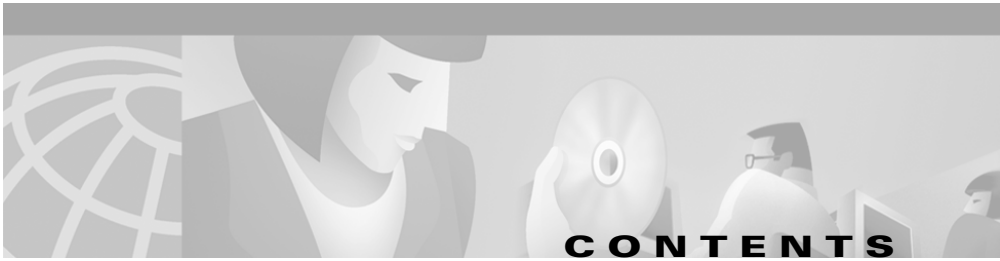
Cisco VPN 5000 Concentrator Software Configuration Guide, Software Version 5.2.x

March 2002

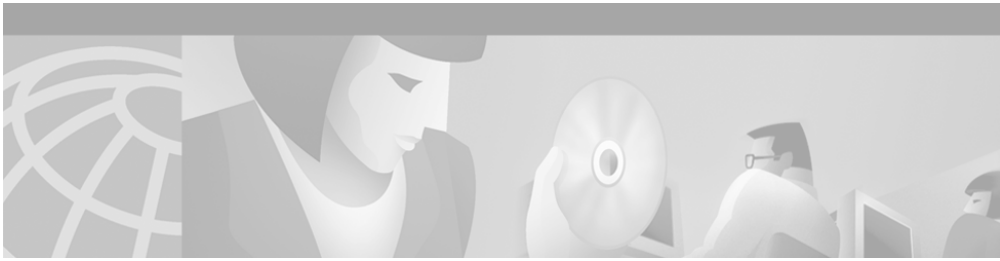
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2087-01

Cisco VPN 5000 Concentrator Software Configuration Guide, Software Version 5.2.x



CONTENTS



About This Guide

This preface defines the objectives, audience, organization, and conventions used in this guide, and gives instructions for obtaining technical assistance and additional information.

Objectives

The purpose of this guide is to help you configure the Cisco VPN 5000 series concentrators for the most common scenarios using the command line interface or by editing a configuration using a text editor. It does not cover every feature, but describes those tasks most commonly required for configuration.

Note This guide only describes IP routing. For IPX and AppleTalk, see the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

Related Documentation

For more information, refer to the following documentation set for Cisco VPN 5000 concentrators:

- *Cisco VPN 5000 Concentrator Series Command Reference Guide*
- *Cisco VPN 5001 Concentrator Hardware Guide*
- *Cisco VPN 5002 Concentrator Hardware Guide*

- *Cisco VPN 5008 Concentrator Hardware Guide*
- *Cisco VPN 5002 and 5008 ESP Card Hardware Guide*
- *Cisco VPN 5001 Concentrator FRU Installation and Replacement Notes*
- *Cisco VPN 5002 Concentrator FRU Installation and Replacement Notes*
- *Cisco VPN 5008 Concentrator FRU Installation and Replacement Notes*
- *Regulatory Compliance and Safety Information for the Cisco VPN 5001 Concentrator*
- *Regulatory Compliance and Safety Information for the Cisco VPN 5002 and 5008 Concentrators*

Audience

This guide is intended primarily for the following audiences:

- Customers with technical networking background and experience
- System administrators who are familiar with the fundamentals of router-based internetworking, but who may not be familiar with VPN 5000 software
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with VPN 5000 software

Organization

This guide contains the following chapters and appendixes:

- Chapter 1, "Introduction," describes the VPN 5000 software features, and tells you how to use the concentrator in your network.
- Chapter 2, "Getting Started," tells you how to set the management port IP address, create a text configuration, or use the command line interface.
- Chapter 3, "Configuring Basic System Parameters," tells you how to set basic system parameters such as the password and concentrator name.
- Chapter 4, "Configuring Basic Interface Settings," tells you how to set Ethernet, HSSI, DS3, and Frame Relay interface settings.

- Chapter 5, “Configuring IP Routing,” tells you how to configure IP routing for each port.
- Chapter 6, “Configuring the IKE Policy for IPSec Tunnel Security,” tells you how to configure VPN tunnel security for IPSec clients and LAN-to-LAN tunnels.
- Chapter 7, “Configuring VPN Groups,” tells you how to create VPN groups for use with the VPN 5000 client.
- Chapter 8, “Authenticating VPN Users,” describes systems you can use to authenticate users for VPN groups.
- Chapter 9, “Configuring VPN LAN-to-LAN Tunnels,” tells you how to create a LAN-to-LAN tunnel between two concentrators.
- Chapter 10, “Installing Certificates on the Concentrator,” tells you how to install root and server certificates on the concentrator for authentication.
- Appendix B, “Installing the Software and Configuration,” tells you how to install or upgrade the VPN 5000 concentrator software, and how to copy the configuration files to or from Flash memory.
- Appendix C, “Recovering from a Software Failure,” tells you how to recover the system from a software failure.
- Appendix A, “Sample Configurations,” includes sample configuration diagrams and text configuration files.
- Appendix E, “Configuring the Firewall for VPN,” tells you how to configure a firewall for VPN traffic.
- Appendix D, “Syntax Conventions,” describes the syntax conventions for the command line interface and the text configuration file.
- Appendix F, “IP Addressing,” describes IP address classes and private addresses, and indicates how to determine the subnet mask.
- The Index provides easy access to topics within the guide.

Document Conventions

The following conventions are used in this guide:

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

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following 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 types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- 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.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

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

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires 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 the following URL to register:

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following 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). In addition, please have available your service agreement number and your product serial number.

Introduction

The Cisco VPN 5000 concentrators provide a network service provider (NSP) or enterprise customer with managed virtual private networks (VPNs) for one or more corporate sites.

The multislot VPN 5002 and 5008 concentrators support up to 5,000 simultaneous VPN connections per Edge Services Processor (ESP) card, allowing you to add capacity as your VPN requirements grow. The VPN 5001 concentrator supports 1500 VPN connections.

Features

Table 1-1 lists the features of the VPN 5000 concentrators.

Table 1-1 Cisco VPN 5000 Features

Feature	Description
Tunneling protocols	• IP Security Protocol (IPSec) • Generic routing encapsulation (GRE)
Link layer protocols	• Frame Relay permanent virtual circuit (PVC) (VPN 5002 or 5008 concentrator WAN ESP cards only) • PPP (VPN 5002 or 5008 concentrator WAN ESP cards only) • Ethernet

Table 1-1 Cisco VPN 5000 Features (continued)

Feature	Description
Key management	Internet Key Exchange (IKE) protocol
Authentication	IPSec Encapsulating Security Payload (ESP) or Authentication Header (AH) using: • Message-digest 5 (MD5) digital signature • Secure Hash Algorithm (SHA)
Encryption	IPSec ESP using Data Encryption Standard (DES) or 3DES
Simultaneous tunnel connections	Combined IPSec client tunnels and LAN-to-LAN tunnels: • VPN 5002 and 5008—5000 per ESP card • VPN 5001—1500 **Note** Each subnet assigned for client IP addresses (**VPN Group** section **LocalIPNet** keyword) uses a connection resource. For example, if you configure 200 VPN groups on a VPN 5008 concentrator with 8 ESP cards, each with one **LocalIPNet**, then the total connection resources available are 39,800 (40,000 minus 200).
Client support	VPN 5000 client
VPN remote access protocols	• IP-in-IP • IPX-in-IP • Microsoft Networking
VPN LAN-to-LAN protocols	• IP-in-IP • IPX-in-IP • AppleTalk-in-IP • Microsoft Networking

Table 1-1 Cisco VPN 5000 Features (continued)

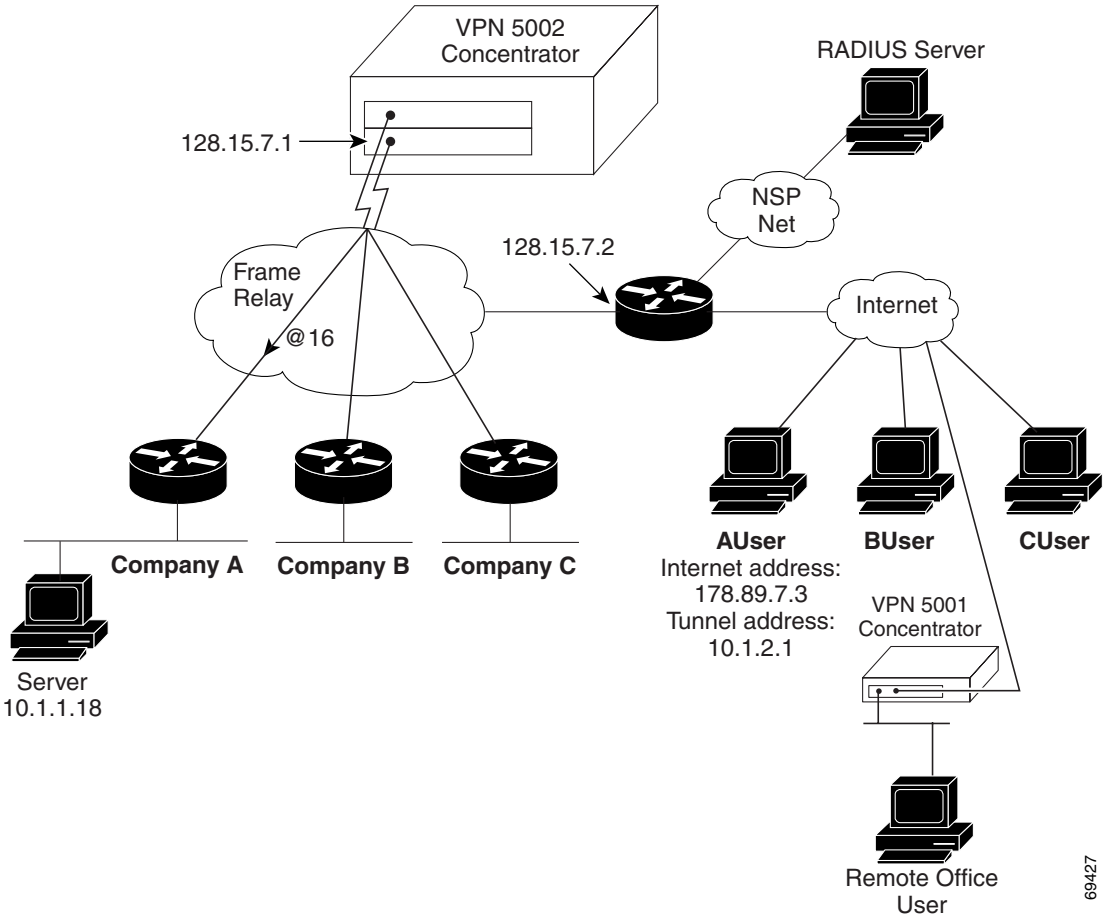
Feature	Description
Client directory support and authentication	• Internal configuration • RADIUS • AXENT Defender with RADIUS component • RSA SecurID • SafeWord with RADIUS in passthrough mode • PKI server-side certificates (also known as hybrid mode) from the following certificate authorities (CAs): – Entrust/PKI with Entrust/VPNConnector – RSA Keon Certificate Server Version 5.5 and earlier
Routing protocols	• RIP • RIP2 • OSPF
Filtering	Full set of IP filters
Management	• Command line over Telnet or console connection • TFTP or XModem for downloading text configuration and software

Using the Concentrator in Your Network

Figure 1-1 shows a VPN 5002 concentrator used by an NSP to provide VPN services for three different companies, Company A, B, and C. All connections to the companies are made through one physical port on an HSSI card.

See Chapter , “Sample Configurations,” for additional network examples.

Figure 1-1 Multiple Companies over Frame Relay



VPN Using the Cisco VPN 5000 Client

The following steps describe how AUser connects to the Company A network:

1. When AUser wants to connect to a server (10.1.1.18) at Company A's site, AUser connects to the local internet service provider (ISP).

2. AUser then uses the VPN 5000 client to connect to the VPN 5002 concentrator's Internet IP address (128.15.7.1), establishing a secure IPSec tunnel.
3. After authenticating the user for Company A's network, AUser sends IP or IPX (Windows users only) packets from its computer to the corporate server through a *tunnel* terminated at the concentrator: the VPN 5000 client encrypts the data and encapsulates it in a routable IPSec packet.
4. The concentrator decrypts, authenticates, and translates the source address in the packets to a tunnel address recognized on Company A's network, in this case, 10.1.2.1.

   This address is used for all traffic sent from Company A to AUser for the duration of the connection.
5. The concentrator forwards the unwrapped, normal IP or IPX packets to Company A through the Frame Relay connection identified by DLCI @16.
6. The concentrator encrypts and encapsulates traffic from Company A back to AUser.

VPN Using a LAN-to-LAN Tunnel

The following steps describe how a large remote office connects to the corporate network using a LAN-to-LAN tunnel between two VPN 5001 concentrators:

1. When a user at the remote office wants to connect to a server (10.1.2.18) on the corporate network, the user simply sends the packet to the server address normally.
2. The VPN 5001 concentrator at the remote office establishes a tunnel with the concentrator at the corporate network.
3. The concentrator then encrypts the data, encapsulates it in a routable IPSec packet, and sends the packet to the corporate VPN 5001 concentrator.
4. The corporate concentrator decrypts and de-encapsulates the packet and forwards it to the server.

Using This Guide

The following sections list the chapters with procedures you need to follow to achieve the following configurations:

- LAN-to-LAN tunnels only
- VPN client tunnels only
- LAN-to-LAN and VPN client tunnels

Note This guide only describes IP routing. For IPX and AppleTalk, see the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

Configuring the Concentrator for LAN-to-LAN Tunnels Only

To configure the concentrator for LAN-to-LAN tunnels only, refer to the following chapters:

1. Chapter 2, "Getting Started," to access the command line interface or create a text configuration.
2. Chapter 3, "Configuring Basic System Parameters," to set the passwords, device name, and time server.
3. Chapter 4, "Configuring Basic Interface Settings," to set port parameters, such as configuring WAN ports for Frame Relay.
4. Chapter 5, "Configuring IP Routing," to configure ports for IP routing.
5. Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security," to set the IKE policy for IPSec tunnels.
6. Chapter 9, "Configuring VPN LAN-to-LAN Tunnels," to configure LAN-to-LAN tunnel partners.
7. (Optional) Chapter 10, "Installing Certificates on the Concentrator," if you use certificates for tunnel authentication.
8. Appendix E, "Configuring the Firewall for VPN," to configure a firewall.

Remember to save your configuration according to the "Saving the Configuration" section on page 2-7.

Configuring the Concentrator for VPN Client Tunnels Only

To configure the concentrator for VPN client tunnels only, refer to the following chapters:

1. Chapter 2, "Getting Started," to access the command line interface or create a text configuration.
2. Chapter 3, "Configuring Basic System Parameters," to set the passwords, device name, and time server.
3. Chapter 4, "Configuring Basic Interface Settings," to set port parameters, such as configuring WAN ports for Frame Relay.
4. Chapter 5, "Configuring IP Routing," to configure ports for IP routing.
5. Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security," to set the IKE policy for IPSec tunnels.
6. Chapter 7, "Configuring VPN Groups," to configure tunneling options for a group of users.
7. Chapter 8, "Authenticating VPN Users," to configure an authentication method, such as a RADIUS server.
8. (Optional) Chapter 10, "Installing Certificates on the Concentrator," if you use server-side certificates as part of your authentication system.
9. Appendix E, "Configuring the Firewall for VPN," to configure a firewall.

Remember to save your configuration according to the "Saving the Configuration" section on page 2-7.

Configuring the Concentrator for LAN-to-LAN and VPN Client Tunnels

To configure the concentrator for LAN-to-LAN and VPN client tunnels, refer to the following chapters:

1. Chapter 2, "Getting Started," to access the command line interface or create a text configuration.
2. Chapter 3, "Configuring Basic System Parameters," to set the passwords, device name, and time server.

3. Chapter 4, “Configuring Basic Interface Settings,” to set port parameters, such as configuring WAN ports for Frame Relay.
4. Chapter 5, “Configuring IP Routing,” to configure ports for IP routing.
5. Chapter 6, “Configuring the IKE Policy for IPSec Tunnel Security,” to set the IKE policy for IPSec tunnels.
6. Chapter 7, “Configuring VPN Groups,” to configure tunneling options for a group of users.
7. Chapter 8, “Authenticating VPN Users,” to configure an authentication method, such as a RADIUS server.
8. Chapter 9, “Configuring VPN LAN-to-LAN Tunnels,” to configure LAN-to-LAN tunnel partners.
9. (Optional) Chapter 10, “Installing Certificates on the Concentrator,” if you use server-side certificates as part of your VPN user authentication system.
10. Appendix E, “Configuring the Firewall for VPN,” to configure a firewall.

Remember to save your configuration according to the “Saving the Configuration” section on page 2-7.

PART 1

Configuring Basic System Parameters

CHAPTER 2

Getting Started

This chapter describes how to set the management port IP address, create a text configuration, or use the command line interface to configure the concentrator.

Note If your concentrator includes Ethernet ports, see the "Configuring VPN-Only Ports" section on page 5-3 to plan your network configuration. The VPN-only feature affects the routing configuration of the concentrator.

Setting the Management IP Address

You can set the management IP address using a directly-connected console or by using Telnet to the default IP address.

Connecting a Console to the Concentrator

Connect a console to the concentrator using one of the following sections.

Connecting Directly to the Console Port

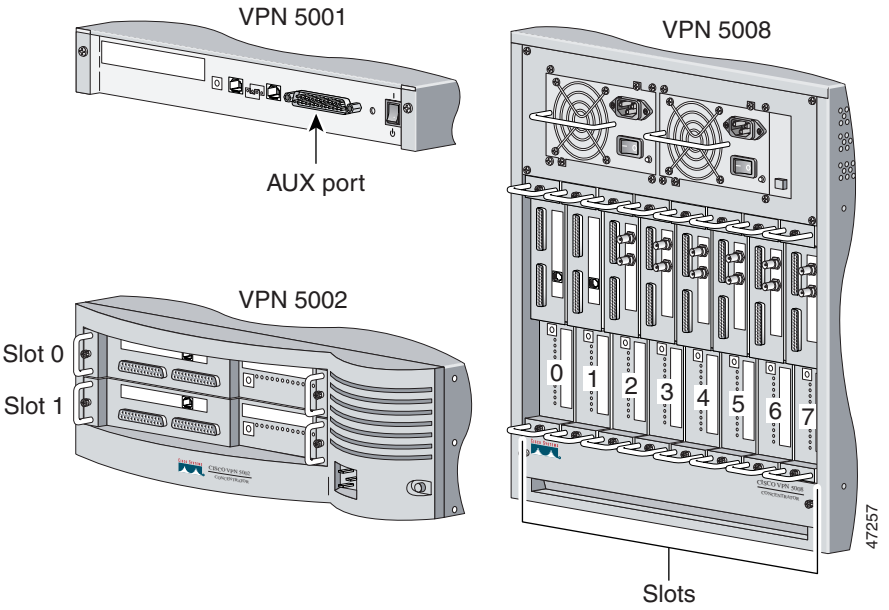
To use the console port to set the IP address, follow these steps:

Step 1 Connect the provided console cable (a standard RS-232 cable) from your terminal or PC to one of the following ports (Figure 2-1):

- VPN 5002 or 5008—Console port on the ESP card in slot 0

  The ESP card in slot 0 controls the entire system.
- VPN 5001—AUX port

Figure 2-1 Slot Numbering



Step 2 Set the terminal emulator to use the following settings:

- 9600 Baud
- 8 bits
- No parity
- 1 stop bit
- No flow control

Step 3 Press the **Return** key one or two times.

Step 4 At the password prompt, enter the default password **`letmein`**.

The command line interface prompt appears.

Using Telnet to the Default IP Address

To use Telnet to set the IP address, follow these steps:

Step 1 Temporarily reconfigure a PC on the same Ethernet segment as the slot 0 Ethernet port (VPN 5002/5008) or Ethernet 0 port (VPN 5001) using the following IP settings:

- IP address: 198.41.12.2
- Subnet mask: 255.255.255.0
- Gateway: 198.41.12.1

If you do not have an Ethernet 0 port, the see "Connecting Directly to the Console Port" section on page 2-1.

Step 2 Telnet to 198.41.12.1.

Step 3 At the password prompt, enter the default normal password **`letmein`**.

The command line interface prompt appears.

Configuring the IP Address

To configure the management IP address, enter the following commands at the prompt.

	Command	Description
Step 1	VPN 5002 or 5008: **configure IP** {**Ethernet** | **WAN**} *slot*:**0** VPN 5001: **configure IP Ethernet** {**0** | **1**}	The *slot* is the ESP card slot.
Step 2	You are prompted for a password. Enter the default: **letmein**	Accesses enabled mode.
Step 3	**IPAddress =** *IP_address*	The port IP address.
Step 4	**SubnetMask =** *subnet_mask*	The port subnet mask.
Step 5	**save**	Writes the configuration changes to Flash memory, and restarts the concentrator. Your Telnet session is disconnected.

Configuration Using a Text Editor

To create a configuration for the concentrator, you can manually edit a text file. You can then download the text file to Flash memory using TFTP or XModem. See the "Copying a Text Configuration File" section on page B-6 for download information. The filename on the concentrator must be:

- VPN 5002 and 5008—vpn5002_8.cfg
- VPN 5001—vpn5001.cfg

The following sections describe the components of a text configuration file.

Sections

The configuration file consists of sections enclosed in brackets with keywords or rules listed underneath. The keyword and its value are separated by an equal sign (*keyword* **=** *value*). Rules consist of a set of arguments.

The section order is only relevant if you have duplicate sections, in which case the first section is used.

For example:

```
[ IP Ethernet 0:0 ]
IPAddress = 10.1.1.1
SubnetAddress = 255.255.255.0

[ IP Filter "ip-in" ]
permit 0.0.0.0 0.0.0.0 tcp dst = smtp
permit 0.0.0.0 0.0.0.0 tcp dst = nntp log
```

Keywords

- Some keywords can occur multiple times in the same section. If you enter multiple instances of a keyword that the software allows only one time, the software uses only the first instance.
- Keywords with Boolean values accept any version (such as On/Off, True/False, 1/0, Yes/No).
- Keywords are not case sensitive.
- Use an equal sign (=) to separate the keyword from its value.
- You can use any amount of space between the equal sign and the keyword and value.

The following keywords all contain valid syntax:

```
keyword1 = value
keyWORD2=value
KEyWorD3       =value
```

Rules

Some sections require rules (a set of arguments) instead of keywords. See the description for each section for syntax conventions.

Text Columns

A section title, keyword, or rule must begin in the line's first column to be parsed correctly. If the section begins in any other column, the system ignores it and includes its keyword values with the previous section. If the keyword begins in any other column, the system ignores it and its value.

```
[ This is one section ]
and

its
data
[ Here is another section ]
and its
data

                                [ This is an invalid section]
its data will be
included with the previous section
```

Comments

Comments and blank lines can occur anywhere in a configuration. If you create your own configuration files, you should document your choices with comments as much as possible to make them easy to edit later.

Comments begin with a pound sign (**#**).

```
#  This is a comment
[ New Section ]        # So is this
```

Configuration Using the Command Line Interface

Only one person at a time can modify a configuration, although up to two users can log in using Telnet while one user can use the console port. The first user to enter a **configure** or **edit config** command can modify the configuration. See Appendix D, "Syntax Conventions," for information about privileges, prompts, and syntax.

Saving the Configuration

After you make changes to the configuration using the commands described in this guide, save your changes by entering the **save** command.

The **save** command writes your changes to Flash memory and restarts the concentrator.

To write your changes without applying or restarting, use the **write** command.

For a complete description of **write** and **save**, see the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

Deleting a Keyword

If you enter a keyword incorrectly during configuration, delete the incorrect keyword and its value by entering the following command at the section prompt:

```
[ section ]# delete keyword
```

If a keyword appears multiple times in a section, the concentrator prompts you to delete or keep each occurrence.

CHAPTER 3

Configuring Basic System Parameters

This chapter describes how to set basic system parameters on the Cisco VPN 5000 concentrator.

Setting the Password and Device Name

The default password is **letmein**. This password provides:

- Normal access—Allows you to use commands to view tables and statistics, but not to make changes to the configuration.
- Enabled access—Allows you to make and save changes to the configuration.

Step 1 To configure the password and device name, create the **General** section using the command line or by editing a text file:

- Command line—Enter the following command:

  ```
  configure General
  ```

- Text file—Create the following header:

  ```
  [ General ]
  ```

Step 2 Enter the following keywords in the **General** section:

Keyword	Description
Password = *string*	**Length:** 8 characters (no spaces allowed) **Default:** letmein Sets the normal password.
EnablePassword = *string*	**Length:** 8 characters (no spaces allowed) **Default:** letmein Sets the enabled password.
DeviceName = "*string*"	**Length:** 32 characters Sets the device name.

See the following sample text configuration:

```
[ General ]
Password = hooray
EnablePassword = eureka
DeviceName = mothership
```

Setting the Time

Many commands require the concentrator to have a valid time and date set. You can set the time either:

- Manually—Each time you reboot or lose power, you must reset the time.
- Using a time server—Automatically supplies the time after a reboot.

Setting the Time Manually

To set the time manually, enter the following command:

sys clock *mm*/*dd*/*yyyy hh*:*mm*

Set this time to Greenwich Mean Time (GMT) if you are using certificates; certificates always use GMT.

Using a Time Server

A time server automatically supplies an accurate time to the system.

Step 1 Create the **Time Server** section using the command line or by editing a text file:

- Command line—Enter the following command:

  ```
  configure Time Server
  ```

- Text file—Create the following header:

  ```
  [ Time Server ]
  ```

Step 2 Enter the following keywords in the **Time Server** section:

Keyword	Purpose
Enabled = On	Uses a time server.
TimeProtocol = {**Timed** | **SNTP**}	Sets the time server protocol. • **Timed** (Default)—Used by UNIX servers • **SNTP**—Used by Windows servers
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**0** | **1**}[.*subinterface*]	Sets the interface that the concentrator uses as a source address for all packets sent to the time server. See Chapter 5, "Configuring IP Routing," to configure and determine which interface to use. This interface must have an IP address.
ServerAddress = *IP_address*	Sets the primary server address.
BackupAddress = *IP_address*	(Optional) Sets the backup server address.
Adjust = [**-**]*number*	Adjusts the time from Greenwich Mean Time (GMT) in minutes. The following values apply for U.S. time zones: PST: -480 MST: -420 CST: -360 EST: -300 **Note** Do not use this keyword if you are using certificates; certificates always use GMT.

See the following sample text configuration:

```
[ Time Server ]
Enabled = On
BindTo = Ethernet 0:0
ServerAddress = 10.1.1.10
```

Setting Logging Options

By default, the system logs configuration, error, and debug information into an internal buffer. If you restart the system, the concentrator clears the buffer. To view the buffer, enter the following command:

```
show system log buffer [n]
```

Where *n* is the number of lines shown, ending with the most recent entries. If you do not specify *n*, the entire log is displayed.

When the buffer is full, the log is overwritten with new data.

By default, the system logs all Notice events and lower.

To configure logging parameters, follow these steps:

Step 1 Create the **Logging** section using the command line or by editing a text file:

- Command line—Enter the following command:

  ```
  configure Logging
  ```

- Text file—Create the following header:

  ```
  [ Logging ]
  ```

Step 2 To perform an action in the following table, enter the corresponding keywords in the **Logging** section:

Action	Keyword	Description
Change the logging level.	**level =** {*n* (0-7) | **emergency** | **alert** | **critical** | **error** | **warning** | **notice** | **info** | **debug**}	The *n* option corresponds to the level. For example, **1** is the same as **alert**. The log includes all events at the specified level and below; for example, **4** includes levels 0 through 4. See Table 3-1 for level descriptions.
Send log messages to the console port.	**LogToAuxPort = On**	You can view log messages in real time on your console. **Note** To toggle the console messages on and off, press **Ctrl-Z** at the console. This command affects only the run-time version. At startup, the concentrator uses the value you set here.

Action	Keyword	Description
Send log messages to a syslog daemon on another host in your network.	**LogToSysLog = On**	A syslog daemon is a UNIX application that handles requests across the network.
	SyslogFacility = **Local0** | **Local1** | **Local2** | **Local3** | **Local4** | **Local5** | **Local6** | **Local7**}	The syslog facility to which the system sends remote log messages.
	SyslogIPAddress = *IP_Address*	The IP address of the remote syslog daemon.
Disable logging for certain ports.	VPN 5002 or 5008: **DisabledPorts =** {**Ethernet** | **WAN**} *slot*:**0** [{**Ethernet** | **WAN**} *slot*:**0**] [...] VPN 5001: **DisabledPorts =** **Ethernet** {**0** | **1**}	The *slot* is the ESP card slot.

See the following sample text configuration:

```
[ Logging ]
Level = Debug
LogToAuxPort = On
```

Logging Levels

The concentrator labels log messages with one of the categories described in Table 3-1.

Table 3-1 Logging Levels

Level Name	Level Number	Description
Emergency	0	You receive logging information only when the system is unusable. These log messages help indicate the source of a problem.
Alert	1	Requires immediate attention.
Critical	2	Indicates a serious problem.
Error	3	Reports exception cases pertaining to violations of protocols or other operational rules. Violations might include illegal packets and improper command syntax.
Warning	4	Reports problems that might need a response. Examples include network number conflicts and resource allocation problems. If Warning messages are repeated, they require a response.
Notice	5	Reports information that might be useful on a day-to-day basis by an administrator but generally does not require any response. Examples include login/logout and LAN-to-LAN connections.
Info	6	Reports routine information such as WAN network connect and disconnect messages.
Debug	7	Reports each action of the device and is the best setting for troubleshooting.

CHAPTER 4

Configuring Basic Interface Settings

This chapter describes how to configure physical interface settings. These settings are carried over to any subinterfaces.

Note The sections described in this chapter require the interface slot or port. See the following list for a description of the slot and port numbering:

- VPN 5001 (facing the back panel)—Port 1 is the left port, and port 0 is the right port.
- VPN 5002—Slot 0 is the top slot. Each card has a single port that is numbered 0.
- VPN 5008—Slot 0 is the far left slot. Each card has a single port that is numbered 0.

Configuring the Ethernet Interface

The Ethernet interface automatically senses 10BaseT or 100BaseT, and full or half duplex if you cabled the Ethernet port at startup. Otherwise, the port defaults to 10BaseT and half duplex. If the autosensing is not working, follow these steps:

Step 1 Create the **Ethernet Interface** section using the command line or by editing a text file:

- Command line—Enter the following command:

  - For the VPN 5002 and 5008:

    configure Ethernet Interface Ethernet *slot*:**0**

  - For the VPN 5001:

    configure Ethernet Interface Ethernet {**0** | **1**}

- Text file—Create the following header:
  - For the VPN 5002 and 5008:

    [Ethernet Interface Ethernet *slot*:**0]**

  - For the VPN 5001:

    [Ethernet Interface Ethernet {**0** | **1**} **]**

Step 2 Enter the following keywords in the **Ethernet Interface** section:

Keyword	Description
Speed = {**10meg** | **100meg** | **Auto**}	Sets the protocol to 10BaseT or 100BaseT. Set the value required by your switch or hub.
Duplex = {**Full** | **Half** | **Auto**}	Sets the duplex mode to full or half duplex. Set the value required by your switch or hub.

See the following sample text configuration:

```
[ Ethernet Interface Ethernet 1:0 ]
Speed = 100meg
Duplex = Full
```

Configuring the HSSI Interface

The HSSI interface on the VPN 5002 or 5008 concentrator, which is a Data Terminal Equipment (DTE), uses the following default settings:

- 16-bit cyclic redundancy check (CRC)
- External clock

To change these settings, follow these steps:

Step 1 Create the **HSSI Interface** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure HSSI Interface WAN *slot*:**0**

- Text file—Create the following header:

  [HSSI Interface WAN *slot*:**0]**

Step 2 Enter the following keywords in the **HSSI Interface** section:

Keyword	Description
CRC = {**32bit** | **16bit**}	Sets the CRC. Both ends of the connection need to use the same CRC setting.
Clocking = {**Internal** | **External**}	Sets the clock. Use an external clock to connect to a DCE, such as a CSU/DSU. Use an internal clock to connect to another DTE HSSI port (with an external clock) back-to-back.

See the following sample text configuration:

```
[ HSSI Interface WAN 1:0 ]
CRC = 32bit
```

Configuring the DS3 Interface

The DS3 interface on the VPN 5002 or 5008 concentrator uses the following defaults:

- 16-bit CRC
- 0 to 100-foot cable
- Noninverted data
- Internal clock
- 44,210 Kbps data rate

To change these settings, follow these steps:

Step 1 Create the **DS3 Interface** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure DS3 Interface WAN *slot*:**0**

- Text file—Create the following header:

  [DS3 Interface WAN *slot*:**0]**

Step 2 Enter the following keywords in the **DS3 Interface** section:

Keyword	Description
CRC = {**32bit** | **16bit**}	Sets the CRC. Both ends of the connection need to use the same CRC setting.
Clocking = {**External** | **Internal**}	Sets the clock. Set the clock to **External** if the DS3 port receives its clock from the DS3 signal. Check with your service provider for this setting.
LBO = {**Long** | **Short**}	Changes the cable length. • **Long**—Sets the cable length to 101 to 900 feet. • **Short** (Default)—Sets the cable length to 0 to 100 feet.
InvertData = {**On** | **Off**}	Sets the data inversion. You can use data inversion to meet pulse density requirements. Only set it to **On** if instructed by your service provider. If a DSU at one end of a DS3 line inverts its data, then the DSU at the other end must do the same.
DS3SubRate = {**3_158** | **6_316** | **9_474** | **12_632** | **15_790** | **18_948** | **22_106** | **25_264** | **28_422** | **31_580** | **34_738** | **37_896** | **41_054** | **44_210**}	Changes the data rate. Unless the remote end is a Larscom CSU/DSU (or equivalent) or another VPN 5002 or 5008 DS3 interface, you must use the default **44_210** Kbps.

See the following sample text configuration:

```
[ DS3 Interface WAN 1:0 ]
CRC = 32bit
LBO = Long
```

Setting the Link Type to Frame Relay

By default, the WAN link is disabled. To set the link type to Frame Relay, follow the steps in this section. For information about PPP, the other option for the link, see the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

If you need to change the Frame Relay defaults on the VPN 5002 or 5008 concentrator, such as the AnnexD maintenance protocol, configure the **Frame Relay** section. See the *Cisco VPN 5000 Concentrator Series Command Reference Guide* for more information.

Step 1 Create the **Link Config** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure Link Config WAN *slot*:**0**

- Text file—Create the following header:

  [Link Config WAN *slot*:**0]**

Step 2 Enter the following keyword in the **Link Config** section:

Keyword	Description
Mode = FrameRelay	Sets the low-level communications protocol to Frame Relay.

See the following sample text configuration:

```
[ Link Config 1:0 ]
Mode = Frame Relay
```

Cisco Systems

PART 2

Configuring IP Routing and VPN Parameters

CHAPTER 5

Configuring IP Routing

This chapter describes how to configure IP routing for each interface on the Cisco VPN 5000 concentrator.

Interface Overview

The following sections describe the types of interfaces for which you can configure IP routing: primary interfaces, subinterfaces, and loopback subinterfaces.

See the "Configuring IP Routing Over a the Tunnel" section on page 9-14 to configure IP routing for LAN-to-LAN tunnels.

Using Primary Interfaces

The primary interface for a VPN 5002 or 5008 concentrator is represented by the type (Ethernet or WAN) followed by *slot*:*port*, where *port* is always 0 (the VPN 5000 concentrators currently only have cards with one port each, and port numbering begins at 0). For the VPN 5001 concentrator, the type is Ethernet, and the port is 0 or 1.

To configure a subinterface, you must also configure the primary interface.

Using Subinterfaces

Subinterfaces allow you to connect separate subnets to the same physical port, allowing you to keep networks separate while they use the same port.

Subinterface Syntax

To configure the **IP** section for a subinterface, use the following syntax to enter the subinterface number after the slot and port:

- VPN 5002 and 5008:

  IP {**Ethernet** | **WAN**} *slot*:**0.***subinterface*

- VPN 5001:

  IP Ethernet {**0** | **1**}.*subinterface*

For example:

```
IP WAN 1:0.1
```

Subinterface Guidelines

See the following guidelines for subinterfaces:

- You can use a maximum of 255 subinterfaces per interface, 1 to 255. 0 is reserved for the primary interface.
- You can use subinterfaces only for Frame Relay and Ethernet connections.
- To use a subinterface, you must also configure IP routing for the primary interface. You must also list the primary interface in the configuration before any subinterfaces.
- You cannot add a subinterface to a VPN-only port.

Using a Loopback Subinterface

Some configurations require a *loopback* address that is internal to the concentrator. To create a loopback address, configure a subinterface on any port and assign it an IP address that is on a unique subnet and therefore not directly connected to any other device.

Do not configure routing protocols (RIP or OSPF) for the loopback subinterface; the address can be advertised by other interfaces. To advertise a loopback address using RIP or OSPF, use at least a /30 (255.255.255.252) subnet mask, which consumes four IP addresses. A /32 (255.255.255.255) subnet mask, while using only one IP address, is not advertised.

Note You cannot assign the first or last address in the subnet. See the "Subnet Masks" section on page F-2 for more information about masking.

- For Ethernet loopback subinterfaces, complete the steps in the:
  - "Creating the IP Section" section on page 5-6
  - "Enabling Routing" section on page 5-7
  - "Setting the IP Address" section on page 5-10.
- For WAN loopback subinterfaces, complete the steps in the:
  - "Creating the IP Section" section on page 5-6
  - "Enabling Routing" section on page 5-7
  - "Configuring Frame Relay" section on page 5-8,
  - "Setting the IP Address" section on page 5-10.

Configuring VPN-Only Ports

The following sections describe the VPN-only feature for IP interfaces and how to set a VPN gateway to send traffic out a VPN-only port.

The primary interfaces of odd-numbered Ethernet ports or slots (1, 3, 5, and 7) are VPN-only ports. You cannot create subinterfaces on these ports.

To configure a VPN-only port, set the VPN gateway and the IP address. You do not need to configure routing protocols, which are not supported on the VPN-only port.

VPN-Only Overview

A VPN-only port can accept and send only VPN traffic. VPN traffic consists of IPSec packets. VPN traffic does not include normal IP traffic, such as routing updates or GRE packets. Because the port accepts only VPN traffic, you can safely locate the port in parallel with your firewall, and connect the port directly to the Internet gateway router.

VPN-Only Port Guidelines

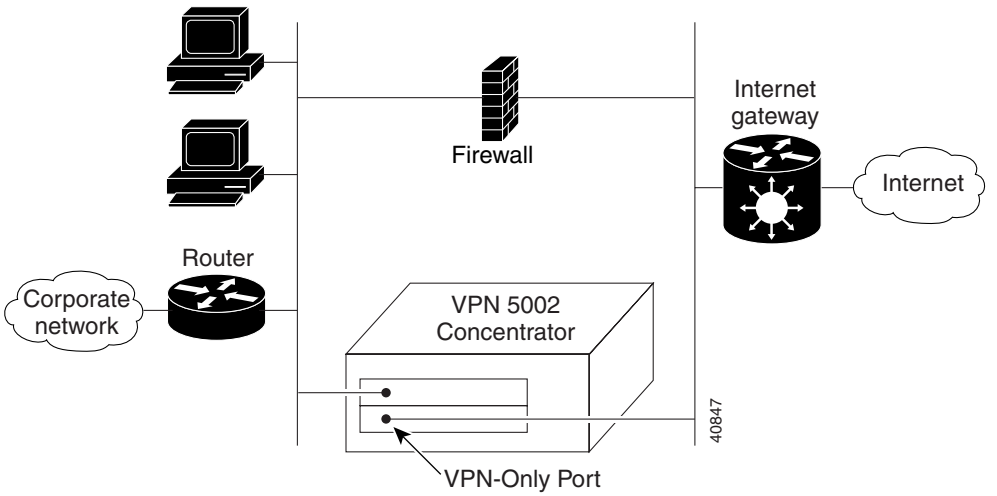
See the following guidelines for VPN-only ports:

- The VPN-only port does not send or accept GRE traffic.
- The VPN-only port only accepts traffic destined for its port address; traffic destined for another address, even if it is another concentrator port, is rejected.
- VPN filtering only occurs if the packets enter the concentrator on the VPN-only port. For example, if packets are destined for the VPN-only port Ethernet 1:0, but the traffic entered the concentrator on Ethernet 0:0, then no filtering occurs.
- The VPN-only port can respond to certain ICMP requests, such as ping and traceroute. To respond to the request, you must configure a static route to send non-VPN ICMP traffic through the VPN-only port. You can specify the host or network from which ICMP requests originate, or you can set a default route.
- You should specify a VPN gateway (as described in the "Identifying a VPN Gateway for a VPN-Only Port" section on page 5-5) that directs all VPN traffic to a directly connected router. If you do not set a VPN gateway for a VPN-only port, you must set static routes.

Using a VPN-Only Port in Your Network

Figure 5-1 shows a VPN 5002 concentrator with a VPN-only port in parallel with the firewall, and a regular port behind the firewall.

Figure 5-1 Using a VPN-Only Port in a Network



Identifying a VPN Gateway for a VPN-Only Port

Because a VPN-only port does not support routing protocols, you must identify a route (the **General** section **VPNGateway** keyword) for VPN traffic to exit the VPN-only port. The concentrator allows you to set a VPN gateway that sends all VPN traffic to an upstream router connected to the VPN-only port. If you do not set a VPN gateway, you must set static routes.

Benefit of a VPN Gateway Over a Static Route

The benefit of a VPN gateway over a static route is:

- The VPN gateway sends all VPN traffic out the VPN-only port regardless of its final destination (which would require many static routes)
- The VPN gateway does not send non-VPN traffic to the VPN-only port, which is not allowed. Static routes send all traffic to the VPN-only port, which causes non-VPN traffic to be dropped.

Configuring a VPN Gateway

To identify the VPN gateway, follow these steps:

Step 1 Access the **General** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure General

- Text file—Create the following header:

  [General]

Step 2 Enter the following keyword in the **General** section:

Keyword	Purpose
VPNGateway = *IP_Address*	*IP_Address* is the upstream router address to which you want all VPN traffic sent.

See the following text configuration with keywords described in this chapter so far:

```
[ General ]
VPNGateway = 10.1.1.1
```

Creating the IP Section

This chapter includes keywords to enter in the **IP** section, unless indicated otherwise. To create the **IP** section, use one of the following methods:

- Command line—Enter the following command:
  - For the VPN 5002 and 5008:

    configure IP {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*]

  - For the VPN 5001:

```
configure IP Ethernet {0 | 1}[.subinterface]
```

- Text file—Create the following header:
  - For the VPN 5002 and 5008:

    ```
    [ IP {Ethernet | WAN} slot:0[.subinterface] ]
    ```

  - For the VPN 5001:

    ```
    [ IP Ethernet {0 | 1}[.subinterface] ]
    ```

Note The **IP** section and some keywords require the interface slot or port. See the following list for a description of the slot and port numbering:

- VPN 5001 (facing the back panel)—Port 1 is the left port, and port 0 is the right port.
- VPN 5002—Slot 0 is the top slot. Each card has a single port that is numbered 0.
- VPN 5008—Slot 0 is the far left slot. Each card has a single port that is numbered 0.

Enabling Routing

To turn on IP routing for an interface or subinterface, enter the following keyword in the **IP** section:

Keyword	Purpose
`Mode = Routed`	Turns on routing.

See the following text configuration with keywords described in this chapter so far:

```
[ IP Ethernet 1:0 ]
Mode = Routed
```

Configuring Frame Relay

You can choose multipoint or point-to-point Frame Relay for the primary interface or for any subinterfaces.

- Point-to-point interfaces allow you to save IP addresses because they can be unnumbered, but you can connect the interface to only one PVC.
- Multipoint interfaces allow you to connect the same interface to multiple PVCs.
- For multipoint subinterfaces, you must enter the **Frame Relay** section **DLCI** keyword for each DLCI. The **DLCI** keyword maps the local DLCI to the remote IP address.
- You can use a mix of multipoint and point-to-point interfaces.

The following sections describe how to configure point-to-point and multipoint interfaces.

Configuring a Point-to-Point Frame Relay Interface

To configure a point-to-point link, enter the following keywords in the **IP** section for your interface. Be sure that the device at the other end of the PVC supports point-to-point Frame Relay.

Keyword	Purpose
`Numbered = {Off | On}`	Specifies whether or not the concentrator assigns an IP address to the interface. If **Numbered = On**, set the IP address according to the "Setting the IP Address" section on page 5-10. Be sure to set an IP address on the same subnet on the remote device.

Keyword	Purpose
PointToPointFrame = On	Specifies that the Frame Relay link is point-to-point.
InterfaceDLCI = *Number*	The local interface DLCI assigned by your Frame Relay provider. The DLCI can be a number between 16 and 991.

See the following text configuration with keywords described in this chapter so far:

```
[ IP WAN 1:0 ]
Mode = Routed
Numbered = On
PointToPointFrame = On
InterfaceDLCI = 21
```

Configuring a Multipoint Frame Relay Interface

To configure a multipoint interface, complete the following steps.

Note This interface must be assigned an IP address.

Step 1 For subinterfaces (or for the primary interface if the Frame Relay network does not support inverse ARP (IARP)), map the local DLCIs to remote IP addresses.

a. Create the **Frame Relay** section for the primary interface:

- Command line—Enter the following command:

  configure Frame Relay WAN *slot*:**0**

- Text file—Create the following header:

  [Frame Relay WAN *slot*:**0]**

b. Map the DLCI to a remote IP address. Enter this keyword for each PVC you want to map, including the PVCs for subinterfaces.

DLCI = *DLCI_Number* **IP=***IP_Address*

- *DLCI_Number*—The local DLCI.
- *IP_Address*—The router address at the other end of the PVC.

For example, to map WAN 0:0 (DLCI 17), WAN 0:0.1 (DLCI 18), and WAN 0:0.2 (DLCI 19), enter:

```
DLCI = 17 IP=10.1.1.1
DLCI = 18 IP=10.1.2.1
DLCI = 19 IP=10.1.3.1
```

See the following sample text configuration:

```
[ Frame Relay WAN 1:0 ]
DLCI = 17 IP=10.1.1.1
DLCI = 18 IP=10.1.2.1
DLCI = 19 IP=10.1.3.1
```

Setting the IP Address

To set an IP address, enter the following commands in the **IP** section for your interface:

Keyword	Purpose
IPAddress = *IP_Address*	The interface IP address.
SubnetMask = *subnet_mask*	The interface subnet mask.

See the following text configuration with keywords described in this chapter so far:

```
[ IP Ethernet 1:0 ]
Mode = Routed
IPAddress = 10.1.1.1
SubnetMask = 255.255.255.0
```

Configuring the Dynamic Routing Protocol

IP routing protocols create and update routing tables that tell routers where to send a particular packet.

For the VPN 5000 concentrator, a dynamic routing protocol provides the following services:

- Informs routers about the VPN client networks identified by the **LocalIPNet** in the **VPN Group** section.

  If you use the **StartIPAddress** keyword, you do not need routing protocols because the clients appear to be on the directly connected network. See Chapter 7, "Configuring VPN Groups," for more information.

- Informs the concentrator about networks on the other end of a proprietary IPSec or GRE LAN-to-LAN tunnel, and advertises local networks to the other end of the tunnel.
- Informs the concentrator where to send incoming packets (for example, from the VPN client networks).

You can specify the following protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF) protocol

If the concentrator does not receive a default route from a routing protocol, you might need to set a static default route. If you do not use a routing protocol at all, configure static routes. See the "Configuring the Default Route or Static Routes" section on page 5-13.

For a VPN-only port (see the "Configuring VPN-Only Ports" section on page 5-3), do not specify a protocol because the port cannot send or accept routing protocol packets.

Using RIP

Gateways and routers that support RIP send routing-update messages at regular intervals, and when the network topology changes. These RIP packets contain information about the networks that the routers and gateways can reach, as well

as the number of routers or gateways that a packet must travel through to reach the destination address. RIP generates more traffic than OSPF, but is easier to configure initially.

To configure RIP, enter the following keyword in the **IP** section for your interface:

Keyword	Purpose
RIPVersion = {V1 | V2 | None}	• **V1**—Broadcasts and accepts RIP packets and periodically updates its routing table with the information provided from these packets. • **V2**—An enhancement of RIP V1 that allows IP subnet information to be shared among routers, and provides for authentication of routing updates. The router uses the multicast address 224.0.0.9 to send and receive RIP V2 packets for this network interface. • **None** (Default)—Disables RIP. Use RIP V2 unless a neighboring router uses V1, in which case all routers should use V1.

See the following text configuration with keywords described in this chapter so far:

```
[ IP Ethernet 1:0 ]
Mode = Routed
IPAddress = 10.1.1.1
SubnetMask = 255.255.255.0
RIPVersion = V2
```

To learn more about these and other settings, see the **IP** section in the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

Using OSPF

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each router's usable interfaces and reachable neighbors.

The advantage of OSPF over RIP is that:

- OSPF link-state database updates are sent less frequently than RIP updates, and the link-state database is updated instantly rather than gradually as stale information is timed out.
- Routing decisions are based on *cost*, which is an indication of the overhead required to send packets across a certain interface. The concentrator calculates the cost of an interface based on link bandwidth rather than the number of hops to the destination. The cost can be configured to specify preferred paths.

The disadvantage of shortest path first algorithms is that they require a lot of CPU cycles and memory.

Configuring OSPF

To enable and configure OSPF, see the **IP** section and the **OSPF Area** section in the *Cisco VPN 5000 Concentrator Series Command Reference Guide*. See the **OSPF Virtual Link** section to configure a virtual link, which is the only way to allow an area that is not contiguous to the backbone area (area 0) to operate.

Configuring the Default Route or Static Routes

This section describes a default route and static routes.

Using a Default Route

If the concentrator does not receive a default route from a routing protocol, you might need to set a static default route. The default route identifies the router IP address to which the concentrator sends all IP packets for which it does not have a route. While the concentrator can reach any directly connected networks, it might not be able to reach other networks several router hops away, in which case it sends the packets to the default gateway identified by the default route.

Using Static Routes

If you do not use a dynamic routing protocol to learn and propagate routes, use static routes. You might want to use static routes if:

- Your network uses a different router discovery protocol from RIP or OSPF.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.

On the concentrator, you need to identify routes for:

- All networks the concentrator needs to reach; for example, all networks that VPN clients need to reach.
- If you are using a **LocalIPNet** in the **VPN Group** section, you also need to set up static routes on neighboring routers to inform them of the path to the VPN client networks.

  If you use the **StartIPAddress** keyword, you do not need static routes on neighboring routers because the clients appear to be on the directly connected network. See Chapter 7, "Configuring VPN Groups," for more information.

The simplest option is to configure a default route to send all traffic to an upstream router, relying on the router to route the traffic for you. However, this approach is not as efficient as using explicit static routes.

Configuring the Default Route or Static Route

To configure a default route or static route, follow these steps:

Step 1 Access the **IP Static** section using the command line or by editing a text file:

- Command line—Enter the following commands:

```
edit config IP Static
append $
```

  The prompt changes to `Append#`.

- Text file—Create the following header:

```
[ IP Static ]
```

Step 2 (Optional) Add a comment by starting the line with a pound sign (#).

If you are using the command line, press the **Enter** key at the end of the comment to go to a new line.

Step 3 Enter a default route or a static route.

- For a default route for all traffic, enter:

  0.0.0.0 0.0.0.0 {*Gateway* | *Port*} *Metric*

  The destination and mask of 0.0.0.0 are wild cards that indicate that any packet that is not routed according to the routing table is sent to the *Gateway* address or through the specified *Port*.

- For a static route for a specific network, enter:

  Destination Mask {*Gateway* | *Port*} *Metric* [**Redist=**{**RIP** | **OSPF1** | **OSPF2** | **none**}]

Table 5-1 describes the static route options.

Table 5-1 Static Route Options

Option	Description
Destination	IP address for the destination network in dotted decimal notation.
Mask	Subnet mask for the *Destination* address in dotted decimal notation.
Gateway	IP address of the upstream router responsible for this network.
Port	Port name for a VPN LAN-to-LAN connection or for an unnumbered Frame Relay link where you do not need to specify the other end's IP address: {**VPN** *VPN_port_number* | **WAN** *slot*:**0**[**.***subinterface*]}

Table 5-1 Static Route Options (continued)

Option	Description
Metric	A value between 1 and 15 (1 is recommended) that specifies the distance or cost to the destination address. A route with a lower metric supersedes a competing route (for example, one learned through a routing protocol). The metric loosely corresponds with the number of hops to the destination. You can artificially inflate or deflate the cost for a route. For example, if there is more than one route to a destination, but the route with the shortest number of hops is over a slow WAN link, you can add a non-WAN route with a deflated metric to supersede the slow WAN route.
Redist	Indicates whether this static route should be redistributed using a routing protocol, enabling other routers to use the concentrator as the gateway for packets with the static route's destination address. Do not redistribute a default gateway. Do not enter spaces around the equal sign in **Redist=***value*. • **RIP**—Redistributes the static route entry using RIP V1 or V2. • **OSPF1**—Redistributes the static route entry using OSPF, using a metric that is the sum of both the external cost and the internal cost used to reach the gateway. • **OSPF2**—Redistributes the static route entry using OSPF, using a metric that is the external cost used to reach the gateway. • **none** (Default)—Does not redistribute the route.

For example, the following route sends all traffic destined for the 167.56.7.0 network to the router IP address 189.5.6.1:

```
167.56.7.0 255.255.255.0 189.5.6.1 1 Redist=RIP
```

Step 4 If you are using the command line, follow these steps:

a. To enter additional routes, press the **Enter** key to go to a new line.

b. After entering the last route, press the **Enter** key to go to a new line, enter a period (**.**) and press **Enter**.

c. Enter the following command to exit the editor and keep your changes:

exit

Enter **quit** to exit the editor without making any changes.

See the following sample text configuration:

```
[ IP Static ]
167.56.7.0 255.255.255.0 189.5.6.1 1 Redist=RIP
# default route:
0.0.0.0 0.0.0.0 10.3.2.1 1
```

Identifying a Domain Name System Server

In IP routing, a Domain Name System (DNS) server resolves names to IP addresses. The DNS server allows the concentrator to use domain names instead of IP addresses for RADIUS servers, SecurID servers, or for hosts to ping or Telnet to. To identify a DNS server for a VPN group's remote users, see Chapter 7, "Configuring VPN Groups."

To identify the DNS server, follow these steps:

Step 1 Create the **Domain Name Server** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure Domain Name Server

- Text file—Create the following header:

  [Domain Name Server]

Step 2 Enter the following keywords in the **Domain Name Server** section:

Keyword	Purpose
PrimaryServer = *IP_address*	Sets the primary DNS server IP address.
SecondaryServer = *IP_address*	(Optional) Specifies a secondary DNS server if the primary is unavailable. You can enter up to two secondary servers as separate keywords.

See the following sample text configuration:

```
[ Domain Name Server ]
PrimaryServer = 10.10.10.23
SecondaryServer = 10.10.8.2
SecondaryServer = 10.10.9.9
```

CHAPTER 6

Configuring the IKE Policy for IPSec Tunnel Security

This chapter describes how to configure the Internet Key Exchange (IKE) policy for IPSec tunnels. These security parameters are global to the concentrator and are not associated with a particular interface.

IKE Overview

IKE ensures the authenticated exchange of secure keys to allow the negotiation of IPSec tunnels over an insecure Internet connection. An IKE session between two peers consists of an encryption algorithm, an authentication algorithm, and a key-exchange method (a protection suite). The IKE initiator proposes one or more protection suites, and if the responder accepts one of these proposals, IKE Phase 1 negotiation proceeds.

IKE consists of two phases:

- Phase 1 sets up an authenticated secure connection that can be used for Phase 2 negotiations.

  This connection is identified by an IKE security association (SA).

  Phase 1 consists of four main tasks:

  - Identify the peers.
  - Authenticate the peers to each other.
  - Negotiate Phase 2 parameters: encryption, authentication, and key-exchange method.

  - Exchange keys and tie the keys to the peers.

  An IKE SA can support many Phase 2 negotiations.

- Phase 2 negotiates the IPSec SAs.

To set Phase 2 negotiation parameters, see the "Configuring a VPN Group for the VPN 5000 Client" section on page 7-2 or Chapter 9, "Configuring VPN LAN-to-LAN Tunnels."

Setting the IKE Policy

To configure tunnel authentication, follow these steps:

Step 1 Access the **IKE Policy** section using the command line or by editing a text file:

- Command line—Enter the following command:

  ```
  configure IKE Policy
  ```

- Text file—Create the following header:

  ```
  [ IKE Policy ]
  ```

Step 2 Enter the following keyword in the **IKE Policy** section:

Keyword	Purpose
`Protection = {MD5_DES_G1 | MD5_3DES_G1 | MD5_DES_G2 | MD5_3DES_G2 | SHA_DES_G1 | SHA_3DES_G1 | SHA_DES_G2 | SHA_3DES_G2}`	**Multi-keyword:** You can enter this command multiple times within this section, in which case the concentrator proposes each of the specified protection suites in order until the tunnel peer accepts the options for the negotiation. Specifies the protection suite for the IKE negotiation. The authentication and encryption algorithms of this protection typically match the Phase 2 transform for VPN groups and LAN-to-LAN tunnels. You might use multiple protection suites if you have a mix of client versions (for example, Windows and Macintosh) or LAN-to-LAN tunnel partners. If offering multiple protections, you usually do not offer DES and 3DES, because the added security of 3DES is only secure if it is required of all logins. The first piece of each option is the authentication algorithm to be used for the negotiation: • **MD5**—Message-digest 5 hash algorithm. • **SHA**—Secure Hash Algorithm, which is considered to be more secure than MD5. The second piece is the encryption algorithm: • **DES** (Data Encryption Standard)—Uses a 56-bit key to scramble the data. • **3DES** (Triple DES)—Uses three different keys and three applications of the DES algorithm to scramble the data. 3DES is subject to restrictions by U.S. encryption export laws, and might not be available in concentrators or clients shipped outside the United States. The third piece is the Diffie-Hellman group to be used for key exchange: • **G1** (Group 1)—Uses a 768-bit algorithm. • **G2** (Group 2)—Uses a 1024-bit algorithm and is more secure than Group 1. **Note** VPN 5000 clients that do not use certificates for authentication only support the G1 key exchange.

See the following sample text configuration:

```
[ IKE Policy ]
Transform = SHA_3DES_G2
```

CHAPTER 7

Configuring VPN Groups

This chapter describes how to configure VPN groups for VPN 5000 clients.

A VPN group comprises a set of parameters applied to related VPN users when they connect to the Cisco VPN 5000 concentrator. Parameters include the IP addresses assigned to the clients, the networks a client can reach, and the security level for tunnels.

For LAN-to-LAN tunnels between concentrators, see Chapter 9, "Configuring VPN LAN-to-LAN Tunnels."

VPN Group Guidelines

To configure VPN groups, see the following guidelines:

- You can create up to 1,000 VPN groups per VPN 5002 or 5008 concentrator, or 100 groups per VPN 5001 concentrator.
- Each group name must be unique on the concentrator.
- You must also set the initial tunnel security parameters in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security."
- Before you create the VPN group, plan your user authentication method by referring to Chapter 8, "Authenticating VPN Users."

Configuring a VPN Group for the VPN 5000 Client

To create a VPN group, follow these steps:

Step 1 To configure the VPN group, create the **VPN Group** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure VPN Group "*Name***"**

  Where *Name* is up to 15 characters in length and unique on the concentrator.

- Text file—Create the following header:

  [VPN Group "*Name***"]**

  Where *Name* is up to 15 characters in length and unique on the concentrator.

Step 2 Enter the following keywords in the **VPN Group** section:

Keyword	Description
MaxConnections = *Number*	The maximum number of client connections for this VPN group. If you do not specify a number, connections are allowed on a first-come, first-serve basis until the maximum connections for the concentrator is reached. If you use **LocalIPNet** with fewer addresses than the maximum connections you set here, the **LocalIPNet** */bits* mask determines the maximum connections. For example, a /24 mask makes the **MaxConnections** 254 by default. See the "Subnet Masks" section on page F-2 for a list of masks and number of hosts.
IPNet = *IP_Address*/*bits*	**Default:** 0.0.0.0/0 (tunnels all traffic) **Multi-keyword:** Enter this keyword up to 64 times to allow access to multiple networks. The network that remote clients can reach through the tunnel; the client tunnels any traffic destined for this network. To allow access to a single host, specify the *bits* as 32. See the "Subnet Masks" section on page F-2 for a description of */bits*. **Note** If the networks a client needs to reach change frequently (through addition of new networks, for example), you can enter a single entry for this keyword that supernets the existing networks and any future networks the client needs to reach. For example, if your LAN includes 10.1.0.0/24, 10.1.1.0/24, and 10.1.2.0/24, but you intend to continue adding networks from 10.1.0.0/16, enter 10.1.0.0/16. The entry 10.1.0.0/16 tunnels all traffic destined for 10.1.0.0/16, which also includes the actual networks currently used.

Keyword	Description
ExcludeIPNet = *IP_Address/bits*	(Optional) **Client Version:** VPN 5000 client Version 5.2 and later **Multi-keyword:** To exclude multiple networks, enter this keyword up to 32 times for 32 networks. A network that you do not want remote clients to reach through the tunnel. Traffic to this network is managed by the local ISP (similar to the **ExcludeLocalLAN** keyword). Typically, this network is part of an **IPNet** network. **ExcludeIPNet** networks take precedence over **IPNet** networks when the client determines whether to tunnel a packet. To exclude tunneling to a single host, specify the *bits* as 32. If you use client Version 5.1 or earlier with a concentrator on which you set the **ExcludeIPNet** keyword, the client displays an error.
DNSPrimaryServer = *IP_Address*	(Optional) The IP address of a Domain Name System (DNS) server on the destination network for this VPN group. When the connected user sends a DNS request, the VPN 5000 client intercepts the request and forwards it to the DNS server on the destination network rather than letting the local ISP DNS server answer.

Keyword	Description
Transform = {**ESP(SHA,DES)** | **ESP(SHA,3DES)** | **ESP(MD5,DES)** | **ESP(MD5,3DES)** | **ESP(MD5)** | **ESP(SHA)** | **AH(MD5)** | **AH(SHA)** | **AH(MD5)+ESP(DES)** | **AH(MD5)+ESP(3DES)** | **AH(SHA)+ESP(DES)** | **AH(SHA)+ESP(3DES)**}	**Default:** ESP(MD5,DES) **Multi-keyword:** Enter up to 12 times to propose each of the specified transforms in order until the tunnel peer accepts the options for negotiation. The protection types and algorithms used for IPSec tunnels. The authentication and encryption algorithms of this transform typically match the IKE policy in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security." You might use multiple protection suites if you have a mix of client versions (for example, Windows and Macintosh). If you enter this keyword multiple times, you usually do not offer DES and 3DES, because the added security of 3DES is only secure if it is required of all logins. **Note** The VPN 5000 client for Mac OS and any client that uses NAT transparency require an ESP-only transform that must be listed before any AH transforms. **The AH(*xxx*)+ESP(*xxx*)** options use the Authentication Header to authenticate packets and the ESP header to encrypt packets. (*continued*)

Keyword	Description
(*continued from previous page*)	The transform comprises the following elements. Header type: • **ESP**—Uses the Encapsulating Security Payload (ESP) header. ESP encrypts the data but does not authenticate the outer IP header. • **AH**—Uses the Authentication Header (AH), which authenticates the entire IP packet including the outer IP header. AH provides stronger end-to-end authentication than ESP, but is incompatible with NAT transparency and the VPN 5000 client for Mac OS. Authentication algorithm used for the negotiation: • **MD5**—The message-digest 5 hash algorithm. • **SHA**—The Secure Hash Algorithm, which is considered to be more secure than MD5. Encryption algorithm: • **DES**—(Data Encryption Standard) uses a 56-bit key to scramble the data. • **3DES**—(Triple DES) uses three different keys and three applications of the DES algorithm to scramble the data. 3DES is subject to restrictions by U.S. encryption export laws, and might not be available in concentrators and clients shipped outside of the United States.

Keyword	Description
If you are using SecurID to authenticate users: `SecurIDRequired = On`	Specifies that all users assigned to this VPN group undergo SecurID authentication. See the "Configuring the Concentrator for SecurID" section on page 8-12 for information about configuring SecurID. **Note** If you are using a RADIUS server in passthrough mode with SecurID to provide the VPN group for users, do not set this keyword to On. Configure the concentrator to use RADIUS only.
If the SecurID user name does not match the companion authentication system user name, enter: `SecurIDUserName = On`	SecurID requires a separate system to provide the VPN group association, such as a **VPN Users** list or RADIUS server. For example, you can specify a username in the **VPN Users** section for each VPN group while SecurID uses individual usernames, requiring you to set this keyword to On. The concentrator then prompts each user for their SecurID user name, which it sends to the SecurID server. See the "Using a SecurID System" section on page 8-12 for more information.

Step 3 Assign IP addresses to VPN clients using one of the following methods:

Method	Keyword	Description
Assign a subnet	**LocalIPNet =** *IP_Address*/*bits*	The network from which the concentrator assigns IP addresses to remote clients. This network must be a unique subnet within the concentrator, routable on the network that clients must reach. See the "Subnet Masks" section on page F-2 for a description of */bits*. This keyword is the preferred method over the **StartIPAddress** keyword, which can only be used for traffic destined for Ethernet ports. The value of using **LocalIPNet** over **StartIPAddress** is that the concentrator adds a single route to the routing table for each VPN group's **LocalIPNet** keyword, which is then redistributed using routing protocols or a static route. **StartIPAddress** adds a route for each remote user, which can make the routing table very large. Moreover, you can keep track of remote networks more easily than by setting address groups. The value of using **StartIPAddress** over **LocalIPNet** is that remote users *appear* to be on the same network as the destination network, and the concentrator does not have to advertise the remote users' network using routing protocols. These addresses cannot be shared with other VPN groups. At the end of the client session, the concentrator returns a client's IP address to the pool. **Note** Each **LocalIPNet** uses a connection resource. For example, of you configure 200 VPN groups on a VPN 5008 concentrator with 8 ESP cards, each with one **LocalIPNet**, then the total connection resources available are 39,800 (40,000 minus 200).

Method	Keyword	Description
Assign a range of addresses	**StartIPAddress =** *IP_Address*	The first IP address in a range from which the concentrator assigns IP addresses to remote clients. The number of addresses in the range is specified by the **MaxConnections** value. The range must be on a directly connected Ethernet network. **StartIPAddress** only works for Ethernet because the concentrator uses Proxy ARP to answer ARP requests with its own Ethernet address for the remote user addresses. For example, the concentrator allows remote access to the directly connected 10.1.1.0/24 network. Using **StartIPAddress**, you can assign remote users 10.1.1.225 to 10.1.1.254. Be sure not to use these addresses on the destination network. These addresses cannot be shared with other VPN groups. At the end of the client session, the concentrator returns a client's IP address to the pool.
	StartSubnetMask = *Mask*	

Method	Keyword	Description
Use a RADIUS server	**AssignIPRADIUS = On**	Uses a RADIUS server to assign addresses to VPN users. You can assign addresses from a unique subnet or from a set-aside range on the destination network. If you use a set-aside range, see the description for **StartIPAddress** in this table for information and restrictions. If you assign a unique IP subnet, you might want to configure a matching **LocalIPNet** keyword in the VPN group to perform the following tasks: • Create a single route on the concentrator. Otherwise, the concentrator creates a route for each user when they connect, possibly creating an overly large routing table. • Advertise the network using a dynamic routing protocol. Otherwise, you must create static routes to the client network on neighboring routers. If you use **LocalIPNet** in addition to **AssignIPRADIUS**, set the RADIUS server to assign addresses only from those specified by the **LocalIPNet**. **Note** If the RADIUS server is unavailable, or an authenticated user is not configured for an address in the RADIUS server, the concentrator assigns the user an address from the existing **LocalIPNet** (or **StartIPAddress** if you have one). If the RADIUS server assigns the same address as one already given to a user from the concentrator, a conflict occurs.

See the following sample text configuration:

```
[ VPN Group engineering ]
MaxConnections = 100
IPNet = 10.2.0.0/24
DNSPrimaryServer = 10.2.2.2
Transform = AH(MD5)+ESP(DES)
```

```
SecurIDRequired = On
SecurIDUserName = On
LocalIPNet = 10.3.8.0/24
AssignIPRADIUS = On
```

CHAPTER 8

Authenticating VPN Users

This chapter describes how to configure each supported user-authentication system and how you might use it in your network with the Cisco VPN 5000 concentrator.

Authentication System Overview

When a user connects to the VPN 5000 concentrator, the user is authenticated, and the concentrator is informed that the user belongs to a particular VPN group. Some authentication systems can authenticate and provide the VPN group. Others perform only one task, requiring you to use one system for authentication and one to provide the VPN group. You can use multiple systems for extra security or ease of configuration.

Table 8-1 shows each supported system and its capabilities.

Table 8-1 Authentication Systems

System	Authenticate	Provide VPN Group
VPN Users list	Yes	Yes
RADIUS[1]	Yes	Yes
AXENT Defender with RADIUS component	Yes	Yes
RSA SecurID	Yes	No

Table 8-1 Authentication Systems (continued)

System	Authenticate	Provide VPN Group
Server-side PKI certificate system[2]	Partial	No
SafeWord with synchronous tokens[3] and RADIUS in passthrough mode	Yes	Yes

1. You can also use a Remote Authentication Dial-In User Service (RADIUS) server for accounting only, or to provide the VPN group only.
2. While a server certificate does not authenticate the user, it can be used in conjunction with another system to replace a portion of the authentication process: the authentication of the server by the client.
3. A token is a separate authentication device.

Table 8-2 shows compatible systems and the benefits of these combinations. Systems in parentheses are optional.

Table 8-2 Combined Authentication Systems

Authentication Systems	Purpose
SecurID + **VPN Users** list + (Server-side certificate)	• SecurID supplies authentication. • The **VPN Users** list provides authentication and the VPN group. • The optional certificate replaces the **VPN Users** list shared secret.
SecurID + RADIUS + (Server-side certificate)	• SecurID supplies authentication. • RADIUS supplies authentication and the VPN group. • The optional certificate replaces the RADIUS shared secret.
SecurID + RADIUS in passthrough mode + Server-side certificate	• SecurID supplies authentication. • RADIUS in passsthrough mode supplies authentication and the VPN group. • The required certificate replaces the RADIUS shared secret.

Table 8-2 Combined Authentication Systems (continued)

Authentication Systems	Purpose
AXENT Defender + RADIUS + Server-side certificate	• RADIUS supplies authentication and the VPN group. • Defender supplies authentication. • The required certificate replaces the RADIUS shared secret.
SafeWord + RADIUS in passthrough mode + (Server-side certificate)	• SafeWord supplies authentication. • RADIUS in passthrough mode supplies authentication and the VPN group. • The optional certificate replaces the RADIUS shared secret.
RADIUS + (Server-side certificate)	• RADIUS supplies authentication and the VPN group. • The optional certificate replaces the shared secret.
All systems + (RADIUS accounting)	RADIUS provides accounting for all authentication system users.

Using a VPN Users List

This section describes how to create a **VPN Users** list. If your user list is small and easy to maintain, you can specify the users in the VPN 5000 concentrator configuration. You might also want to use a user list in conjunction with SecurID. See the "Using a SecurID System" section on page 8-12 for more information.

To create a **VPN Users** list, follow these steps:

Step 1 Create the **VPN Users** section using the command line or by editing a text file:

- Command line—Enter the following commands:

```
edit config VPN Users
append $
```

  The prompt changes to `Append>`.

- Text file—Create the following header:

```
[ VPN Users ]
```

Step 2 (Optional) Add a comment by starting the line with a pound sign (#).

If you are using the command line, press the **Enter** key at the end of the comment to go to a new line.

Step 3 Enter a user using the following syntax:

username **Config="***VPN_group***" SharedKey=***Shared_Secret*

Table 8-3 describes the user options.

Table 8-3 User Name Options

Option	Description
username	**Length:** 1 to 60 alphanumeric characters. Alphanumeric characters include a-z, A-Z, and 0-9. A unique user. Your entry must be the same as the name entered in the user's client. Each *username* must be unique to the concentrator. The *username* is case sensitive.
"*VPN_group***"**	The **VPN Group** section name to which the user belongs. Do not enter spaces around the equal sign in **Config="***VPN_group***"**.
Shared_Secret	**Length:** 1 to 255 alphanumeric characters. Alphanumeric characters include a-z, A-Z, and 0-9. The password to authenticate the user with the concentrator and to enable packet encryption. Enter the same shared secret into the VPN client. Do not enter spaces around the equal sign in **SharedSecret=***Shared_Secret*.

Step 4 If you are using the command line, follow these steps:

a. To enter additional users, press the **Enter** key to go to a new line.

b. After entering the last user, press the **Enter** key to go to a new line, enter a period (**.**) and press **Enter**.

c. Enter the following command to exit the editor and keep your changes:

exit

Enter **quit** to exit the editor without making any changes.

See the following sample text configuration:

```
[ VPN Users ]
# generic SecurID users:
engineering config=engineering sharedkey=hello
marketing config=marketing sharedkey=letmein
```

Using a RADIUS Server

RADIUS is a protocol supported by many third-party authentication servers. RADIUS servers can authenticate users, inform the concentrator about the VPN group, and provide accounting statistics for VPN usage.

This section describes how to configure the concentrator for RADIUS or for RADIUS in passthrough mode.

RADIUS Guidelines

Consider the following guidelines on how to use a RADIUS server in your network:

- You can use a server-side certificate with a RADIUS server to replace the shared secret.
- You can use RADIUS for its accounting capabilities alone, for all users regardless of the authentication system.
- You can use a RADIUS server to provide the group association (for example, with a SecurID system) or client IP address.

Configuring the Concentrator for RADIUS

To configure the concentrator to use a RADIUS server for authentication and accounting, follow these steps.

To use a RADIUS server in passthrough mode, see the "Using RADIUS in Passthrough Mode" section on page 8-9.

Step 1 Create the **Radius** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure Radius

- Text file—Create the following header:

  [Radius]

Step 2 To communicate with the RADIUS server, enter the following keywords in the **Radius** section:

Keyword	Purpose
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	The interface that the concentrator uses as a source address for all packets sent to the RADIUS server. You must configure the RADIUS server using this port's IP address.
Secret = "*String*"	**Length:** 1 to 31 ASCII characters A shared secret used by the concentrator and RADIUS server to validate packets exchanged between them. This secret must match the secret configured in the RADIUS server.
PrimAddress = {*IP_Address* | *Domain_Name*}	The IP address or fully qualified domain name of the primary RADIUS server.
SecAddress = {*IP_Address* | *Domain_Name*}	(Optional) The IP address or fully qualified domain name of the backup RADIUS server. If the concentrator receives no response from the primary RADIUS server, then the concentrator uses this secondary server.

Step 3 To use the server for accounting, enter the following keyword:

Keyword	Purpose
`Accounting = On`	Sends accounting information for all users to this RADIUS server.

Step 4 To use the server for authentication, enter the following keywords:

Keyword	Purpose
Authentication = On	Uses a RADIUS server for authentication.
Challengetype = {**CHAP** | **PAP** | **Challenge**}	The challenge type the RADIUS server uses to validate the user. • **CHAP** (Default)—The user is sent a CHAP challenge. • **PAP**—The user is sent a PAP challenge. You must also set the **PAPAuthSecret** for the concentrator to validate the user. • **Challenge**—The concentrator sends a null password to the RADIUS server instead of requiring the client to enter a password. The RADIUS server then prompts the client for the password.
If you set the **Challengetype** keyword to **PAP**, enter: **PAPAuthSecret = "***String***"**	**Length:** 1 to 255 ASCII characters A password for the VPN 5000 concentrator to authenticate and encrypt packets from the VPN 5000 client before the packets are passed on to the RADIUS server. Enter this authentication password in the client in addition to the RADIUS password.
If you are not using a server certificate: **VPNPassword =** *Number*	**Values:** 64 to 191 **Default:** 69 The attribute number the RADIUS server assigns to the Tunnel-Password attribute. For information about server certificates, which replace the Tunnel-Password, see Chapter 10, "Installing Certificates on the Concentrator."
VPNGroupInfo = *Number*	**Values:** 64 to 191 **Default:** 77 The attribute number the RADIUS server assigns to the Connect-Info attribute (the VPN group name).

See the following sample text configuration:

```
[ Radius ]
BindTo = Ethernet 1.0.1
Secret = googol
PrimAddress = 10.9.8.3
SecAddress = 10.9.7.1
Authentication = On
Challengetype = CHAP
```

Configuring the RADIUS Server to Communicate with the Concentrator

Configure the RADIUS server to communicate with the concentrator by specifying the concentrator IP address (equal to the **Radius** section **BindTo** IP address) as well as the shared secret (equal to the **Radius** section **Secret** string).

See the *Cisco VPN 5000 Concentrator Series Command Reference Guide* for the RADIUS attributes you need to define in the dictionary file to authenticate each user. See the documentation that was shipped with your server for more information.

Using RADIUS in Passthrough Mode

Use a RADIUS server in passthrough mode to support a SafeWord system or, optionally, to use a SecurID system. Passthrough mode allows the RADIUS server to act as an intermediary between the concentrator and the other authentication system.

Note Passthrough mode does not support some SecurID or SafeWord functionality, such as allowing users to change their PIN.

Configuring the Concentrator for RADIUS in Passthrough Mode

Configure the concentrator to use a RADIUS system according to the "Configuring the Concentrator for RADIUS" section on page 8-5, but set the following keywords in the **Radius** section for passthrough mode:

```
Challengetype = PAP
PAPAuthSecret = "String"
```

Note If you are using SecurID with RADIUS in passthrough mode, do not also configure the concentrator to use SecurID in the **SecurID** section or in the **VPN Group** section. Only configure the RADIUS parameters.

Configuring the RADIUS Server for Passthrough Mode

In addition to the RADIUS dictionary file attributes listed in the *Cisco VPN 5000 Concentrator Series Command Reference Guide*, use the following attributes:

- Attribute number 200 for the token password.
- Attribute number 2 for the user password. For example, for the Cisco Secure RADIUS server, set the password for all users to one of the following values:
  - **sdi** (SecurID)
  - **safeword** (SafeWord)

  Check with your RADIUS manufacturer for the exact values of these passwords for use with SecurID or SafeWord.

Using AXENT Defender

You must use an AXENT Defender system with a RADIUS server that supports Defender, such as Cisco Secure or the AXENT RADIUS server. Defender comprises both a server and a token for each user. The user enters a PIN in the token, which generates a special one-time password that the user enters into the client prompt.

AXENT Defender Guidelines

Consider the following guidelines for using AXENT Defender:

- Defender requires VPN 5000 client Version 4.2.x or later.
- You must use a server-side certificate to replace the RADIUS shared secret.

Configuring the Concentrator for AXENT Defender

Because the concentrator requires a RADIUS server with AXENT Defender, configure the concentrator to communicate with a RADIUS server according to the "Using a RADIUS Server" section on page 8-5. Be sure to set the following keyword in the **Radius** section to work with AXENT Defender:

```
Challengetype = Challenge
```

Challenge specifies that the concentrator sends a null password to the RADIUS server instead of requiring the client to enter a password. The RADIUS server then prompts the client for the AXENT Defender token password.

Using a SafeWord System

SafeWord comprises both a RADIUS server and a separate token for each user. The VPN 5000 concentrator supports synchronous SafeWord tokens. SafeWord requires the username and token password to be combined to *username*,*token*. To achieve this combination using SafeWord alone, you need to change the username in the VPN 5000 client every time you connect to *username*,*token*.

Because this method is cumbersome to users, we recommend using an additional RADIUS server in passthrough mode. The passthrough RADIUS server only requires the username as entered in the VPN 5000 client. The SafeWord system then sends a prompt through the passthrough server to the client for the token password.

See the "Using RADIUS in Passthrough Mode" section on page 8-9 to configure the concentrator. If you choose to use SafeWord without a passthrough RADIUS server, see the "Configuring the Concentrator for RADIUS" section on page 8-5 to configure the concentrator for a regular RADIUS server.

Using a SecurID System

SecurID, from RSA Security, comprises both a server (called the ACE/Server) and a separate token for each user. The user logs in and enters a password consisting of a PIN combined with a one-time code generated by the token. SecurID does not return the VPN group to the concentrator, so you must use SecurID with another system. For example:

- SecurID plus a **VPN Users** list. You can add a single user to the VPN 5000 user list that specifies the VPN group. All users log in to the concentrator with the same user name, but are then authorized by the SecurID system individually.
- SecurID plus a RADIUS server. Configure the concentrator for both SecurID and RADIUS. See the "Using a RADIUS Server" section on page 8-5 for more information about using a RADIUS server.
- SecurID plus a RADIUS server in passthrough mode. In this case, do not configure the concentrator for SecurID in the **SecurID** section or in the **VPN Group** section. See the "Using RADIUS in Passthrough Mode" section on page 8-9 for more information.

You can also use any of the above combinations using a server-side certificate.

If you are not using a RADIUS server in passthrough mode, set up the VPN 5000 concentrator to communicate with the ACE/Server, and configure the ACE/Server with user settings (as described in the following sections).

Configuring the Concentrator for SecurID

The server portion of the SecurID system is the ACE/Server. To configure the concentrator to communicate with the ACE/Server, follow these steps.

Note In addition to entering the following commands, you must also set the **VPN Group** section **SecurIDRequired** keyword to On.

Step 1 Create the **SecurID** section using the command line or by editing a text file:

- Command line—Enter the following command:

```
configure SecurID
```

- Text file—Create the following header:

```
[ SecurID ]
```

Step 2 Enter the following keywords in the **SecurID** section:

Keyword	Purpose
Enabled = On	Enables SecurID.
PrimaryServer = *IP_Address*	Sets the IP address of the primary ACE/Server.
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	Sets the interface that the concentrator uses as a source address for all packets sent to the ACE/Server. You must also configure the ACE/Server with this interface's IP address.

See the following sample text configuration:

```
[ SecurID ]
Enabled = On
PrimaryServer = 10.9.8.3
BindTo = Ethernet 1.0.1
```

Configuring the ACE/Server

To configure the ACE/Server for communication with the VPN 5000 concentrator, see the guide that was shipped with the server. Configure the concentrator as a Communication Server in the Client Type drop-down menu in the ACE/Server Add Client dialog box (under Client > Add Client).

The first time the concentrator contacts an ACE/Server, it exchanges a shared secret based in part on the concentrator's IP address. If you change the concentrator IP address after you initially connect to the ACE/Server, the

concentrator and server are no longer able to communicate. To re-establish contact, uncheck the **Sent Node Secret** check box in the ACE/Server Add Client dialog box, and enter the following command on the concentrator:

```
reset securid secret {IP_address | all}
```

Where *IP_address* resets the secret for a specific ACE/Server, and **all** resets the secrets for all ACE/Servers.

Using a Server-Side PKI Certificate System

The concentrator can use server-side certificates (also known as Hybrid mode) in conjunction with RADIUS, SecurID, or Defender to replace the shared secret.

See the *Cisco VPN 5000 Concentrator Series Command Reference Guide* for an overview of how certificates work.

To configure the VPN 5000 concentrator to use certificates, see Chapter 10, "Installing Certificates on the Concentrator." To use a root certificate with the VPN 5000 client, see the *Cisco VPN 5000 Client User Guide* for your platform. The concentrator does not support user certificates.

Supported CAs

The VPN 5000 concentrator supports server certificates from:

- Entrust/PKI with Entrust/VPNConnector
- RSA Keon Certificate Server (Version 5.5 and earlier)
- The concentrator configured as a certificate generator (CG)

CHAPTER 9

Configuring VPN LAN-to-LAN Tunnels

A LAN-to-LAN tunnel allows two sites, each with a Cisco VPN 5000 concentrator or compatible device, to securely connect over the Internet or other network connection. All traffic destined from one LAN to the other is tunneled, without individual hosts having to use VPN clients.

This chapter describes how to configure IP routing over the tunnel (if applicable), and how to create a LAN-to-LAN tunnel using one of the following methods:

- Proprietary IPSec—A LAN-to-LAN tunnel between two VPN 5000 concentrators.
- Standard IPSec—A LAN-to-LAN tunnel between the VPN 5000 concentrator and a third-party device.
- Dynamic responder—LAN-to-LAN tunnels between the VPN 5000 concentrator and multiple concentrators or third-party devices.
- GRE—A LAN-to-LAN tunnel between a VPN 5000 concentrator and a concentrator or third-party device.

For IPSec tunnels, you must also set initial tunnel security parameters described in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security."

Note Make sure that the IP address of the port on each end of the tunnel is routable on the network the tunnel runs over. For example, if the tunnel runs over the Internet, the tunnel ends must have Internet-routable addresses. If the tunnel runs over a Frame Relay connection, you can use addresses, including private addresses, that are only routable on the tunnel partner networks.

Using a Proprietary IPSec Tunnel

A proprietary IPSec tunnel between two VPN 5000 concentrators sends and receives traffic to and from all connected networks in a pair of IPSec Security Associations (SAs), and allows routing protocols across the tunnel. Use this tunnel type between two VPN 5000 concentrators.

To create a proprietary IPSec tunnel, follow these steps:

Step 1 Create the **Tunnel Partner** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure Tunnel Partner VPN [*slot*:]*number*

  - *number*—A unique identifier for this tunnel, between 0 and 1 less than the maximum tunnels per ESP card (for example, 4999).
  - *slot*—For modular platforms. Load-balances the VPN processing. The slot you enter here is not related to the slot at which the tunnel terminates; rather, you specify the slot to identify the ESP card processor that handles the VPN processing for this tunnel. For several tunnels, divide them evenly among the slots, making sure not to exceed the maximum tunnels supported by an ESP card. By default, the *slot* is 0.

  You can reuse the *number* for each slot. For example, 0:1 and 1:1 are allowed.

- Text file—Create the following header:

  [Tunnel Partner VPN [*slot*:]*number* **]**

  See the command line bullet above for a description of the section syntax.

Step 2 To configure the tunnel partner and tunnel properties, enter the following keywords in the **Tunnel Partner** section:

Keyword	Purpose
Partner = *IP_Address*	The IP address of the interface at the remote end of the tunnel.
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	The local interface that acts as the endpoint for the tunnel.
KeyManage = {**Auto** | **Initiate** | **Respond**}	Specifies the concentrator that establishes the tunnel. • **Auto** (Default)—The concentrator compares the IP addresses of the **BindTo** port and the **Partner** and makes the lower IP address the initiator, while the higher IP address is always the responder. The initiator establishes the tunnel at startup using IKE. • **Initiate**—The concentrator always initiates the tunnel at startup using IKE. It does not respond to tunnel establishment attempts from the peer. • **Respond**—The concentrator uses IKE, but only responds to tunnel establishment attempts from other concentrators. It does not initiate tunnel establishment.

Keyword	Purpose
If you are using certificates for authentication or are connecting to a dynamic responder: **Mode = Main**	The IKE Phase 1 negotiation mode between the devices. Phase 1 controls how the two devices identify and authenticate each other so that tunnel sessions can be established. Main mode accomplishes the Phase 1 tasks in 6 packets. It keeps the identities of the peers secret (unless the identities are the IP addresses of the peers). This setting must match the Phase 1 negotiation mode of the remote peer. Main mode is required for tunnels using certificates and for tunnels to a dynamic responder. The default is **Aggressive**, which accomplishes the four Phase 1 tasks in 3 packets with some restrictions on the key exchange. We recommend Aggressive mode if you are not using certificates.
Transform = {**ESP(SHA,DES)** | **ESP(SHA,3DES)** | **ESP(MD5,DES)** | **ESP(MD5,3DES)** | **ESP(MD5)** | **ESP(SHA)** | **AH(MD5)** | **AH(SHA)** | **AH(MD5)+ESP(DES)** | **AH(MD5)+ESP(3DES)** | **AH(SHA)+ESP(DES)** | **AH(SHA)+ESP(3DES)**}	**Default:** ESP(MD5,DES) **Multi-keyword:** Enter up to 12 times to propose each of the specified transforms in order until the tunnel peer accepts the options for negotiation. The authentication and encryption algorithms used for tunnel sessions. The authentication and encryption algorithms of this transform typically match the IKE policy in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security." See the "Configuring a VPN Group for the VPN 5000 Client" section on page 7-2 for more information about transform options.

Step 3 To connect to a dynamic responder, or to connect only two networks and avoid using routing protocols, enter the following keywords:

LocalAccess = *IP_Address*/*bits*	A local host or subnet that a peer can reach through the tunnel. To allow access to only a single host, specify **32** in the *bits* portion. See the "Subnet Masks" section on page F-2 for a description of */bits*.
Peer = *IP_Address*/*bits*	A host or subnet connected to the remote tunnel partner that the concentrator can reach through the tunnel. To allow access to only a single host, specify **32** in the *bits* portion. See the "Subnet Masks" section on page F-2 for a description of */bits*. Any packets destined for the **Peer** network are tunneled.

Step 4 Use one of the following methods to authenticate the tunnel peer:

Method	Keyword	Description
Shared Key	**SharedKey = "***Pass_Phrase***"**	**Length:** 1 to 255 characters Generates session keys that are used to authenticate and encrypt each packet received or sent through the tunnel. Enter the same key on both concentrators.
Certificates	**Certificates = On**	The tunnel initiator always determines the method of authentication. If you enable certificates, but you set a **SharedKey**, the tunnel partner (if they are the initiator) can successfully use the shared key, See Chapter 10, "Installing Certificates on the Concentrator," for more information about certificate authentication.

Step 5 Configure IP routing according to the "Configuring IP Routing Over a the Tunnel" section on page 9-14.

See the following sample text configuration:

```
[ Tunnel Partner VPN 0:0 ]
Partner = 198.48.8.1
BindTo = Ethernet 0.0.3
Mode = Main
Transform = ESP(SHA,3DES)
```

```
Certificates = On
```

Using a Standard IPSec Tunnel Partner

This section describes how to create a standard IPSec tunnel to a third-party device.

Guidelines for Connecting Networks over a Standard IPSec Tunnel

To connect networks, see the following guidelines:

- A standard IPSec tunnel includes only one local and remote network pair.

  For example, use one tunnel to connect network A to network B and a separate tunnel to connect network A to network C.

- You must specify a separate **Tunnel Partner** section for each tunnel (for each network pair).

  For example, in **Tunnel Partner VPN 0:1**, you can connect network A to network B. To connect network A to network C, create a **Tunnel Partner VPN 0:2** section.

- You can only use an IP address pair (the local **BindTo** port address and the remote **Partner** address) one time on the concentrator.

  For example, use Ethernet 1:0 and the remote address 129.78.90.6 for one **Tunnel Partner** section, but to create another tunnel, you must use Ethernet 1:0 to connect to a different address on the remote concentrator, or vice versa.

Tip To consolidate traffic in one tunnel, supernet the networks on each side of the tunnel if possible.

For example, connect the following networks:

- Local networks 10.1.0.0/24, 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24

- Remote networks 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24

Set the following keyword values:

- Set the **LocalAccess** keyword to 10.1.0.0/22, which includes the networks 10.1.0.0 through 10.1.3.0.
- Set the **Peer** keyword to 192.168.0.0/22, which includes the networks 192.168.0.0 through 192.168.3.0.

Configuring a Standard IPSec Tunnel

To create a standard IPSec tunnel from a local interface to an IP address on a remote device, follow these steps:

Step 1 Create the **Tunnel Partner** section using the command line or by editing a text file:

- Command line—Enter the following commands:

```
context change "context_name"
configure Tunnel Partner VPN [slot:]number
```

  - *number*—A unique identifier for this tunnel, between 0 and 1 less than the maximum tunnels per ESP card (for example, 4999).
  - *slot*—For modular platforms. Load-balances the VPN processing. The slot you enter here is not related to the slot at which the tunnel terminates; rather, you specify the slot to identify the ESP card processor that handles the VPN processing for this tunnel. For several tunnels, divide them evenly among the slots, making sure not to exceed the maximum tunnels supported by an ESP card. By default, the *slot* is 0.

  You can reuse the *number* for each slot. For example, 0:1 and 1:1 are allowed.

- Text file—Create the following header in the CVC you are configuring:

```
[ Tunnel Partner VPN [slot:]number ]
```

  See the command line bullet above for a description of the section syntax.

Step 2 To configure the tunnel partner and tunnel properties, enter the following keywords in the **Tunnel Partner** section:

Keyword	Purpose
Partner = *IP_Address*	The IP address of the interface at the remote end of the tunnel.
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	The local interface that acts as the endpoint for the tunnel.
Transform = {**ESP(SHA,DES)** | **ESP(SHA,3DES)** | **ESP(MD5,DES)** | **ESP(MD5,3DES)** | **ESP(MD5)** | **ESP(SHA)** | **AH(MD5)** | **AH(SHA)** | **AH(MD5)+ESP(DES)** | **AH(MD5)+ESP(3DES)** | **AH(SHA)+ESP(DES)** | **AH(SHA)+ESP(3DES)**}	**Default:** ESP(MD5,DES) **Multi-keyword:** Enter up to 12 times to propose each of the specified transforms in order until the tunnel peer accepts the options for negotiation. The authentication and encryption algorithms used for tunnel sessions. The authentication and encryption algorithms of this transform typically match the IKE policy in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security." See the "Configuring a VPN Group for the VPN 5000 Client" section on page 7-2 for more information about transform options.
Mode = Main	The IKE Phase 1 negotiation mode between the devices. Phase 1 controls how the two devices identify and authenticate each other so that tunnel sessions can be established. This setting must match the Phase 1 negotiation mode of the remote peer. We recommend Main mode for standard IPSec tunnels. **Main** accomplishes the Phase 1 tasks in 6 packets. It keeps the identities of the peers secret (unless the identities are the IP addresses of the peers).

Keyword	Purpose
KeyManage = {**Initiate** | **Respond**}	• **Initiate**—The concentrator always initiates the tunnel at startup using IKE. It does not respond to tunnel establishment attempts from the peer. This setting allows the VPN 5000 concentrator to keep the tunnel up until the peer performs an IKE Phase 1 rekey (typically every 24 hours). Because the tunnel stays up, the concentrator can successfully send traffic whenever required. However, after the Phase 1 rekey, the tunnel fails and must be re-established using the **vpn tunnel down** and **up** commands (see the *VPN 5000 Concentrator Series Command Reference Guide*). • **Respond**—The concentrator uses IKE, but only responds to tunnel establishment attempts from other concentrators. It does not initiate tunnel establishment. This setting allows the tunnel to be re-established automatically by the peer after a Phase 1 rekey. However, if the peer does not need to send traffic and takes the tunnel down, the VPN 5000 concentrator cannot send any traffic until the tunnel is re-established by the peer.
LocalAccess = *IP_Address*/*bits*	A local host or subnet that a peer can reach through the tunnel. To allow access to only a single host, specify **32** in the *bits* portion. See the "Subnet Masks" section on page F-2 for a description of */bits*.
Peer = *IP_Address*/*bits*	A host or subnet connected to the remote tunnel partner that the concentrator can reach through the tunnel. To allow access to only a single host, specify **32** in the *bits* portion. See the "Subnet Masks" section on page F-2 for a description of */bits*. Any packets destined for the **Peer** network are tunneled.

Step 3 Use one of the following methods to authenticate the tunnel peer:

Method	Keyword	Description
Shared Key	**SharedKey = "***Pass_Phrase***"**	**Length:** 1 to 255 characters Generates session keys that are used to authenticate and encrypt each packet received or sent through the tunnel. Enter the same key on both concentrators.
Certificates	**Certificates = On**	The tunnel initiator always determines the method of authentication. If you enable certificates, but you set a **SharedKey**, the tunnel partner (if they are the initiator) can successfully use the shared key, See Chapter 10, "Installing Certificates on the Concentrator," for more information about certificate authentication.

See the following sample text configuration:

```
[ Tunnel Partner VPN 0:0 ]
Partner = 198.48.8.1
BindTo = Ethernet 0.0.3
Mode = Main
Transform = ESP(SHA,3DES)
KeyManage = Initiate
LocalAccess = 10.1.1.0/24
Peer = 10.2.1.0/24
Certificates = On
```

Using a Dynamic Responder

This section describes how to configure a concentrator to respond to tunnel sessions initiated by any other concentrator, which can be a VPN 5000 concentrator or third-party equipment. A remote concentrator can connect to the dynamic responder as long as it is authorized with a **SharedKey** or a certificate.

Note When the Cisco IOS device performs an IKE Phase 1 rekey (typically every 24 hours), the Cisco IOS device takes the tunnel offline. The dynamic responder then waits for the Cisco IOS device to re-establish the tunnel. If in this period traffic needs to go from the VPN 5000 concentrator to the Cisco IOS device (or if the tunnel fails for any other reason), the traffic is dropped. Cisco IOS only re-establishes the tunnel when it has traffic to send.

Configuring a Dynamic Responder

To create a dynamic responder, follow these steps:

Step 1 Create the **Tunnel Partner** section using the command line or by editing a text file:

- Command line—Enter the following command:

```
configure Tunnel Partner VPN Default
```

- Text file—Create the following header:

```
[ Tunnel Partner VPN Default ]
```

Step 2 To configure the tunnel partner and tunnel properties, enter the following keywords in the **Tunnel Partner** section:

Keyword	Purpose
VPN 5002 or 5008: **BindTo = {Ethernet | WAN}** *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	The local interface that acts as the endpoint for the tunnel.
Transform = {**ESP(SHA,DES)** | **ESP(SHA,3DES)** | **ESP(MD5,DES)** | **ESP(MD5,3DES)** | **ESP(MD5)** | **ESP(SHA)** | **AH(MD5)** | **AH(SHA)** | **AH(MD5)+ESP(DES)** | **AH(MD5)+ESP(3DES)** | **AH(SHA)+ESP(DES)** | **AH(SHA)+ESP(3DES)**}	**Default:** ESP(MD5,DES) **Multi-keyword:** Enter up to 12 times to propose each of the specified transforms in order until the tunnel peer accepts the options for negotiation. The authentication and encryption algorithms used for tunnel sessions. The authentication and encryption algorithms of this transform typically match the IKE policy in Chapter 6, "Configuring the IKE Policy for IPSec Tunnel Security." See the "Configuring a VPN Group for the VPN 5000 Client" section on page 7-2 for more information about transform options.

Step 3 Use one of the following methods to authenticate the tunnel peer:

Method	Tunnel Partner Keywords	Description
Shared Key	**SharedKey = "***Pass_Phrase***"**	**Length:** 1 to 255 characters Generates session keys that are used to authenticate and encrypt each packet received or sent through the tunnel. Enter the same key on both concentrators.
Certificates	The tunnel initiator always determines the method of authentication. Because the dynamic responder always responds, If you enable certificates, but you also set a **SharedKey**, the tunnel partner (if they initiate the tunnel) can successfully use the **SharedKey**. See Chapter 10, "Installing Certificates on the Concentrator," for more information about certificate authentication.	

See the following sample text configuration:

```
[ Tunnel Partner VPN Default ]
BindTo = Ethernet 0.0.3
Transform = ESP(SHA,3DES)
```

Configuring a GRE Tunnel Partner

The following steps describe how to create a GRE tunnel from a local interface to an IP address on a remote concentrator. GRE does not provide authentication or encryption like IPSec does.

To create a GRE tunnel from a local interface to an IP address on a remote device, follow these steps:

Step 1 Create the **Tunnel Partner** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure Tunnel Partner VPN [**0:**]*number*

  - **0:**—For VPN 5002 and 5008, GRE tunnels always use the card in slot 0 for processing. If you do not enter the slot number, slot 0 is used by default. However, you might want to enter the slot to make it easier to keep track of available identifiers (**Tunnel Partner VPN 56** is the same as **Tunnel Partner VPN 0:56**).
  - *number*—A unique identifier for this tunnel, between 0 and 1 less than the maximum tunnels per ESP card (for example, 4999).

- Text file—Create the following header:

  [Tunnel Partner VPN [**0:**]*number* **]**

  See the command line bullet above for a description of the section syntax.

Step 2 To configure the tunnel partner and tunnel properties, enter the following keywords in the **Tunnel Partner** section:

Keyword	Purpose
Partner = *IP_Address*	The IP address of the interface at the remote end of the tunnel.
VPN 5002 or 5008: **BindTo =** {**Ethernet** | **WAN**} *slot*:**0**[.*subinterface*] VPN 5001: **BindTo = Ethernet** {**1** | **0**}[.*subinterface*]	The local interface that acts as the endpoint for the tunnel.
KeyManage = Manual	Sets the tunnel type to GRE.

Step 3 Configure IP routing according to the "Configuring IP Routing Over a the Tunnel" section on page 9-14.

See the following sample text configuration:

```
[ Tunnel Partner VPN 0:0 ]
Partner = 198.48.8.1
BindTo = Ethernet 0.0.3
KeyManage = Manual
```

Configuring IP Routing Over a the Tunnel

After you create the **Tunnel Partner** section, you must configure IP routing by entering the following commands. Only proprietary IPSec and GRE tunnels allow IP routing over the tunnel.

Step 1 Access the **IP** section using the command line or by editing a text file:

- Command line—Enter the following command:

  configure IP VPN [*slot*:]*Tunnel_Partner_Number*

Where the [*slot*:]*Tunnel_Partner_Number* is he slot and number you specified for the **Tunnel Partner** section.

- Text file—Create the following header:

  [IP VPN [*slot*:]*Tunnel_Partner_Number* **]**

  Where the [*slot*:]*Tunnel_Partner_Number* is he slot and number you specified for the **Tunnel Partner** section.

Step 2 To enable routing, enter the following keyword in the **IP** section:

Keyword	Description
Mode = Routed	Enables routing.

Step 3 Configure a routing protocol or static routes according to the "Configuring the Dynamic Routing Protocol" section on page 5-11 or the "Configuring the Default Route or Static Routes" section on page 5-13.

For a static route, specify the gateway *Port* as **VPN** [*slot*:]*number*. For example:

```
10.2.1.0 255.255.255.0 VPN 1:1 1
```

CHAPTER 10

Installing Certificates on the Concentrator

A public key infrastructure (PKI) certificate system (also known as "digital certificates" or "certificates") allows a tunnel peer (such as the Cisco VPN 5000 concentrator) to authenticate another tunnel peer, without the network administrator having to enter or maintain passwords or shared secrets in a database. A shared secret is a password known by both sides that is used to encrypt and decrypt the data. Certificates are special encrypted text files (generated by a trusted certificate authority (CA), which is an application that you install and configure on a computer in your network) that are used to encrypt and decrypt the data.

For a detailed description of how certificates work, see the *Cisco VPN 5000 Concentrator Series Command Reference Guide*.

This chapter describes:

- Certificate Guidelines
- Setting Up a Certificate Generator if you are not using a CA
- Requesting a Server Certificate
- Installing a Certificate on a Concentrator
- Managing Certificates

Note See the *Cisco VPN 5000 Client User Guide* for your platform for instructions on installing certificates on the client.

Certificate Guidelines

See the following guidelines to use certificates.

Features

The concentrator supports:

- Server-side certificates with clients
- Full certificate authentication between servers
- Certificate generation by the concentrator

Limitations

The concentrator does not support:

- CRLs
- Client user certificates
- Certificate chaining
- Certificates larger than 1400 bytes
- Multiple CAs per concentrator—Use only one root and server certificate per concentrator.

Supported CAs

The VPN 5000 concentrator supports certificates from:

- Entrust/PKI Version 5.0 with Entrust/VPNConnector
- RSA Keon Certificate Server Version 5.5 and earlier
- VPN 5000 concentrator configured as a certificate generator (CG)

Setting Up a Certificate Generator

This section describes how to set up a VPN 5000 concentrator as the CG for your network, generate the root certificate, distribute the root certificate, and generate a server certificate for the CG. You can also archive to a server or transfer to another concentrator the root certificate and private key bundle.

Setting a Concentrator as a Certificate Generator

To set the concentrator as a CG, follow these steps:

Step 1 Create the **Certificates** section using the command line or by editing a text file:

- Command line—Enter the following command:

  ```
  configure Certificates
  ```

- Text file—Create the following header:

  ```
  [ Certificates ]
  ```

Step 2 Enter the following keywords in the **Certificates** section:

Keyword	Purpose
`CertificateGenerator = On`	Makes the server a CG.
`ValidityPeriod =` *`Days`*	**Values:** 1 to 9999 days **Default:** 365 The default validity period of CG-generated certificates. You can override this value when you request a certificate using the **certificate generate** command.

Step 3 You must download or save these changes to the concentrator before generating any certificates on the CG.

Downloading or saving the configuration causes the concentrator to reboot.

- To download a text file, see the "Copying a Text Configuration File" section on page B-6.
- To save your command line changes, enter **save**.

See the following sample text configuration:

```
[ Certificates ]
CertificateGenerator = On
```

Creating a Root Certificate

The CG creates the root certificate, which identifies the CG. When you install the root certificate on each tunnel peer, this certificate allows the peer to verify the server certificate created by the CG.

To create a root certificate on a CG, complete the following steps:

Step 1 Set the time according to the "Setting the Time" section on page 3-2.

Step 2 On the CG, enter:

certificate generate root *key_length* [**locality** *city*] [**state** *state*] [**country** *country_code*] [**organization "***organization_name***"**] [**commonname "***common_name***"**] [**days** *validity_period*]

Table 10-1 describes the options.

Table 10-1 Certificate Generate Options

Option	Description
key_length	**Values:** 512, 1024, or 2048 The number of bits generated for the key. We recommend using a key length of 1024. A large key can take the system up to an hour to generate.
city	A text string with no spaces identifying the city name in which the concentrator resides.
state	A text string with no spaces identifying the state or province name in which the concentrator resides.
country_code	A 2-letter country code in which the concentrator resides.
"*organization_name*"	A phrase, with spaces allowed, identifying the company name or other organization name.
"*common_name*"	**Default:** The device name (**General** section **DeviceName** keyword). For a CG, the concentrator adds "CG," for example, VPN5008CG. A phrase, with spaces allowed, identifying the concentrator name, or a description of the certificate.
validity_period	**Values:** 1 to 9999 days The validity period of the certificate. If you do not enter a value, the system uses the value you set for **ValidityPeriod** on the CG.

For example:

```
certificate generate root 1024 locality boulder state co country US
organization "Cisco IT" commonname "Cisco Root Cert" days 120
```

Note The optional **days**, **locality**, **state**, **country**, **organization**, and **commonname** values do not need to match the values in the server certificates or requests.

Distributing the Root Certificate

To distribute the root certificate, follow these steps.

Note We recommend running the commands in this procedure on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Step 1 After you enter the command to generate the certificate in the previous section, wait for the concentrator to generate the root certificate.

Depending on the key length, the concentrator can take up to one hour to create the certificate in a background process. To determine if the generator is finished (idle) or still generating (busy), enter the following command:

```
show certificate generator
```

The system log also documents a completed certificate with a Notice level message. See the "Setting Logging Options" section on page 3-5 for more information on viewing the log.

Step 2 When the concentrator is finished generating, view the root certificate by entering:

```
show certificate pem root [x509]
```

Where **x509** displays the certificate in X.509 format instead of the default PKCS #7 format. The concentrator and VPN 5000 client can import both formats.

The console displays the root certificate text.

Step 3 Select the text, making sure to select the entire block, including the last carriage return.

Selecting the last carriage return might require you to select the area in front of the prompt that follows the text.

Step 4 Copy the root certificate into a text file for distribution to clients or other concentrators, or keep the text on the clipboard to paste into a concentrator.

See the *Cisco VPN 5000 Client User Guide* for your platform for instructions to install the root certificate on the client. To install the root certificate on another VPN 5000 concentrator, see the "Installing a Certificate on a Concentrator" section on page 10-14.

Generating the CG Server Certificate

The CG can generate its own server certificate, which allows tunnel peers with root certificates to authenticate the CG. Other concentrators must request a certificate from the CG or CA, which can approve or reject the request. See the "Requesting a Server Certificate" section on page 10-10 to generate other server certificates.

To generate the CG server certificate, follow these steps:

Step 1 Before you generate the server certificate, create the root certificate according to the "Creating a Root Certificate" section on page 10-4.

Step 2 To generate the server certificate for the CG, enter:

certificate generate server *key_length* [**locality** *city*] [**state** *state*] [**country** *country_code*] [**organization "***organization_name***"**] [**commonname "***common_name***"**] [**days** *validity_period*]

See Table 10-1 on page 10-5 for a description of the options. For example:

```
certificate generate server 1024 commonname "VPN 5002 Server"
```

Depending on the key length, the concentrator can take up to one hour to create the certificate in a background process.

Step 3 To determine if the generator is finished (idle) or still generating (busy), enter the following command:

```
show certificate generator
```

The system log also documents a completed request with a Notice level message. See the "Setting Logging Options" section on page 3-5 for more information on viewing the log.

Transferring the CG Root Certificate and Private Key

If you are using the VPN 5000 concentrator as a CG, and you need to replace the system, you can use the following procedures to transfer the root certificate and private key bundle to a new CG or to a file server for archiving purposes. Generating server certificates can be time consuming, and this procedure allows you to keep any existing server certificates if the CG fails.

Note We recommend running the commands in these procedures on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Exporting the Bundle

To export the root certificate and private key bundle, follow these steps:

Step 1 On the original CG, enter:

certificate cg export *password*

Where *password* is up to 50 characters in length. This password encrypts the root certificate and private key bundle. The same password decrypts the bundle when you use import it.

The console displays the root certificate and private key bundle in PKCS#12 format:

```
Successful

-----BEGIN PKCS12-----
MIID7QIBAzCABgkqhkiG9w0BBwGggASCA6QwggOgMIAGCSqGSIb3DQEHBqCAMIIB
rAIBADCCAaUGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEGMA4ECKmsDZ+H17J9AgII
AICCAXh2rRTQEg8507Af1I3n7JQ0sYOFSfZY8QjsxEJpG0CPC5/op7AeoOiOdxqt
j2WCBtKJldom1FDOLQYeHk9Y9RUo8BkVFs8r3ZWm/bhLDvuL3m1v2qe1Uvr4Ha6+
lCNUTaOWyJefAGgYbMYZFsBY3LWuGwzmXU3km1b/DVkcY+tPEERn0XaFgavgl2xH
kquBryxnrEBepoNfZJf7KLlcYT7lj3cAHYXPA0TJDTvLu9Za30cWtz53YHeUr7MU
QX9Unek2//halTB7frZYu2V8njoeqIQFNMcZmtb2xPFugAjNXgXkQHNziRYkuW5A
sj5EAweIcpgSrXEMX5fz3djZSytKjktmN0LU1WNVgt9csUGQPK3XDmLN4EojdBOJ
LtS0uR6GXduRbXNKCiwgzaDztvajacqgppzkc+MZ52+MftS3orE3ltk/A/3tSAlm
qYAbw/6IbnA4HkQ8IktFQryYf/5O04BbiRNOxApZyHD6vjHBP0vCo1GxYK1BAAAA
ADCABgkqhkiG9w0BBwGggASCAcYwggHCMIIBvgYLKoZIhvcNAQwKAQKgggGGMIIB
gjAcBgoqhkiG9w0BDAEDMA4ECJU6PZuUJtwzAgIIAASCAWB2XZvTeZ2jBfCvgTu+
```

```
DJgNm/rjt6TZV4Q7P5g3j2k2MitQYpPayeyqTMVCFWqSUH59eBc9HJ734aenkd2A
tbPf+/gm+ZQ4G4Qvpdtml/haxYgd5B8RgUGt/YEcyv0WdFdA+yuijYC3eqWfgaaa
lELHjFX7kAnUGdVtMpe2gTgN1W89thsCDbR7//Ff43BEemE81N4O9EpDbqpz4DP/
4fSIB9nv4rLpNQv6Q+DYozkpJ9flqpkzjR3HVTXwaOY2c+zpccCyLX4ys6aMSomS
JNeFQBhoGqtq9dVKnfwTcxHjKGo06hT7wNCoJNi9Lgt9VEWyPVLTEBI7gpMZyE8S
07A0f7GmVLNsaklAhaNoFJWhkbux2px7D593X+WHqIaGSWA5q+ILyww2zFuh1ANz
m5KDcHCI3m0RnooLCuGPIrP390oyFjlb9v763ApaF+guSMvfD4YGROHXg/PvIY2M
UZTRMSUwIwYJKoZIhvcNAQkVMRYEFH2Jol4uCF1co0XgcEAQ1zQT1pLmAAAAAAAA
AAAwLTAhMAkGBSsOAwIaBQAEFK8iq4HQUYmhGKZKimGIjY3+KzA5BAh9H5wSyh0g
Jg==
-----END PKCS12-----
```

Step 2 Copy the bundle to the clipboard or to a text editor.

When you select the text on the console, be sure to include the carriage return after the last line. Selecting the last carriage return might require you to select the area in front of the prompt that follows the text.

Note The CG still has the root certificate and private key installed after exporting a copy.

Importing the Bundle

To import the root certificate and private key bundle, follow these steps.

Note If the system already has a root certificate, it is overwritten by this new one.

Step 1 Enable the CG feature on the new CG (see the "Setting a Concentrator as a Certificate Generator" section on page 10-3).

Step 2 At the prompt, enter:

`certificate cg import` *`password`*

Where *password* matches the password used when you exported the bundle.

Step 3 Paste the bundle at the prompt, add a period (**.**) on a separate line after the request, and press the **Enter** key.

If the import is successful, you see the following message:

```
PKCS12 Import Successful
```

Requesting a Server Certificate

To request a server certificate for a non-CG concentrator, complete the steps in the following sections. A server certificate allows clients and tunnel peers with root certificates to authenticate the concentrator.

Note For a valid server certificate, you must complete the following steps. For example, you cannot copy another concentrator's certificate and paste it into your concentrator; the certificate does not work.

Generating a Certificate Request

To request the certificate, follow these steps.

Note We recommend running the commands in this procedure on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Step 1 On the concentrator that needs the certificate, enter the following command at the prompt:

certificate generate request *key_length* [**locality** *city*] [**state** *state*] [**country** *country_code*] [**organization "***organization_name***"**] [**commonname "***common_name***"**] [**days** *validity_period*]

See Table 10-1 on page 10-5 for a description of the options.

For example:

```
certificate generate request 1024 locality sanjose state ca country US
organization "Cisco" commonname "Cisco Server"
```

Step 2 Wait for the request to be fulfilled.

Depending on the key length, the concentrator can take up to an hour to create the request in a background process. To determine if the generator is finished (idle) or still generating (busy), enter the following command:

```
show certificate generator
```

The system log also documents a completed request with a Notice level message. See the "Setting Logging Options" section on page 3-5 for more information on viewing the log.

Step 3 When the concentrator is finished generating, view the request by entering:

```
certificate request show
```

The console displays the request text in PKCS #10 and PEM format, as in the following example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDExBCb2IncyBJbnRyYVBvcnQyMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDfEX5KdJyxKFJn2b0VLDd96YmYZSz9kyayugaW
aWacZpOT4njtiSohK4OYavJkoJBuVjjiozfS03zA1U21xepwQqrzG0RZUKCPCnE0
sxIpGo0bcMQFGwmKQ5f6Oj1QKzy117EwQjvd8CciCM8ae+ugLlGd7eIj6LAcrcbM
Z9lIVQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEALJndSfRXsuzqd4p+fCPrDacF
BX8LnLpiw4hFX8Z4quSULAp2F6Sz3AUIe3muxhWpQkrYriT7ki5tD7nzhLWkzwGE
aiRlhosfBBVA/5Wk/KXP9k8AyfHDSDdVGQRV19Qgu2ggmQI1P2tsJ6zM5GMr+9/T
389ZA4HO9kt8DA658w0=
-----END CERTIFICATE REQUEST-----
```

Step 4 Select the text, making sure to select the entire block, including the last carriage return.

Selecting the last carriage return might require you to select the area in front of the prompt that follows the text.

Step 5 Copy the request text to the clipboard or into a text file in preparation for requesting a certificate from a CA or CG.

Requesting a Certificate from a Certificate Authority

To request a server certificate from a CA, provide the request to the CA according to the CA's requirements. Entrust/PKI requires Entrust/VPNConnector in which to paste certificate requests.

See the "Installing a Certificate on a Concentrator" section on page 10-14 to install the server certificate.

Requesting a Certificate from a Certificate Generator

To request a certificate from a CG, follow these steps.

Note We recommend running the commands in this procedure on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Step 1 On the CG, enter:

```
certificate request import
```

The system prompts you to paste the request.

Step 2 Paste the request at the prompt, adding a period (**.**) on a separate line after the request, and press the **Enter** key.

Step 3 To view the identifier for the request, enter:

```
certificate request pending
```

The console shows a list of requests, each with an identifying number, as in the following example:

```
Id  Requested By          Request Date
1   /CN=Goldy's VPN 5000  Feb 17 15:02:35 2000 GMT
2   /CN=Bob's VPN 5000    Feb 18 11:05:27 2000 GMT
```

Note the identifier, and approve or reject the request:

- To reject the request, enter:

  certificate request reject *identifier*

- To approve the request, enter:

  certificate request approve *identifier* [*days*]

  Where *days* overrides the validity period in the request.

  The console immediately displays the server certificate text in PKCS #7 and PEM format, as in the following example:

```
-----BEGIN PKCS7-----
MIAGCSqGSIb3DQEHAqCAMIIB1wIBATEAMIAGCSqGSIb3DQEHAQAAoIIBvTCCAbkw
ggFjoAMCAQICAQEwDQYJKoZIhvcNAQEEBQAwZjELMAkGA1UEBhMCQVUxETAPBgNV
BAgTCENvbG9yYWRvMRAwDgYDVQQHEwdCb3VsZGVyMRswGQYDVQQKExJDb21wYXRp
YmxlIFN5c3RlbXMxFTATBgNVBAMTDEludHJhcG9ydCBDQTAeFw05OTEyMDEwMDEx
MzFaFw05OTEyMzEwMDExMzFaMGYxCzAJBgNVBAYTAkFVMREwDwYDVQQIEwhDb2xv
cmFkbzEQMA4GA1UEBxMHQm91bGRlcjEbMBkGA1UEChMSQ29tcGF0aWJsZSBTeXN0
ZW1zMRUwEwYDVQQDEwxJbnRyYXBvcnQgQ0EwWjALBgkqhkiG9w0BAQEDSwAwSAJB
AKcGdw1H2Mr7ZMIflx8rWzb2S56WimZtO4mxcAoQa7yezyZ8cXN+o+QkvxsTLSsM
3YRHWE4voI6hIJbOG1gnUD0CAwEAATANBgkqhkiG9w0BAQQFAANBABnW5Np3La8t
Z5P6Od3BDX7BKbefLMJXoDPN31cbAqy40L/WVwKKWGoD/M+QTrHKMt+T1RhlTr+Z
Gl3QT4+6wPwxAAAAAAA=
-----END PKCS7-----
```

Step 4 If you approved the request, select the text, making sure to select the entire block, including the last carriage return.

Selecting the last carriage return might require you to select the area in front of the prompt that follows the text.

Step 5 Copy the certificate text to the clipboard or into a text file in preparation for installing it on the concentrator.

Installing a Certificate on a Concentrator

This section describes how to install a root or server certificate on the concentrator. You can install one root and one server certificate on a concentrator.

For information about copying the root certificate from a CG, see the "Distributing the Root Certificate" section on page 10-6. For information about obtaining a server certificate, see the "Requesting a Server Certificate" section on page 10-10.

Note Some CAs allow you to create a combined server and root certificate. The following steps work for combined or single certificates.

To install a server certificate or a root certificate on a non-CG concentrator, follow these steps.

Note We recommend running the commands in this procedure on a directly connected console. Because the input and output of the command contains a large amount of text, a Telnet session might not handle the text properly.

Step 1 On the concentrator that requires a certificate, enter:

```
certificate import
```

The system prompts you to paste the PEM-formatted X.509 or PKCS #7 certificate.

Note If you used a CA, make sure the header and footer of the certificate uses one of the following formats:

```
-----BEGIN PKCS7-----
...
-----END PKCS7-----
```

or

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Step 2 Copy the certificate from a CA or CG and paste the certificate at the prompt.

Step 3 Add a period (**.**) on a separate line after the request, and press the **Enter** key.

The concentrator shows the certificate text and prompts you to approve the import.

Managing Certificates

The following sections describe how to verify, remove, and view certificates.

Verifying a Server Certificate

For a concentrator with both a root certificate and a server certificate, you can verify that the server certificate is signed by the root certificate and has not expired by following these steps:

Step 1 Make sure the time is set on the concentrator according to the "Setting the Time" section on page 3-2.

Step 2 Enter the following command at the prompt:

```
certificate verify
```

Either a message informing you of a failure and the reason for the failure or a message confirming the successful verification appears.

Viewing Certificate Details

You can view basic information about installed certificates or you can view detailed information about a certificate.

- View available certificates by entering the following command at the prompt:

  show certificate installed

  The console shows information about each certificate, as in the following example.

```
Root Certificate:
    Serial Number: 77:37:3a:33:37:3a:33:61:3a:33:33:3a:33:37:3a:33
    Issuer: C=US,O=Cisco Systems,OU=SLP BU,L=Boulder,ST=Colorado
    Subject: C=US,O=Cisco Systems,OU=SLP BU,L=Boulder,ST=Colorado
    Validity
        Not Before: Apr 21 00:00:00 2000 GMT
        Not After : Apr 20 23:59:59 2005 GMT
    MD5 Fingerprint: B0:DD:DD:DE:13:29:3C:54:95:F7:BD:5C:B7:0C:CA:E6

Server Certificate:
    Serial Number: 37:37:3a:33:37:3a:33:61:3a:33:33:3a:33:37:3a:33
    Issuer: C=US,O=Cisco Systems,OU=SLP BU,L=Boulder,ST=Colorado
    Subject: CN=IntraPortCarrier_A5C5C600
    Validity
        Not Before: Apr 24 00:00:00 2000 GMT
        Not After : Apr 24 23:59:59 2001 GMT
    MD5 Fingerprint: 2A:93:5F:02:7A:9D:68:80:63:8E:29:68:DA:5A:9A:BD
```

- View additional certificate details by entering the following command at the prompt:

  show certificate details {**root** | **server**}

  The console displays the certificate details for the selected certificate type. The following example shows a typical display:

```
Server Certificate:
    Version: 3 (0x2)
    Serial Number: 33:33:3a:33:33:3a:33:61:3a:33:33:3a:33:33:3a:33

    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=US,O=Cisco Systems,OU=SLP BU,L=Boulder,ST=Colorado
    Subject: CN=IntraPortCarrier_A5C5C600
    Validity
        Not Before: Apr 24 00:00:00 2000 GMT
        Not After : Apr 24 23:59:59 2001 GMT
```

```
MD5 Fingerprint: 2A:93:5F:02:7A:9D:68:80:63:8E:29:68:DA:5A:9A:BD
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: md5WithRSAEncryption
    01:0c:40:40:fb:84:e3:eb:49:f4:0b:da:69:f7:6d:cd:d1:16:
    ae:e9:d1:a9:f3:a1:b2:03:33:a8:3a:19:a1:4c:cc:1b:5e:e1:
    e9:a5:06:6b:02:c1:5d:6a:93:a2:60:a3:47:6c:5b:2b:2a:91:
    9f:30:a7:76:77:ba:d4:84:d8:89:bd:b9:31:d2:1a:82:52:37:
    14:24:4f:a5:23:bb:65:fb:3e:96:7e:17:50:87:de:7d:dd:a0:
    21:30:80:4f:0b:26:87:7b:1a:84:a3:df:89:78:c9:dc:80:87:
    cd:a4:d8:f2:a2:e0:4b:0e:59:dd:36:59:3d:59:8f:d0:7e:b2:
    2f:97
```

Sample Configurations

This appendix includes the following sample configurations for the Cisco VPN 5000 concentrators:

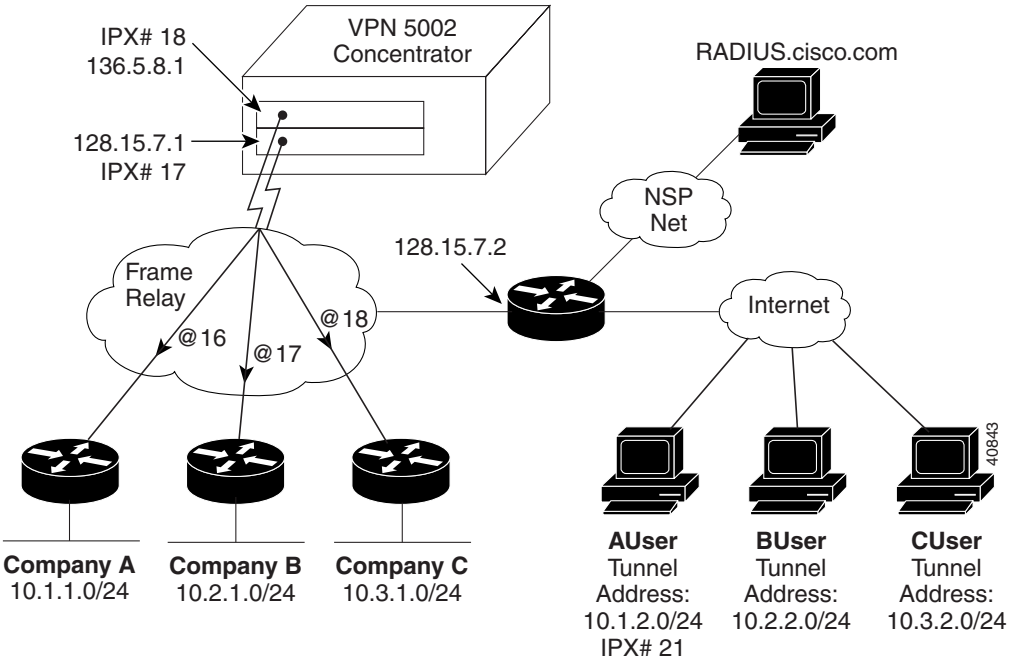
- Frame Relay Configuration
- Proprietary IPSec LAN-to-LAN Tunnel Configuration
- Remote Users, Offices, and a Central Site Configuration
- Standard IPSec Tunnel with Cisco IOS Device Configuration

Each VPN 5000 configuration is in text file format, with section heads in brackets.

Frame Relay Configuration

You can keep customer networks secure by binding each customer's VPN group to their Frame Relay DLCI. Figure A-1 shows three customers connecting to the same concentrator HSSI or DS3 port over Frame Relay. Company A uses IP and IPX. User authentication is done through a RADIUS server.

Figure A-1 VPN Groups Bound to Frame Relay DLCIs




```
[ General
Password                  = hello
DeviceName                = mydevice

[ Domain Name Server ]
PrimaryServer             = 209.165.201.29

[ Time Server ]
Enabled                   = On
ServerAddress             = 209.165.201.30
BindTo                    = WAN 0:0

[ Logging ]
Level                     = Debug
LogToAuxPort              = On

[ Link Config WAN 0:0 ]
Mode                      = FrameRelay
```

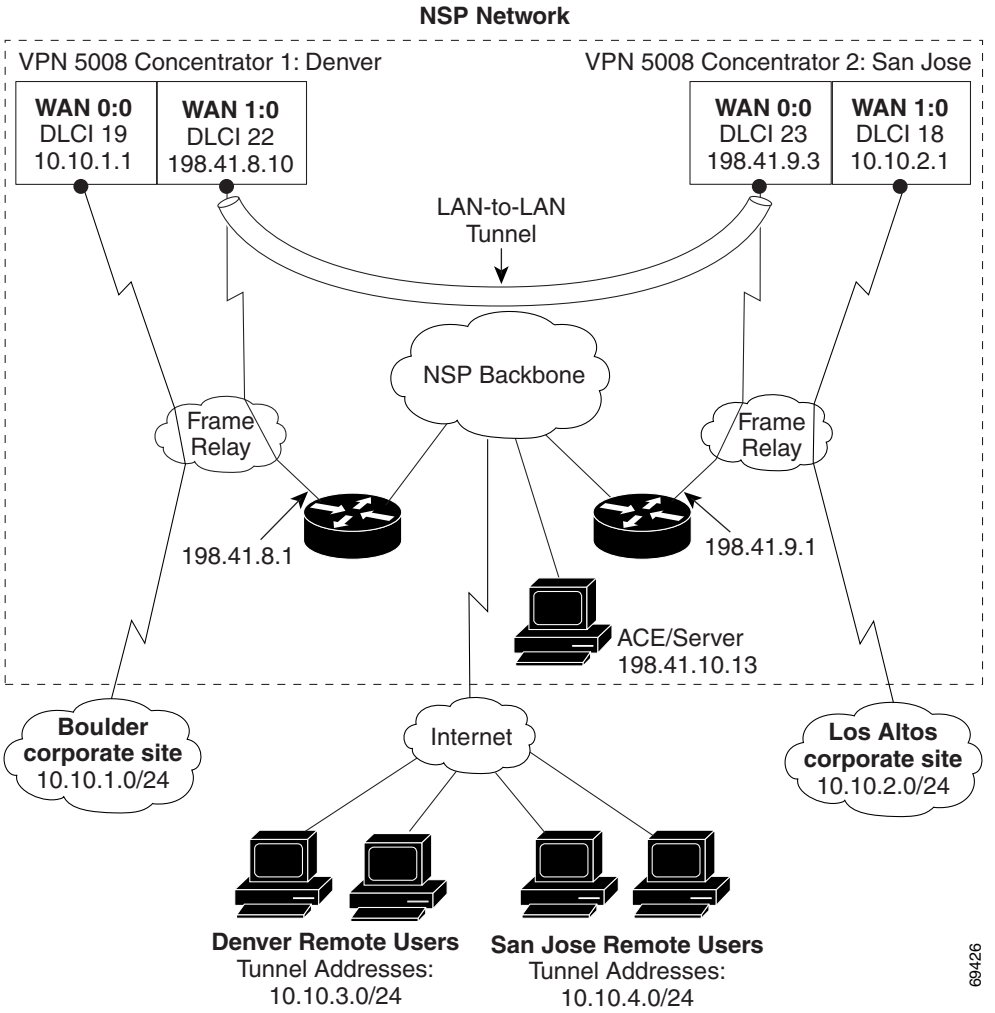
```
[ Link Config WAN 1:0 ]
Mode                    = FrameRelay

[ IKE Policy ]
Protection              = MD5_DES_G1

[ IP WAN 0:0 ]
Mode                    = Routed
IPAddress               = 136.5.8.1
SubnetMask              = 255.255.255.0
RIPVersion              = V2
Numbered                = On

[IP WAN 1:0]
Mode                    = Routed
IPAddress               = 128.15.7.1
SubnetMask              = 255.255.255.0
RIPVersion              = V2
Numbered                = On

[ IPX WAN 0:0 ]
Mode                    = Routed
Numbered                = On
Net                     = 18

[ IPX WAN 1:0 ]
Mode                    = Routed
Numbered                = On
Net                     = 17

[ Radius ]
PrimAddress             = radius.cisco.com
Secret                  = Myradiussecret
BindTo                  = WAN 0:0
Accounting              = On
Authentication          = On
ChallengeType           = PAP
PAPAuthSecret           = MyPAPSecret

[ IP Static ]
# Default route
0.0.0.0 0.0.0.0 128.15.7.2 1
```

```
[ VPN Group "CompanyA" ]
Transform                = esp(3des,md5)
VPNgroupDLCI             = 16
MaxConnections           = 254
LocalIPNet               = 10.1.2.0/24
IPNet                    = 10.1.1.0/24
LocalIPXNet              = 21

[ VPN Group "CompanyB" ]
Transform                = esp(3des,md5)
VPNgroupDLCI             = 17
MaxConnections           = 254
LocalIPNet               = 10.2.2.0/24
IPNet                    = 10.2.1.0/24

[ VPN Group "CompanyC" ]
Transform                = esp(3des,md5)
VPNgroupDLCI             = 18
MaxConnections           = 254
LocalIPNet               = 10.3.2.0/24
IPNet                    = 10.3.1.0/24
```

Proprietary IPSec LAN-to-LAN Tunnel Configuration

Figure A-2 shows an example VPN with two corporate sites connected to an NSP at two geographical locations.

Figure A-2 LAN-to-LAN Tunnel



Remote users who connect to their server can access the networks at both corporate sites. For example:

1. A Denver user connects to the Internet.
2. The user then uses the VPN 5000 client to connect to the Denver concentrator.
3. Any traffic destined for the Boulder corporate site is sent over Frame Relay.
4. Any traffic destined for the Los Altos corporate site is sent over the LAN-to-LAN tunnel to the San Jose concentrator.
5. The traffic is then sent over Frame Relay to the Los Altos site.

The following sections show the configuration settings for the Main CVC and Company CVC for Concentrator 1 and Concentrator 2.

Cisco VPN 5008 Concentrator 1 Configuration for Proprietary IPSec Tunnel

The following configuration applies to the Denver VPN 5008 concentrator 1 connected to the Boulder site (see Figure A-2).

```
[ General ]
Password                = hello
DeviceName              = DenverVPN
IPRouteFilters          = Private

[ IP Route Filter Private ]
# Prevents private 10.0.0.0 networks from
# being advertised out WAN 1:0
deny 10.0.0.0/8 out from wan 1:0
permit 0.0.0.0

[ Link Config WAN 0:0 ]
Mode                    = FrameRelay

[ Link Config WAN 1:0 ]
Mode                    = FrameRelay

[ IKE POLICY ]
Protection              = MD5_3DES_G1

[ Logging ]
Level                   = Debug
LogToAuxPort            = On
```

```
[ Domain Name Server ]
PrimaryServer            = 198.41.10.14

[ Time Server ]
Enabled                  = On
ServerAddress            = 198.41.10.15
BindTo                   = WAN 1:0

[ SecurID ]
PrimaryServer            = 198.41.10.13
BindTo                   = WAN 1:0
Enabled                  = On

[ IP Static ]
# Default route
0.0.0.0 0.0.0.0 198.41.8.1 1

[ IP WAN 1:0 ]
Mode                     = Routed
IPAddress                = 198.41.8.10
SubnetMask               = 255.255.255.0
Numbered                 = On
PointtoPointFrame        = On
InterfaceDLCI            = 22
OSPFenabled              = On
OutFilters               = Private
OSPFAreaID               = 0

[ IP Filter Private ]
# Prevents traffic from the private networks
# from exiting out WAN 1:0
deny 10.0.0.0/8 0.0.0.0 ip
permit 0.0.0.0 0.0.0.0 ip

[ IP WAN 0:0 ]
Mode                     = Routed
OSPFEnabled              = On
Numbered                 = On
IPAddress                = 10.10.1.1
SubnetMask               = 255.255.255.0
OSPFAreaID               = 1
PointtoPointFrame        = On
InterfaceDLCI            = 19
```

```
[ VPN Group "Denver" ]
Transform                = ESP(MD5,3DES)
MaxConnections           = 254
LocalIPNet               = 10.10.3.0/24
# Supernet the destination networks for future expansion.
# IPNet Routes all traffic for 10.10.0.0 through 10.10.255.255
IPNet                    = 10.10.0.0/16
SecurIDRequired          = On
SecurIDName              = On

[ VPN Users ]
#Use a single user name for the group to assign
#the group name.
User Config=Denver SharedKey=mykey

[ Tunnel Partner VPN 0:1 ]
Partner                  = 198.41.9.3
BindTo                   = WAN 1:0
Certificates             = On
Transform                = ESP(MD5,3DES)
Mode                     = Main

[ IP VPN 0:1 ]
Mode                     = Routed
OSPFenabled              = On
OSPFAreaID               = 1
Numbered                 = Off

[ IP Static ]
# Default route to a router on the company's private network
0.0.0.0 0.0.0.0 10.10.1.2 1
```

Cisco VPN 5008 Concentrator 2 Configuration for Proprietary IPSec Tunnel

The following configuration applies to the San Jose VPN 5008 concentrator 2 connected to the Los Altos site (see Figure A-2).

```
[ General ]
Password                 = hello
DeviceName               = SanJoseVPN
IPRouteFilters           = Private
```

```
[ IP Route Filter Private ]
# Prevents private 10.0.0.0 networks from
# being advertised out WAN 0:0
deny 10.0.0.0/8 out from wan 0:0
permit 0.0.0.0

[ IP WAN 0:0 ]
Mode                    = Routed
IPAddress               = 198.41.9.3
SubnetMask              = 255.255.255.0
OSPFenabled             = On
OSPFAreaID              = 0
PointtoPointFrame       = On
InterfaceDLCI           = 23
Numbered                = On
OutFilters              = Private

[ IP Filter Private ]
# Prevents traffic from the private networks
# from exiting out WAN 0:0
deny 10.0.0.0/8 0.0.0.0 ip
permit 0.0.0.0 0.0.0.0 ip

[ IP WAN 1:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 10.10.2.1
OSPFEnabled             = On
Numbered                = On
OSPFAreaID              = 1
PointtoPointFrame       = On
InterfaceDLCI           = 18

[ Link Config WAN 0:0 ]
Mode                    = FrameRelay

[ Link Config WAN 1:0 ]
Mode                    = FrameRelay

[ IKE POLICY ]
Protection              = MD5_DES_G1

[ Logging ]
Level                   = Debug
LogToAuxPort            = On

[ Domain Name Server ]
PrimaryServer           = 198.41.10.14
```

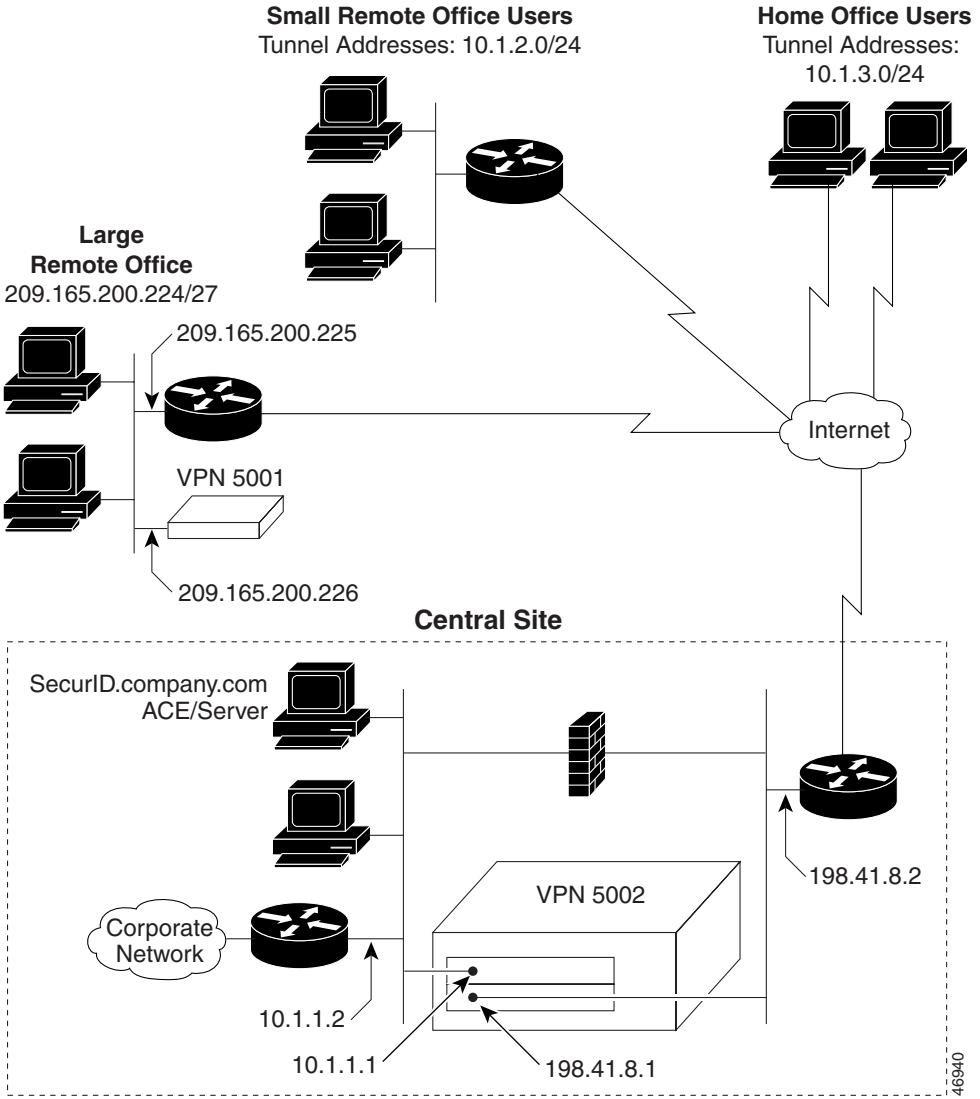
```
[ Time Server ]
Enabled                  = On
ServerAddress            = 198.41.10.15
BindTo                   = WAN 0:0

[ SecurID ]
PrimaryServer            = 198.41.10.13
BindTo                   = WAN 0:0
Enabled                  = On

[ VPN Group SanJose ]
Transform                = ESP(MD5,3DES)
MaxConnections           = 254
LocalIPNet               = 10.10.4.0/24
IPNet                    = 10.10.1.0/24
IPNet                    = 10.10.2.0/24
SecurIDRequired          = On
SecurIDName              = On

[ VPN Users ]
#Use a single user name for the group to assign the group name.
User Config=SanJose SharedKey=mykey

[ Tunnel Partner VPN 0:1 ]
Partner                  = 198.41.8.10
BindTo                   = WAN 0:0
Certificates             = On
Transform                = ESP(MD5,3DES)
Mode                     = Main

[ IP VPN 0:1 ]
Mode                     = Routed
OSPFenabled              = On
OSPFAreaID               = 1
Numbered                 = Off

[ IP Static ]
# Default route to a router on the company's private network
0.0.0.0 0.0.0.0 10.10.2.2 1
```

Remote Users, Offices, and a Central Site Configuration

Figure A-3 shows the VPN 5002 concentrator at the central site with remote users and remote offices connecting over the Internet. A larger remote office includes a VPN 5001 concentrator that connects to the central site over the Internet using a LAN-to-LAN tunnel. User authentication is done using a SecurID system and a **VPN Users** list.

Note Remote office users cannot communicate with other remote users, only with the central site.

Figure A-3 Enterprise Network



Cisco VPN 5002 Concentrator at the Central Site Configuration

The following sample configuration is in text file format.

```
[ General
Password                = hello
DeviceName              = mydevice
# Sends all VPN traffic through Ethernet 1:0 to the upstream router:
VPNGateway              = 198.41.8.2

[ IP Ethernet 0:0 ]
Mode                    = Routed
IPAddress               = 10.1.1.1
SubnetMask              = 255.255.255.0
RIPVersion              = V2

[ IP Ethernet 1:0 ]
Mode                    = Routed
IPAddress               = 198.41.8.1
SubnetMask              = 255.255.255.0

[ IKE POLICY ]
Protection              = MD5_DES_G1

[ Logging ]
Level                   = Debug
LogToAuxPort            = On

[ Domain Name Server ]
PrimaryServer           = 10.1.1.3

[ Time Server ]
Enabled                 = On
ServerAddress           = 10.1.1.4
BindTo                  = Ethernet 0:0

[ Tunnel Partner VPN 1:1 ]
# For "VPN 1:1," the first number represents the slot that
# processes the traffic. The second number is a unique identifier for
# this tunnel.
Partner                 = 209.165.200.226
BindTo                  = Ethernet 1:0
SharedKey               = Mysecret
Transform               = AH(MD5)+ESP(3DES)
```

```
[ IP VPN 1:1 ]
Mode                    = Routed
RIPVersion              = V2
Numbered                = Off

[ VPN Group SmallOffice ]
Transform               = ESP(MD5,3DES)
LocalIPNet              = 10.1.2.0/24
IPNet                   = 10.1.1.0/24
SecurIDRequired         = On
SecurIDName             = On

[ VPN Group RemoteUsers ]
Transform               = ESP(MD5,3DES)
LocalIPNet              = 10.1.3.0/24
IPNet                   = 10.1.1.0/24
SecurIDRequired         = On
SecurIDName             = On

[ SecurID ]
Enabled                 = On
PrimaryServer           = SecurID.company.com
BindTo                  = Ethernet 0:0

[ VPN Users ]
#Use a single user name for each group to assign
#the group name.
AUser Config=SmallOffice SharedKey=Amykey1
BUser Config=RemoteUsers SharedKey=Bmykey1

[ IP Static ]
# Default route
0.0.0.0 0.0.0.0 10.1.1.2 1
```

Cisco VPN 5001 Concentrator at the Large Remote Office Configuration

The following sample configuration is in text file format.

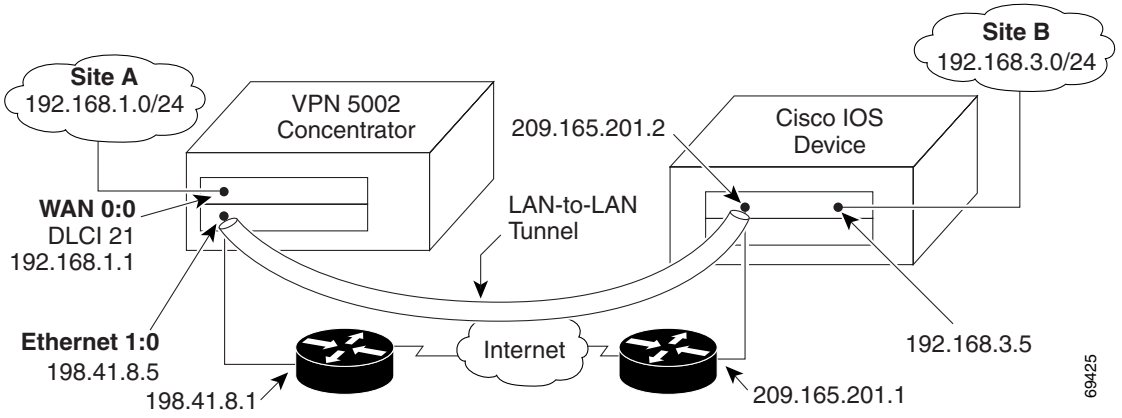
```
[ General ]
Password                = hello
DeviceName              = mydevice
```

```
[IP Ethernet 0]
Mode                    = Routed
IPAddress               = 209.165.200.226
SubnetMask              = 255.255.255.248
RIPVersion              = V2

[ IP Ethernet 1 ]
Mode                    = Off

[ IKE POLICY ]
Protection              = MD5_DES_G1

[ Logging ]
Level                   = Debug
LogToAuxPort            = On

[ Tunnel Partner VPN 1 ]
Partner                 = 198.41.8.1
BindTo                  = Ethernet 0
SharedKey               = "Mysecret"
Transform               = AH(MD5)+ESP(3DES)

[ IP VPN 1 ]
Mode                    = Routed
RIPVersion              = V2

[ IP Static ]
# Default route
0.0.0.0 0.0.0.0 209.165.200.225 1
```

Standard IPSec Tunnel with Cisco IOS Device Configuration

Figure A-4 shows a standard IPSec tunnel connecting Sites A and B over the Internet. Site A uses a VPN 5002 concentrator while Site B uses a Cisco IOS device that supports IPSec.

Figure A-4 Standard IPSec Tunnel with IOS



Cisco VPN 5002 Concentrator Standard IPSec Tunnel Configuration

The following configuration shows how to configure a VPN 5002 concentrator to interoperate with a Cisco IOS device (see Figure A-4).

```
[ General ]
Password                = hello
DeviceName              = mydevice

[ IP Ethernet 1:0 ]
SubnetMask              = 255.255.255.0
IPAddress               = 198.41.8.5
Mode                    = Routed

[ IKE Policy ]
# This value must match the Cisco IOS crypto isakmp policy command
# for hash (md5 or sha). IOS uses DES and G1 by default.
Protection              = MD5_DES_G1

[ Time Server ]
Enabled                 = On
ServerAddress           = 192.168.10.57
BindTo                  = WAN 0:0
```

```
[ IP WAN 0:0 ]
Mode                    = Routed
RIPVersion              = V2
Numbered                = On
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1
PointtoPointFrame       = On
InterfaceDLCI           = 21

[ Tunnel Partner VPN 0:1 ]
BindTo                  = Ethernet 1:0
# The Transform keyword must match a transform in the Cisco IOS
# crypto ipsec transform-set command.
Transform               = ESP(MD5,DES)
SharedKey               = letmein
Mode                    = Main
KeyManage               = Initiate
Partner                 = 209.165.201.2
LocalAccess             = 192.168.1.0/24
Peer                    = 192.168.3.0/24

[ Domain Name Server ]
PrimaryServer           = 192.168.10.56

[ IP Static ]
# Default route to a router on the company's private network
0.0.0.0 0.0.0.0 192.168.1.2 1
```

Cisco IOS Device Standard IPSec Tunnel Configuration

The following sample shows the output of the **more** command on a Cisco IOS device. See the "Cisco VPN 5002 Concentrator Standard IPSec Tunnel Configuration" section on page A-16 for comments about values that must match between the two devices.

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco-3640
!
enable password letmein
!
!
!
!
!
ip subnet-zero
ip cef
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key letmein address 198.41.8.1
!
!
crypto ipsec transform-set compatible esp-des esp-md5-hmac
!
crypto map compatible-crypt 1 ipsec-isakmp
 set peer 198.41.8.1
 set transform-set compatible
 match address 101
!
!
!
!
!
!
!
```

```
!
interface FastEthernet0/0
 ip address 209.165.20.2 255.255.255.224
 duplex auto
 speed auto
 crypto map compatible-crypt
!
interface FastEthernet0/1
 ip address 192.168.3.5 255.255.255.0
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.1
no ip http server
!
access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
tftp-server slot0
tftp-server system
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password letmein
 login
!
end
```

Cisco Systems

PART 4

Troubleshooting and Maintenance

APPENDIX B

Installing the Software and Configuration

This appendix describes how to install or upgrade the system software on the Cisco VPN 5000 concentrator and how to download or back up a text configuration file in Flash memory.

Downloading the Software to the Concentrator

The VPN 5002 and VPN 5008 concentrators use the same software file; the VPN 5001 concentrator uses a different software file.

You can download the software:

- With TFTP using the concentrator as a TFTP server
- With TFTP using the concentrator as a TFTP client
- With XModem on the console port

Using the Concentrator as a TFTP Server to Download Software

To download the software, follow these steps:

Step 1 Enable TFTP by entering the following command at a console or Telnet session:

tftp enable [*timeout*] [*TFTP_client_IP_address*]

- *Timeout*—The amount of time in seconds that TFTP is enabled after you enter the command. The default is 60 seconds.
- *TFTP_client_IP_address*—The IP address allowed to connect with TFTP to the concentrator. If you used Telnet to enter this command, the default is the Telnet host IP address. You must enter a value if you are using a console connected directly to the console port.

Step 2 Use a TFTP client on your PC to transfer the software file in binary mode before the **tftp enable** command times out.

The software file name can be any name. After you download the file, the concentrator restarts.

Note If you see the message, "Incorrect filename," on your TFTP client, you forgot to set the file type to binary.

Using the Concentrator as a TFTP Client to Download Software

To download the software from a TFTP server, follow these steps:

Step 1 Copy the software file into your TFTP server download directory (usually the tftpboot directory).

The software file name can be any name.

Step 2 On the concentrator, enter the following command at the prompt:

tftp get code *TFTP_server remote_filename*

- *TFTP_server*—The TFTP server IP address.
- *Remote_filename*—The software file name. The filename can include a directory path. For example:

```
tftp get code 10.1.1.1 /vpn5002_a/vpn-5002-5008-5.2.23-3des.dld
```

After you download the file, the concentrator restarts.

Downloading Software Through the Console Port

If the concentrator interface is not available for TFTP downloads, you can use XModem on the console port to download the software from an attached PC. To perform the download, follow these steps:

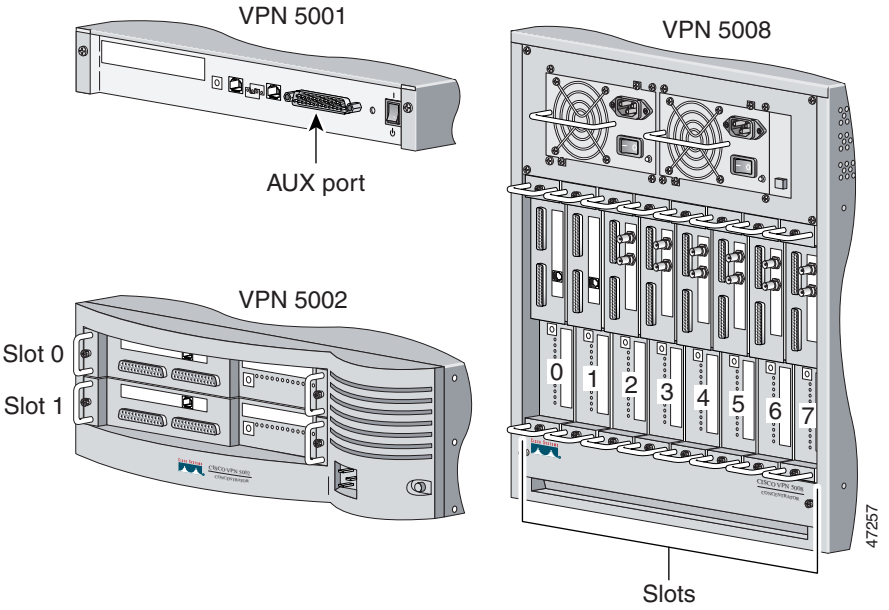
Step 1 Copy the software to the PC you want to connect to the console port.

Note If you are using HyperTerminal on Windows, we recommend that you browse to the file before initiating the transfer, then cancel the action. After you browse to the file, the file is the default location for the rest of the session. This action helps minimize the time to start the download after setting the VPN 5000 concentrator into receive mode so that a timeout does not occur.

Step 2 Connect the provided console cable (a standard RS-232 cable) from your PC to one of the following ports (Figure B-1):

- VPN 5002 or 5008—Console port on the ESP card in slot 0
- VPN 5001—AUX port

Figure B-1 Slot Numbering



Step 3 Set the terminal emulator to use the following settings:

- 9600 Baud
- 8 bits
- No parity
- 1 stop bit
- No flow control

Step 4 Set the file transfer method to:

- Xmodem-1K
- Binary
- 16-bit CRC mode

Step 5 Start the download by following the steps for one of the following options:

- To download software from the VPN 5000 concentrator prompt (available after starting up in the currently installed software):

a. At the prompt, enter:

set baud rate *baud*

Where *baud* is the rate at which to download the image. We recommend 115200 or the fastest rate supported by your terminal emulator.

The concentrator prompts you to set the PC terminal emulator baud rate to match the entered value.

b. Set the terminal emulator to the corresponding rate.

Note If you are using HyperTerminal on Windows, you must disconnect the COM connection before you are allowed to change the baud rate. You must reconnect for the new baud rate to take effect.

c. Press any key.

If you set the rates correctly, you see a readable confirmation string.

d. At the concentrator command line prompt, enter:

sys rxmodem

- To download software from the Boot-Block Downloader prompt (available if there is no software installed, or if you set the test switch to 3):

a. At the prompt, enter:

rxmodem *baud*

Where *baud* is the rate at which to download the image. We recommend 115200 or the fastest rate supported by your terminal emulator.

The concentrator prompts you to set the PC terminal emulator baud rate to match the entered value.

b. Set the terminal emulator to the corresponding rate.

Note If you are using HyperTerminal on Windows, you must disconnect the COM connection before you are allowed to change the baud rate. You must reconnect for the new baud rate to take effect.

c. Press any key.

If you set the rates correctly, you see a readable confirmation string.

Step 6 Initiate the transfer in the terminal emulator.

Step 7 The terminal emulator displays the file transfer progress. When finished, the concentrator reboots automatically.

Step 8 Reset the terminal emulator port rate to 9600 baud.

Copying a Text Configuration File

You can copy the configuration file to or from the concentrator by using the concentrator as a TFTP server or as a TFTP client. The following sections describe both methods.

Note The configuration space in Flash memory is 64 KB.

Using the Concentrator as a TFTP Server to Copy the Configuration

To download or upload the configuration, follow these steps:

Step 1 Enable TFTP by entering the following command at a console or Telnet session:

tftp enable [*timeout*] [*TFTP_client_IP_address*]

- *Timeout* is the amount of time in seconds that TFTP is enabled after entering the command. The default is 60 seconds.
- *TFTP_client_IP_address* is the IP address allowed to connect using TFTP to the concentrator. If you used Telnet to enter this command, the default is the Telnet host IP address. You must enter a value if you are using a console connected directly to the console port.

Step 2 Use a TFTP client on your PC to copy the configuration file in ASCII mode before the **tftp enable** command times out.

To **put** the configuration on the concentrator, specify the filename as vpn5002_8.cfg (for the VPN 5002 or 5008) or vpn5001.cfg (for the VPN 5001). After you download the configuration, the concentrator restarts.

Using the Concentrator as a TFTP Client to Copy the Configuration

To download or upload the configuration to or from a TFTP server, follow these steps:

Step 1 To download, copy the configuration file into your TFTP server file directory (usually the tftpboot directory).

To upload a file to some TFTP servers, a file with the same name must already exist, and its permissions must allow you to write over it.

Step 2 On the concentrator, enter the following command at the prompt:

tftp {**get** | **put**} **config** *TFTP_server remote_filename*

- **get**—Downloads the file to the concentrator. After you download the configuration, the concentrator restarts.
- **put**—Uploads the file to the TFTP server file directory.
- *TFTP_server*—The TFTP server IP address.
- *remote_filename*—The filename on the TFTP server. To **get** a configuration, specify the filename as vpn5002_8.cfg (for the VPN 5002 or 5008) or vpn5001.cfg (for the VPN 5001). To **put** a configuration, you can specify any fileneme to save it on the TFTP server. The filename can include a directory path. For example:

```
tftp get config 10.1.1.1 /vpn5002_a/vpn5002_8.cfg
```

APPENDIX C

Recovering from a Software Failure

If the Cisco VPN 5000 concentrator does not boot, does not accept new software, or has corrupted software or configurations, you can use the test switch to allow you to reboot and download new software.

For the VPN 5002 or 5008 concentrator, use the switch on the ESP card in slot 0. For the VPN 5001, use the switch on the back of the unit. When you download new software to slot 0, the system overwrites the software on all other ESP cards. If a card in another slot malfunctions, you can use its switch to erase its software, after which the card downloads the software from slot 0.

Caution Contact technical support before using the test switch. The test switch can erase your software and configuration files, which can result in a loss of service and unrecoverable configurations.

Refer to Table C-1 for a description of each test switch setting, and set the switch to a number using a small flat-blade screwdriver in the arrow slot. Figure C-1 shows the test switch and slot.

Figure C-1 Test Switch

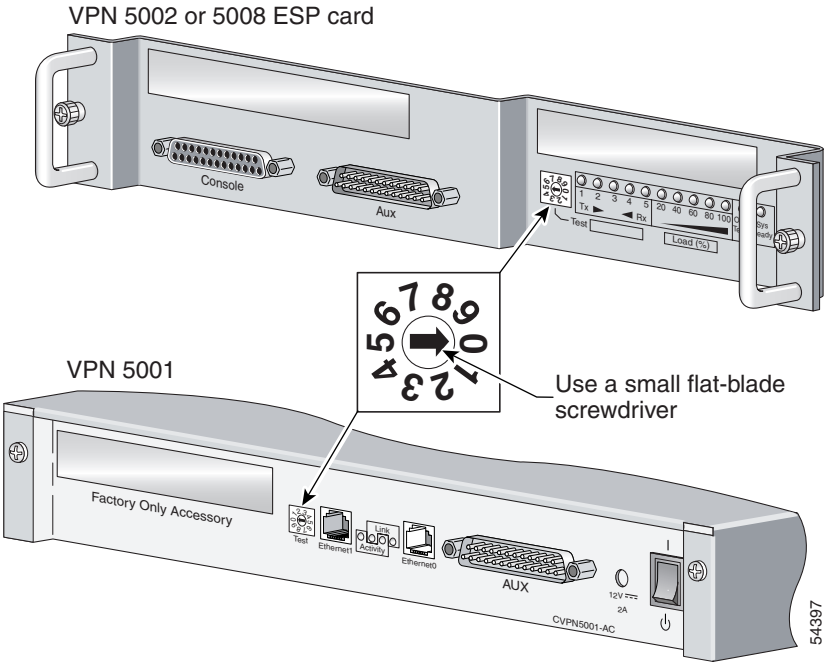


Table C-1 Test Switch Actions

Switch Setting	Description
0	Normal operation
1	Do not use
2	Do not use

Table C-1 Test Switch Actions (continued)

Switch Setting	Description
3	Boots a limited OS that you can use to set the IP address and download a new software version. This setting does **not** erase the OS or configuration files. For example: 1. Attach a console directly to the console port. 2. Set the switch to 3 and restart. 3. Set the switch back to 0. The following prompt appears after the system restarts: `VSR Downloader>` 4. Set the IP address of slot 0 (VPN 5002 or 5008) or port 0 (VPN 5001) using the following command: **setip** *address mask* [*gateway*] 5. Copy new software using TFTP according to the "Downloading the Software to the Concentrator" section on page B-1. The concentrator automatically has TFTP enabled with no timeout, and allows any TFTP client to connect and issue a TFTP put command. After you download the software, the system restarts using the new software.
4	Do not use

Table C-1 Test Switch Actions (continued)

Switch Setting	Description
5	Erases the OS and configuration in Flash memory, and then boots a limited OS that you can use to set the IP address and download a new software version. For example: **1.** Attach a console directly to the console port. **2.** Set the switch to 5 and restart. **3.** Wait approximately 45 seconds for the concentrator to complete the following steps according to the console: Erase code flash Erase configuration After erasing the code and configuration, the Ethernet or WAN TX LEDs begin strobing, and the following message appears on the console: `Reset rotary switch and restart device` **4.** Set the switch back to 0. The following prompt appears after the system restarts: `VSR Downloader>` **5.** Set the IP address of slot 0 (VPN 5002 or 5008) or port 0 (VPN 5001) using the following command: **setip** *address mask* [*gateway*] **6.** Copy new software using TFTP according to the "Downloading the Software to the Concentrator" section on page B-1. The concentrator automatically has TFTP enabled with no timeout, and allows any TFTP client to connect and issue a TFTP put command. After you download the software, the system reboots using the new software.

Table C-1 Test Switch Actions (continued)

Switch Setting	Description
6	Erases the configuration in Flash memory. The system uses the default settings in the OS. For example: 1. Set the switch to 6 and restart. 2. Set the switch back to 0 and restart.
7	Do not use
8	Boots only to the command line so you can edit the configuration. The concentrator does not load the configuration, so the concentrator does not establish network connectivity. However, if your configuration causes the system to stop responding, this switch allows you to make changes to the configuration. For example: 1. Set the switch to 8 and restart. 2. Set the switch back to 0. 3. Edit the configuration file normally and enter **`save`**. The system reboots normally.
9	Allows the **letmein** password for 5 minutes after each startup. For security purposes, limit access to the chassis to authorized personnel only. You can leave the setting at 9 permanently; it is the same as setting 0 except for the **letmein** password 5 minutes after startup. Your normal passwords also work during the initial 5 minutes.

PART 5

Reference

APPENDIX D

Syntax Conventions

This chapter describes the command syntax conventions for the Cisco VPN 5000 concentrator, including privileges, prompts, and command types.

Privileges

The VPN 5000 concentrator has *enabled* and *normal* modes. In normal mode, entered using the first system password, you can view tables and statistics, but cannot modify the configuration.

Enabled mode requires an additional password. You can enter enabled mode in the following ways:

- If you did not set an enabled password according to the **General** section, then the normal password enters enabled mode.
- If you entered a privileged command, you are prompted for the enabled password.
- Use the **enable** command.

If you do not use the command line for 5 minutes, enabled mode times out.

Prompts

Command line prompts inform you which mode you are in as well as which section and port your commands apply to. Table D-1 describes the prompts in the VPN 5000 software.

Table D-1 VPN 5000 Command Line Prompts

Prompts	Description
Privileges	
string>	Normal mode. The *string* depends on the section and port you are configuring. The prompt always ends with > for edit config modes, even though you are in enabled mode.
string#	Enabled mode. The *string* depends on the section and port you are configuring. The prompt always ends with > for edit config modes, even though you are in enabled mode.
**string*# **string*>	You have made changes to the configuration. The asterisk (*) stays until you use the **write** or **save** commands to write the configuration to Flash memory. The asterisk (*) does not display in edit config mode.
Strings	
device_name	Displays when you are not in any section. For example: `CiscoVPN_1#`
[*Section_Name*]	Displays when you are in a configuration section. All commands entered at this prompt apply to the section and port, number, or name. For example: `[ IP Ethernet 0:0 ]#`
Edit	Displays when you are in edit config mode for the entire configuration. The prompt always ends with >, even though you are in enabled mode. For example: `Edit>`

Table D-1 VPN 5000 Command Line Prompts (continued)

Prompts	Description
`Edit [ Section_Name ]`	Displays when you are in edit config mode for a section. The prompt always ends with >, even though you are in enabled mode. For example: `Edit [ IP Filter "ip-in" ]>`
`Append`	Displays when you are in edit config mode and you are appending a line to a section. The prompt always ends with >, even though you are in enabled mode. For example: `Append>`

Syntax Formatting

Depending on the command syntax, you might see a variety of symbols and font styles in this document. Table D-2 describes the syntax font styles and symbols used in this guide.

Table D-2 Syntax Font Styles and Symbols

Style or Symbol	Description
Boldface	Enter bold text exactly as shown.
Italics	Indicates a variable for which you supply the value. In contexts that do not allow italics, variables are enclosed in angle brackets (< >).
Plain text	Plain text represents the screen display, such as a prompt. Do not enter plain text as part of the command.
<variable>	Indicates a variable for which you supply values, in contexts where italics cannot be used.
[**x**]	Keywords in square brackets are optional.
[**x** | **y**]	Keywords in square brackets separated by vertical bars indicate an optional keyword with a choice between values.

Table D-2 Syntax Font Styles and Symbols (continued)

Style or Symbol	Description
{**x** | **y** | **z**}	A choice of required keywords appear in braces separated by vertical bars. You must select one.
[**x** {**y** | **z**}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to select one. If you do, you have some required choices.

Command Types

Manage the VPN 5000 software using configuration and management commands.

Configuration Command Description

Configuration commands (**configure** or **edit config)** allow you to configure a section, after which all further configuration commands apply to that section. The **configure** command can edit all sections with keywords. Using the **configure** command, for example, you enter the section for a particular name or interface:

```
device# configure IP Ethernet 2:0
```

Then enter as many keywords as you want to apply to the section:

```
[ IP Ethernet 2:0 ]# keyword = value
[ IP Ethernet 2:0 ]# keyword = value
...
```

The **configure** command formats and checks the input and offers a help facility (**Help** or *keyword* **= ?**).

The **edit config** command allows you to enter rules directly into the configuration file with a special text editor. The **edit config** command is required for sections with rules, although the command can also edit keyword sections. The **edit config** command does not check the syntax or provide help for the particular section.

For example, enter the section for a particular name:

```
device# edit config IP Filter "ip-in"
```

Then append lines to the section:

```
Edit [ IP Filter "ip-in" ]> append $
Append> rule 1
Append> rule 2
Append> .
Edit [ IP Filter "ip-in" ]> exit
device#
```

If you make any changes using the **configure** or **edit config** command, the changes do not take effect until you write them and restart using the **save** command. To save your changes without restarting (or applying), you must use the **write** command.

Management Command Description

You can enter management commands at any time and at any prompt. They allow you to:

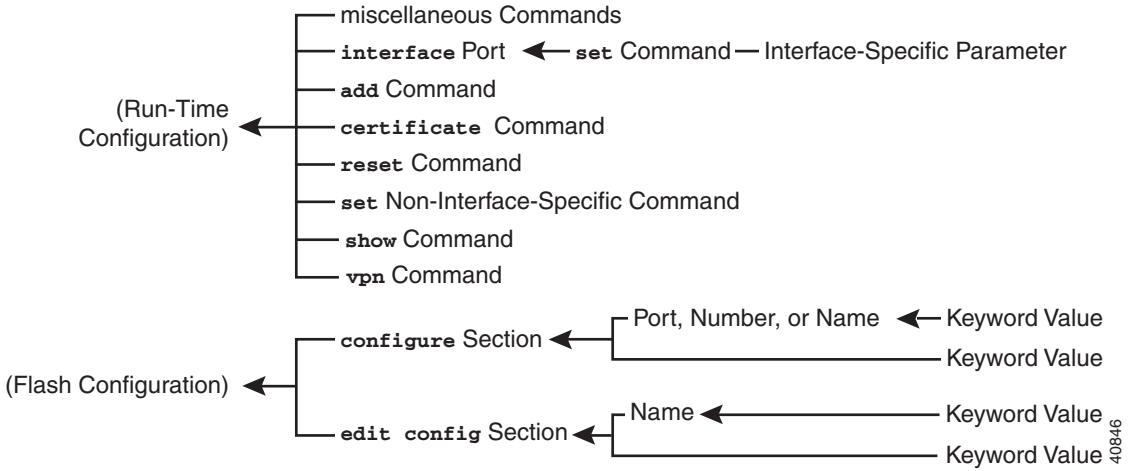
- Perform system tasks
- Change run-time parameters that are not permanently stored
- Show and edit tables and statistics

Some management commands apply to a particular interface, and you must first specify the interface before you enter further commands.

Command Hierarchy

Figure D-1 shows the hierarchy of commands, where commands entered after changing to a particular section apply only to that section.

Figure D-1 Command Hierarchy



Strings and Names

For commands that allow you to enter a string or name, to accommodate spaces and special characters always use double quotation marks (“) before and after the string. If you are not using any spaces or special characters, you do not need to use double quotation marks.

You can use any special character, with the following exceptions:

- For section names, you cannot use the pound sign (#), backslash (\), or double quotation marks (“) within the string.
- In keyword values and rules within double quotation marks (“), you can use \\ for a backslash and \” for double quotation marks.

See the section descriptions in the *Cisco VPN 5000 Concentrator Series Command Reference Guide* for string length restrictions.

Table D-3 lists special sequences to format the text for viewing in a third-party application. If you enter any of these special sequences in double quotation marks (“), only \\, \”, and \ are supported.

Table D-3 Special Characters

Function	Character	Example
Continue the line on the next line	\	"Charles Darwin" Config = "CompanyA" SharedKey = \ "MySharedKey" Auth = "My Authentication Pass\ Phrase" Encrypt = "Encrypt Pass Phrase" If a string is continued onto a second or succeeding line, there must be space at the beginning of the line. Thus, the following text is allowed: AdminName="This text is on line 1 This text is on line 2.\ This text is also on line 2." The following text is an error: AdminName="This text is on line 1 This text is on line 2.\ This text is also on line 2."
New line	\n	IPaddress = 0.0.0.0 \n Mask = 255.255.255.0
Tab	\t	IPaddress \t = 0.0.0.0
Space at the beginning of a line or multiple spaces	\<space>	IPaddress \ \ \ = 0.0.0.0
" (double quotation mark)	\"	Password = "\"Word\"" (the double quotation marks (") are part of the password you enter)
Control character	\<ASCII octal digits>	\15 \15 represents a carriage return.
Backslash	\\	Password = "\\Word" (the \ is part of the password you enter)

Configuring the Firewall for VPN

If all VPN 5000 interfaces are behind your firewall, configure the firewall to allow VPN packets for the following tunnel types:

- IPSec:
  - Allow packets to the concentrator with a destination UDP port of 500 (ISAKMP), and from the concentrator with a source UDP port of 500.
  - If you are using NAT transparency, allow packets to the device with a destination TCP port of 80, and from the device with a source TCP port of 80 (by default). If you change the TCP port using the **General** section **NATTransport** keyword, set the port number appropriately.
  - If you are using the default Encapsulating Security Payload (ESP) protocol, allow packets with IP protocol 50 to and from the concentrator.
  - If you are using the Authentication Header (AH) protocol, allow packets with IP protocol 51 to and from the concentrator.
- GRE:
  - If you are using manually keyed LAN-to-LAN tunnels with no encryption and no authentication, allow packets with IP protocol 47 (GRE) to and from the concentrator.

To configure your firewall, see the guide that came with it.

APPENDIX F

IP Addressing

This appendix describes how to use IP addresses in the Cisco VPN 5000 concentrator. An IP address is a 32-bit number written in dotted decimal notation: four 8-bit fields (octets) converted from binary to decimal numbers, separated by dots. The first part of an IP address identifies the network on which the host resides, while the second part identifies the particular host on the given network. The network number field is called the network prefix. All hosts on a given network share the same network prefix but must have a unique host number. In classful IP, the class of the address determines the boundary between the network prefix and the host number.

Classes

IP host addresses are divided into three different address classes: Class A, Class B, and Class C. Each class fixes the boundary between the network prefix and the host number at a different point within the 32-bit address. Class D addresses are reserved for multicast IP.

- Class A addresses (1.xxx.xxx.xxx through 126.xxx.xxx.xxx) use only the first octet as the network prefix.
- Class B addresses (128.0.xxx.xxx through 191.255.xxx.xxx) use the first two octets as the network prefix.
- Class C addresses (192.0.0.xxx through 223.255.255.xxx) use the first three octets as the network prefix.

Because Class A addresses have 16,777,214 host addresses, and Class B addresses 65,534 hosts, you can use subnet masking to break these huge networks into smaller subnets.

Private Networks

If you need large numbers of addresses on your network, and they do not need to be routed on the Internet, you can use private IP addresses that the Internet Assigned Numbers Authority (IANA) recommends. The following address ranges are designated as private networks that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Subnet Masks

A subnet mask allows you to convert a single Class A, B, or C network into multiple networks. With a subnet mask, you can create an *extended* network prefix that adds bits from the host number to the network prefix. For example, a Class C network prefix always consists of the first three octets of the IP address. But a Class C *extended* network prefix uses part of the fourth octet as well.

Subnet masking is easy to understand if you use binary notation instead of dotted decimal. The bits in the subnet mask have a one-to-one correspondence with the Internet address:

- The bits are set to 1 if the corresponding bit in the IP address is part of the extended network prefix.
- The bits are set to 0 if the bit is part of the host number.

Example 1: If you have the Class B address 129.10.0.0 and you want to use the entire third octet as part of the extended network prefix instead of the host number, you must specify a subnet mask of 11111111.11111111.11111111.00000000. This subnet mask converts the Class B address into the equivalent of a Class C address, where the host number consists of the last octet only.

Example 2: If you want to use only part of the third octet for the extended network prefix, then you must specify a subnet mask like 11111111.11111111.11111000.00000000, which uses only 5 bits of the third octet for the extended network prefix.

You can write a subnet mask as a dotted decimal mask or as a */bits* ("slash *bits*") mask. In Example 1, for a dotted decimal mask, you convert each binary octet into a decimal number: 255.255.255.0. For a */bits* mask, you add the number of 1s: /24. In Example 2, the decimal number is 255.255.248.0 and the /bits is /21.

You can also supernet multiple Class C networks into a larger network by using part of the third octet for the extended network prefix. For example, 192.168.0.0/20.

Determining the Subnet Mask

To determine the subnet mask based on how many hosts you want, see Table F-1.

Table F-1 Hosts, Bits, and Dotted Decimal Masks

Hosts[1]	/Bits Mask	Dotted Decimal Mask
16,777,216	/8	255.0.0.0 Class A Network
65,536	/16	255.255.0.0 Class B Network
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8,192	/19	255.255.224.0
4,096	/20	255.255.240.0
2,048	/21	255.255.248.0
1,024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C Network
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240

Table F-1 Hosts, Bits, and Dotted Decimal Masks

Hosts[1]	/Bits Mask	Dotted Decimal Mask
8	/29	255.255.255.248
4	/30	255.255.255.252
Do not use	/31	255.255.255.254
1	/32	255.255.255.255 Single Host Address

1. The first and last number of a subnet are reserved, except for /32, which identifies a single host.

Determining the Address to Use with the Subnet Mask

The following procedures describe how to determine the network address to use with a subnet mask for a Class C-size and a Class B-size network.

Class C-Size Network Address

For a network between 2 and 254 hosts, the fourth octet falls on a multiple of the number of host addresses, starting with 0. For example, the 8-host subnets (/29) of 192.168.0.x are:

Subnet with Mask /29 (255.255.255.248)	Address Range[1]
192.168.0.0	192.168.0.0 to 192.168.0.7
192.168.0.8	192.168.0.8 to 192.168.0.15
192.168.0.16	192.168.0.16 to 192.168.0.31
…	…
192.168.0.248	192.168.0.248 to 192.168.0.255

1. The first and last address of a subnet are reserved. In the first subnet example, you cannot use 192.168.0.0 or 192.168.0.7.

Class B-Size Network Address

To determine the network address to use with the subnet mask for a network with between 254 and 65,534 hosts, you need to determine the value of the third octet for each possible extended network prefix. For example, you might want to subnet an address like 10.1.*x*.0, where the first two octets are fixed because they are used in the extended network prefix, and the fourth octet is 0 because all bits are used for the host number.

To determine the value of the third octet, follow these steps:

Step 1 Calculate how many subnets you can make from the network by dividing 65,536 (the total number of addresses using the third and fourth octet) by the number of host addresses you want.

For example, 65,536 divided by 4096 hosts equals 16.

Therefore, there are 16 subnets of 4096 addresses each in a Class B-size network.

Step 2 Determine the multiple of the third octet value by dividing 256 (the number of values for the third octet) by the number of subnets:

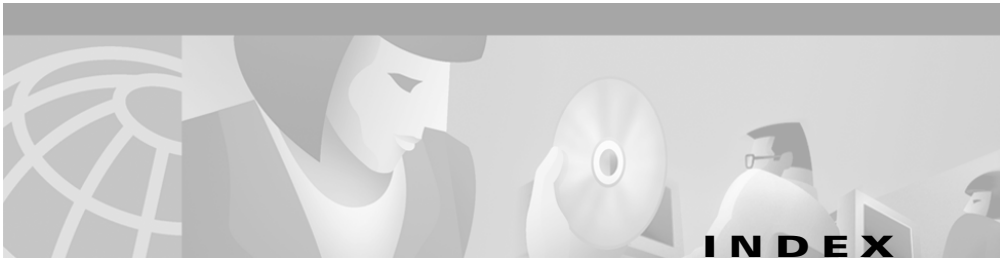
In this example, 256/16 = 16.

The third octet falls on a multiple of 16, starting with 0.

Therefore, the 16 subnets of the network 10.1 are:

Subnet with Mask /20 (255.255.240.0)	Address Range[1]
10.1.0.0	10.1.0.0 to 10.1.15.255
10.1.16.0	10.1.16.0 to 10.1.31.255
10.1.32.0	10.1.32.0 to 10.1.47.255
…	…
10.1.240.0	10.1.240.0 to 10.1.255.255

1. The first and last address of a subnet are reserved. In the first subnet example, you cannot use 10.1.0.0 or 10.1.15.255.



Symbols

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

X