base Group)

Sessions ->
```

3.5 Monitoring > General Statistics

```
1) Protocol Statistics
2) Server Statistics
3) Event Statistics
4) MIB II Statistics
5) Back

General -> _
```

3.5.1 Monitoring > General Statistics > Protocol Statistics

```
1) PPTP Statistics
2) L2TP Statistics
3) IPSec Statistics
4) HTTP Statistics
5) Telnet Statistics
6) DNS Statistics
7) VRRP Statistics
8) SSL Statistics
9) SSH Statistics
10) NAT Statistics
11) Back

General -> _
```

3.5.2 Monitoring > General Statistics > Server Statistics

```
1) Authentication Statistics
2) Accounting Statistics
3) Filtering Statistics
4) DHCP Statistics
5) Address Pool Statistics
6) Load Balancing Statistics
7) Compression Statistics
8) Admin AAA Authentication Statistics
9) Bandwidth Management Statistics
10) Back

General -> _
```

3.5.3 Monitoring > General Statistics > Event Statistics

```
Event Statistics
.
.
.
1) Refresh Event Statistics
2) Reset Event Statistics
3) Restore Event Statistics
4) Back

General -> _
```

3.5.4 Monitoring > General Statistics > MIB II Statistics

```
1) Interface-based
2) System-level
3) Back

MIB2 -> _
```

3.6 Monitoring > Dynamic Filters

```
Current Dynamic Filters
.
.
.
1) View Dynamic Filter Rules
2) Back

Dynamic Filters ->
```

Troubleshooting and System Errors

Appendix A describes common errors that can occur while configuring and using the system, and how to correct them. It also describes LED indicators on the system and its expansion modules.

Files for Troubleshooting

The VPN 3000 Concentrator 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, CONFIG.BAK—Normal configuration file used to boot the system, and backup configuration file

Event Logs

The VPN Concentrator 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. See Configuration | System | Events and Monitor | Event Log.

The VPN Concentrator 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. See Configuration | System | Events and Administration | File Management | Files.

Crash Dump File

If the VPN Concentrator crashes during operation, it saves internal system data in nonvolatile memory (NVRAM), and then automatically writes this data to a CRSHDUMP.TXT file in flash memory when it is rebooted. This file contains the crash date and time, software version, tasks, stack, registers, memory, buffers, and timers., which are helpful to Cisco support engineers. In case of a crash, we ask that you send this file when you contact Technical Assistance Center (TAC) for assistance. See Administration | File Management | Files for information on managing files in flash memory.

Configuration Files

The VPN Concentrator 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 | Files for information on managing files in flash memory.

VPN Concentrator Manager Errors

Table B-1 lists errors that might occur while using the HTML-based VPN Concentrator Manager with a browser.

Table B-1 VPN Concentrator Manager Errors

Symptom	Problem	Possible Cause	Solution
Browser Refresh or Reload Button Logs Out the Manager.	You clicked the **Refresh** or **Reload** button on the *browser* navigation toolbar, and the Manager logged out. The main login screen appears.	To protect access security, clicking **Refresh / Reload** on the browser toolbar automatically logs out the Manager session.	Do not use the browser navigation toolbar buttons with the VPN Concentrator Manager. Use only the Manager **Refresh** button where it appears on a screen. We recommend that you hide the browser navigation toolbar to prevent mistakes.
Browser Back or Forward Button displays an Incorrect Screen or Incorrect Data.	You clicked the **Back** or **Forward** button on the *browser* navigation toolbar, and the Manager displayed the wrong screen or incorrect data.	To protect security and the integrity of data entries, clicking **Back** or **Forward** on the browser toolbar deletes pointers and values within the Manager.	Do not use the browser navigation toolbar buttons with the VPN Concentrator Manager. Navigate using the location bar at the top of the Manager window, the table of contents in the left frame, or links on Manager screens. We recommend that you hide the browser navigation toolbar to prevent mistakes.
The Manager displays the Invalid Login or Session Timeout screen.	You entered an invalid administrator login name and password combination.	• Typing error • Invalid (unrecognized) login name or password.	Reenter the login name and password and click **Login**. Use a valid login name and password. type carefully.

Table B-1 VPN Concentrator Manager Errors (continued)

Symptom	Problem	Possible Cause	Solution
The Manager displays the Invalid Login or Session Timeout screen.	The Manager session has been idle longer than the configured timeout interval.	• No activity for (interval) seconds. The Manager resets the inactivity timer only when you click an action button (such as **Apply**, **Add**, or **Cancel**) 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. • Default timeout interval is 600 seconds (10 minutes). • Timeout interval set too low for normal use.	On the Administration | Access Rights | Access Settings screen, change the Session Timeout interval to a larger value and click **Apply**.
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.	You tried to perform some operation that is not allowed.	The screen displays a message that describes the cause.	Click **Retry the operation** to return to the screen where you were working and correct the mistake. Carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost. Click **Go to main menu** to go to the main Manager screen.
The Manager displays a screen with the message, "You are using an old browser or have disabled JavaScript..."	The VPN Concentrator Manager cannot work with the browser that you have invoked.	• You are using the Manager with an unsupported browser. • You are using the Manager with an obsolete browser. • You are using a browser that does not have JavaScript enabled.	Use Microsoft Internet Explorer version 4.0 or higher. Use Netscape Navigator version 4.5 or higher. Be sure JavaScript is enabled in the browser. See the section "Browser Requirements" in Chapter 1 of the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

Table B-1 VPN Concentrator Manager Errors (continued)

Symptom	Problem	Possible Cause	Solution
The Manager displays a screen with the message, "Not Allowed/You do not have sufficient authorization to access the specified page."	You tried to access an area of the Manager that you do not have authorization to access.	• You logged in using an administrator login name that has limited privileges. • You logged in from a workstation that has limited access privileges.	Log in using the system administrator login name and password. (Defaults are admin/admin.) Log in from a workstation with greater access privileges. Have the system administrator change your privileges on the Administration | Access Rights | Administrators screen. Have the system administrator change the privileges of your workstation on the Administration | Access Rights | Access Control List screen.
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.	The Manager could not find a screen.	• You updated the software image and did not clear the browser's cache.	Clear the browser cache: delete its temporary internet files, history files, and location bar references. Then try again.
		• There is an internal Manager error.	Please note the system information on the screen and contact TAC for assistance.
Microsoft Internet Explorer displays a Script Error dialog box that includes the error message, "No such interface supported."	While using a Manager function that opens another browser window (such as Save Needed, Help, or Software Update), Internet Explorer cannot open the window and displays the error dialog box.	A bug in the Internet Explorer JavaScript interpreter.	1. Click **No** on the error dialog box. 2. Log out of the Manager. 3. Close Internet Explorer. 4. Reinstall Internet Explorer.

Command-Line Interface Errors

Table B-2 lists errors that might occur while using the menu-based Command-line Interface from a console or Telnet session.

Table B-2 VPN 3000 Concentrator Command-Line Interface Errors

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

LED Indicators

LED indicators on the VPN Concentrator and its expansion modules are normally green. The usage gauge LEDs are normally blue. LEDs that are amber or off might indicate an error condition. NA means not applicable; that is, the LED does not have that state.

Contact TAC if any LED indicates an error condition.

VPN Concentrator (front) LEDs

The LEDs on the front of the VPN 3000 Concentrator are as follows:

LED Indicator	Green	Amber	Off
System	Power on. Normal Blinking Green (Model 3005 only)—System is in a shutdown (halted) state, ready to power off.	System has crashed and halted. *Error.*	Power off. (All other LEDs are also off.)
The LEDs below exist only on Models 3015–3080			
Ethernet Link Status 1 2 3	Connected to network and enabled. Blinking Green—Connected to network and configured, but disabled.	NA	Not connected to network or not enabled.
Expansion Modules Insertion Status 1 2 3 4	SEP or SEP-E module installed in system.	NA	Module not installed in system.
Expansion Modules Run Status 1 2 3 4	SEP or SEP-E module operational.	Module failed during operation. *Error.*	If installed, module failed diagnostics or encryption code is not running. *Error.*
Fan Status	Operating normally.	Not running or RPM below normal range. *Error.*	NA
Power Supplies A B	Installed and operating normally.	Voltage(s) outside of normal ranges. *Error.*	Not installed.
CPU Utilization	This statistic selected for usage gauge display.	NA	Not selected.
Active Sessions	This statistic selected for usage gauge display.	NA	Not selected.
Throughput	This statistic selected for usage gauge display.	NA	Not selected.

Usage Gauge LEDs *(Models 3015–3080 only)*	Steady or Intermittent Blue	Blinking Blue
Left to right sequential segments, varying number	Normal operation.	NA
All 10 segments	NA	VPN Concentrator is in a shutdown (halted) state, ready to power off.

VPN Concentrator Rear LEDs

The LEDs on the rear of the VPN 3000 Concentrator are as follows:

LED Indicator	Green	Amber	Off
Private / Public / External Ethernet Interfaces (connected to network)			
Link	Carrier detected. Normal.	NA	No carrier detected. *Error.*
Tx	Transmitting data. Normal. Intermittent on.	NA	Not transmitting data. Idle. Intermittent off.
Coll	NA	Data collisions detected.	No collisions. Normal.
100	Speed set at 100 Mbps.	NA	Speed set at 10 Mbps.

SEP Module LEDs

SEP (Scalable Encryption Processing) module LEDs are present only on models 3015 through 3080 and are visible from the rear of the VPN Concentrator.

SEP Module LED	Green	Amber	Off
Power	Power on. Normal.	NA	Power is not reaching the module. It might not be seated correctly. *Error.*
Status (SEP only)	Encryption code is running. Normal.	SEP module failed during operation. *Error.*	SEP module failed diagnostics or encryption code is not running. *Error.*
Activity (SEP-E only)	Encryption code is running. Normal.	SEP-E module failed during operation. *Error.*	SEP-E module failed diagnostics or encryption code is not running. *Error.*

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

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

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

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

This Limited Warranty is void if failure of the Software has resulted from modification, accident, abuse, or misapplication.

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.

This Agreement is governed by the laws of the State of Massachusetts.

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.

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.

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

COPYRIGHT1.1a (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 FINISHED 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

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

Client SNMP

author tpanton@ibm.net (Tim Panton)

SSH

SSL Plus

TCP Compression / Uncompression

Telnet Server

SID: 1.1

Revision History:
1.197/06/23 21:17:43 root

Regulatory Standards Compliance

Standards Compliance

The VPN 3000 Concentrator complies with the following regulatory standards:

Specification	Description
Regulatory compliance	Products bear CE Marking indicating compliance with (99/5/EEC) directives, which includes the following safety and EMC standards.
Safety	UL 60950 CAN/CSA-C22.2 No. 60950 EN 60950 IEC 60950 TS 001 AS/NZS 3260
EMC	FCC Part 15 (CFR 47) Class A ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI Class A EN55024 ETS300 386-2 EN50082-1 EN61000-3-2 EN61000-3-3
Telecom (E1)	CTR 12/13 ACA TS016
Telecom (T1)	US FCC Part 68 Canadian CS03 JATE Green Book

FCC Part 68 Notice

The equipment complies with Part 68 of the FCC rules. On the tray of this equipment is a label that contains, among other information, the FCC registration number. If requested, this information must be provided to the telephone company.

This equipment cannot be used on telephone company-provided coin services. Connection to the Party Line Service is subject to state tariffs.

If this equipment causes harm to the telephone network, the telephone company notifies you in advance that temporary discontinuance of service might be required. If advance notice is not practical, the telephone company notifies the customer as soon as possible. Also, you are advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company can make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company provides advance notice in order for you to make the necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact us for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company can request you remove the equipment from the network until the problem is resolved.

We recommend that you install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightning strikes and other electrical surges.

This equipment uses the Uniform Service Order Code (USOC) jacks described below.

Model Name	Facility Interface Code	Service Order Code	Jack Type
CVPN_3000-2T	04DU9-1SN	6.0N	RJ48C

CS-03 Certification

The equipment is CS-03 certified. Refer to Table C-1 for CS03 approval details for equipment. Observe the following general information and safety precautions:

The industry Canada label identifies CS-03 certified equipment. This certification means that the equipment meets certain telecommunications network protection, operation, and safety requirements as described in the appropriate terminal equipment requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing the equipment, ensure that it is permissible to connect them to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Warning **Do not attempt to make such connections yourself. Contact the appropriate electric inspection authority or electrician as appropriate.**

Table C-1 CS03 Approval

Model Number	Approval Number
CVPN3005-T1	#2461 10854 A
CVPN3000-2T1	#2461 10854 A

JATE

The equipment meets the requirements of the Japan Approvals Institute for Telecommunications Equipment (JATE). Refer to Table C-2 for JATE approval details.

Table C-2 JATE Approval

Applicant Name	Model Number	Approval Number
Nihon Cisco Systems	CVPN3000-2T1	#D00-0687 JP
Nihon Cisco Systems	CVPN3005-T1	#D00-0687 JP

EMC Environmental Conditions for Product to be Installed in the European Union

This equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under user's control.
- Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
- Where applicable, AC power distribution shall be one of the following types: TN-S and TN-C [as defined in IEC 364-3]

In addition, if equipment is operated in a domestic environment, interference might occur.

(FCC) Class A Warning

"Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense."

[cfr reference 15.21]

For Class A equipment

"NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense."

[cfr reference 15.105]

Canada Class A Warning

This Class 'A' digital apparatus complies with Canadian ICES-003.
Cet appareil numerique de la classe 'A' e_t conforme á la norme NMB-003 de Canada.

(CISPR 22) Class A Warning

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Japan (VCCI) Class A Warning

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Translation:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Taiwan (BSMI) Class A Warning

警告使用者：這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，
在這種情況下，使用者會被要求採取某些適當的對策。

Hungarian Class A Warning

Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Translation:

This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022), the Class A equipment are derived for typical commercial establishments for which special conditions of installation and protection distance are used.

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X

Y