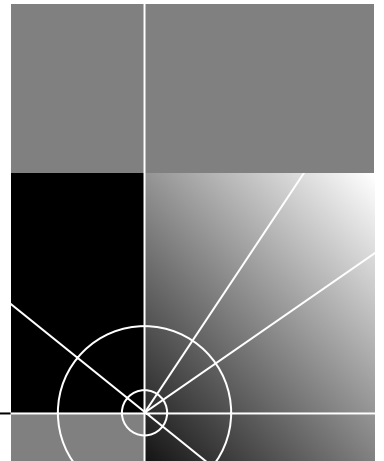




VPN Configuration Guide

<http://www.3com.com/>

Published July 1999



3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 1999, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, NETBuilder, NETBuilder II, and OfficeConnect are registered trademarks and PathBuilder and Total Control are trademarks of 3Com Corporation.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

Guide written by Linda Lininger. Edited and Illustrated by Amy Guzules. Produced by Julie Laccabue.

CONTENTS

ABOUT THIS GUIDE

Accessing the Live VPN Demonstration Site	7
Conventions	9
Related Documentation	10
Year 2000 Compliance	10

INTRODUCTION TO VIRTUAL PRIVATE NETWORKS

What Is a Virtual Private Network?	11
Components of a Tunnel	11
What Protocols Are Used by VPN Software?	14
What Types of VPNs Are There?	15
Remote Access Services VPN	15
Site-to-Site VPN	17
Web Link Health Monitor	19
Secure VPN Manager	19
InfoVista	19
Tunneling Concepts	20
Authentication Mechanisms	20
SysCallerID Authentication	20
Standards-based PPP Authentication	20
Multiprotocol Tunneling	21
Tunnel Peers	22
Encryption	22
Key Encryption Key	22
IPSec Security	23
IKE	23
Compression	23
Network Address Translation	24

CONFIGURING REMOTE ACCESS SERVICES VPNs

Two Types of RAS VPNs	25
Configuring the Central Site	27
Configuring IP and IPX Connectivity	30
Configuring RAS	30
Provisioning IP Addresses	30
Configuring DHCP Support Using a DHCP Server	31
Configuring SNMP	32
Setting Up System Basics	32
Configuring RAS User Authentication	33
Configuring an External RADIUS Support for RAS	33
Configuring RAS Tunnels with a Local User Authentication Database	35
Configuring Tunnel Switching	37
Configuring the Client	38
Configuring the Client Workstation	39
Connecting to the Tunnel Terminator	46

CONFIGURING SITE-TO-SITE VPNs

Configuring the VLL Central Site Router	50
Configuring the Central Site Router	51
Configuring the VLL Remote Site	53
Configuring the Dial-Up Central Site Router	56
Configuring the Dial-Up Remote Site	59
Configuring Tunnel Switching	63
Adding IPsec Security	66
Central Site IPsec Configuration	66
Remote Site IPsec Configuration	67
Configuring Internet Key Exchange (IKE)	68
Configuring IKE for Tunnel Mode IPSEC	69
Router 1	69
Router 2	71
Router 3	72
Configuring IKE for Transport Mode	73
Router 1, Router 2, and Router 3	74
Configuring IKE with a Non-3Com Security Gateway	75

INDEX

ABOUT THIS GUIDE

This guide describes how to configure the two basic types of virtual private networks (VPNs): Remote Access Services (RAS) and site-to-site.

Audience

This guide is intended for Network Managers and Administrators who are responsible for the planning, installation, and maintenance of VPN environments.

This guide assumes that the reader is familiar with the Enterprise OS software, user interface functions, and concepts relating to 3Com[®] products.

Accessing the Live VPN Demonstration Site

The configurations presented in this guide are designed to provide you access to the live 3Com VPN demonstration site, which has been named "ACME Corporation."

You can use the remote client and remote site dial-up configuration examples to actually tunnel to the ACME Corporation demonstration central site.



The ACME Corporation site is currently not accessible using the virtual leased line (VLL) configuration described in this guide.

When you have tunnelled to the demonstration site, you can access the VPN information on the ACME Corporation central site server. This information includes the ASCII text configuration files used in the examples in this guide. You can copy these files and modify them to configure your installation.

- See "Configuring the Client" in Chapter 2 for instructions on how to use the Microsoft Dial-Up Networking to initiate a Remote Access Services (RAS) tunnel to the ACME Corporation RAS tunnel

terminator. These instructions include the user names and passwords you should use to establish this tunnel.

- See “Configuring the Dial-Up Remote Site” in Chapter 3 for instructions on how to configure a remote site for dial-up access to the ACME Corporation site-to-site tunnel terminator. These instructions include the user names and passwords you should use for initiating either a PPTP or L2TP tunnel.

Contents Road Map

This guide contains three main chapters:

- Chapter 1, “Introduction to Virtual Private Networks,” contains basic information about virtual private networks. “Tunneling Concepts,” in this chapter, provides background information and concepts related to VPN tunneling.
- Chapter 2, “Configuring Remote Access Services VPNs,” describes two types of Remote Access Services (RAS) VPNs: the remote/mobile client dial-up RAS VPN and the extranet/partner access client RAS VPN. Chapter 2 contains two configuration examples:
 - “Configuring the Central Site” contains procedures for establishing basic system settings, provisioning IP addresses, and configuring RAS authentication.
 - “Configuring the Client” contains procedures for setting up and using Microsoft Dial Up Networking to establish a tunnel to the central site tunnel terminator.
- Chapter 3, “Configuring Site-to-Site VPNs,” describes site-to-site VPNs, which can be configured with dial-on-demand tunnels or using a virtual leased line (VLL) configuration where the connection provided by the internet service is persistent at both ends.
 - “Configuring the VLL Central Site Router” describes how to set up the central site that terminates VLL tunnels.
 - “Configuring the VLL Remote Site” describes how to set up a remote site router that initiates VLL tunnels.
 - “Configuring the Dial-Up Central Site Router” describes how to set up a central site router that terminates dial on demand tunnels.
 - “Configuring the Dial-Up Remote Site” describes how to set up a remote site to initiate dial-on-demand tunnels.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons




Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions


Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Syntax	Evaluate the syntax provided and supply the appropriate values. Placeholders for values you must supply appear in angle brackets. Example: <p>Enable RIPIP using:</p> <pre>SETDefault !<port> -RIPIP CONTROL = Listen</pre> <p>In this example, you must supply a port number for <port>.</p>
Commands	Enter the command exactly as shown in text and press the Return or Enter key. Example: <p>To remove the IP address, enter:</p> <pre>SETDefault !0 -IP NETaddr = 0.0.0.0</pre> <p> <i>This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case-sensitive.</i></p>
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: <p>Press Ctrl+Alt+Del</p>

Table 2 Text Conventions (continued)

Convention	Description
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none">■ Emphasize a point.■ Denote a new term at the place where it is defined in the text.■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.

Related Documentation

The following documents contain information relating to the configuration steps presented in this guide:

- *Using Enterprise OS Software, Version 11.3*
- *Reference to Enterprise OS Software, Version 11.3*
- *Using the PathBuilder Switch*

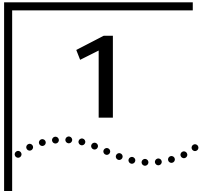
Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

<http://www.3com.com/>

Year 2000 Compliance

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

<http://www.3com.com/products/yr2000.html>



INTRODUCTION TO VIRTUAL PRIVATE NETWORKS

This chapter provides basic information about what a virtual private network (VPN) is, the components of a tunnel, how a VPN works, and tools for monitoring VPN performance.

What Is a Virtual Private Network?

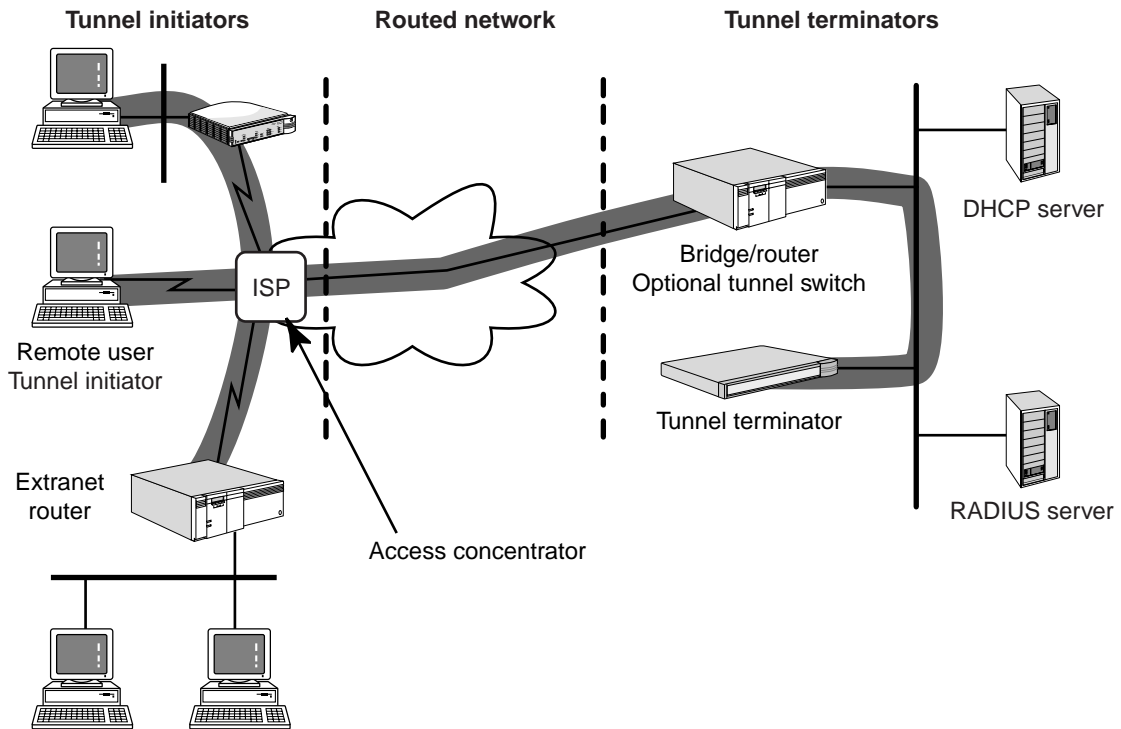
A VPN is a connection that has the appearance and many of the advantages of a dedicated link, but occurs over a shared network. Using a technique called “tunneling,” data packets are transmitted across a public routed network, such as the Internet or other commercially available network, in a private “tunnel” that simulates a point-to-point connection.

This approach enables network traffic from many sources to travel through separate tunnels across the same infrastructure. It allows network protocols to traverse incompatible infrastructures. It also enables traffic from many sources to be differentiated, so that it can be directed to specific destinations.

Components of a Tunnel

The basic components of a tunnel are shown in Figure 1 and include the following:

- A tunnel initiator (TI).
- A routed network.
- An optional tunnel switch.
- One or more tunnel terminators (TT).

Figure 1 Basic VPN Connection

Tunnel initiation and termination can be performed by a variety of network devices and software.

A tunnel can be started by any one of the following devices:

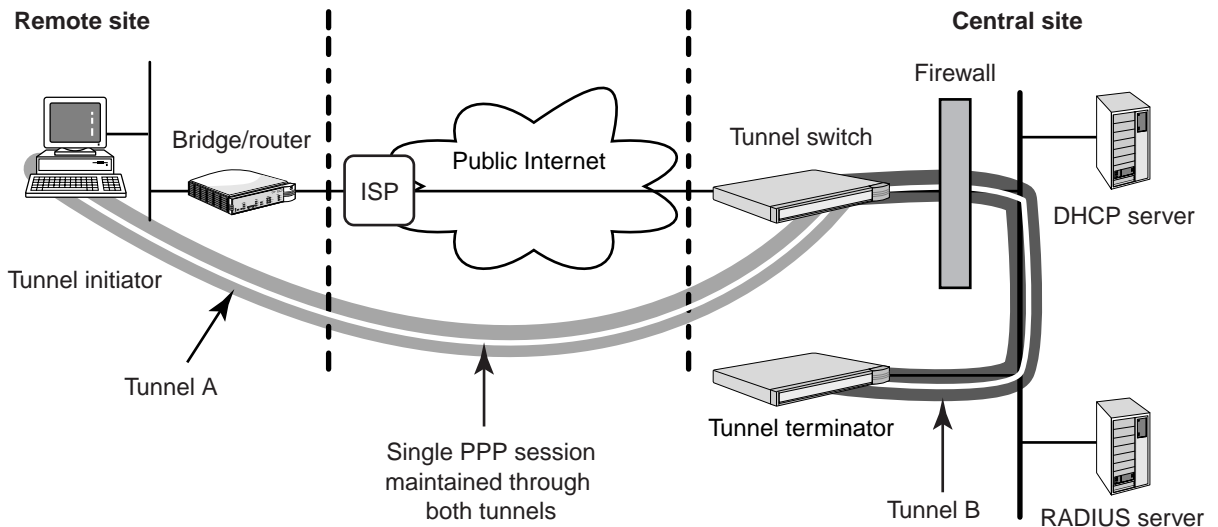
- An end user's laptop equipped with an analog PC modem card and VPN-enabled dial-up software (basic tunneling and security capabilities are bundled into Windows 9x and Windows NT 4.0).
- A VPN-enabled extranet router on an enterprise branch or home office LAN.
- A VPN-enabled access concentrator at a network service provider point of presence (POP).

A tunnel can be ended by a tunnel terminator or switch on an enterprise network or on an ISP's network.

In addition, VPNs usually contain one or more security servers, such as the RADIUS server shown in Figure 1. Along with the conventional application of firewalls and address translation, VPNs can provide for data encryption, authentication, and authorization.

Tunnel switching, shown in Figure 2, can be employed to enhance the security of your network. You can configure a router outside the corporate firewall as a tunnel switch with the tunnel terminator located inside the firewall. The firewall can then be configured to permit only those tunnels with the source as the tunnel switch and the destination as the tunnel terminator. Tunnel switching with this type of device specific configuration removes the need to allow all tunnel requests through the firewall. In addition, the user community does not need to be modified when central site structural changes are made, because access to the central site is tunneled through one device.

Figure 2 Basic Tunnel Switching Components



What Protocols Are Used by VPN Software?

The earliest VPN software used the Point-to-Point Tunneling Protocol (PPTP). This was a defacto standard that was challenged by another protocol, Layer 2 Forwarding (L2F). The industry called for a single standard, which caused the two protocols to be merged into a more secure and improved tunneling protocol called Layer 2 Tunneling Protocol (L2TP). L2TP has been defined and is currently being implemented by many networking companies.

PPTP uses GRE (General Routing Encapsulation) to transport data and TCP port 1723 for the control frames. Most other VPN software uses UDP (Unnumbered Datagram Protocol) for transport. Some VPN software companies use a combination of these protocols or have implemented proprietary VPN protocols. It is important that both ends of the tunnel use the same tunneling protocol.

An Enterprise OS device can support PPTP and L2TP and can be a tunnel initiator, tunnel terminator, or tunnel switch for those protocols.

A 3Com OfficeConnect® LAN modem cannot initiate or terminate tunnels, but it can be used to pass VPN data between VPN clients and servers using simple IP forwarding. A LAN modem is transparent to Enterprise OS platforms, PPTP, L2TP, GRE (used by PPTP) and UDP (used by L2TP, IPSec, and other VPN software). Table 3 contains a list of well-known tunneling ports.

Table 3 Well-Known Tunneling Ports

Protocol	Port
Point-to-Point Tunneling Protocol (PPTP)	TCP port 1723
General Routing Encapsulation (GRE)	IP protocol Type 47
Layer 2 Tunneling Protocol (L2TP)	UDP port 1701
AH	IP protocol type 51
ESP	IP protocol type 50

What Types of VPNs Are There?

This guide describes two basic VPN strategies: Remote Access Services (RAS) and site-to-site.



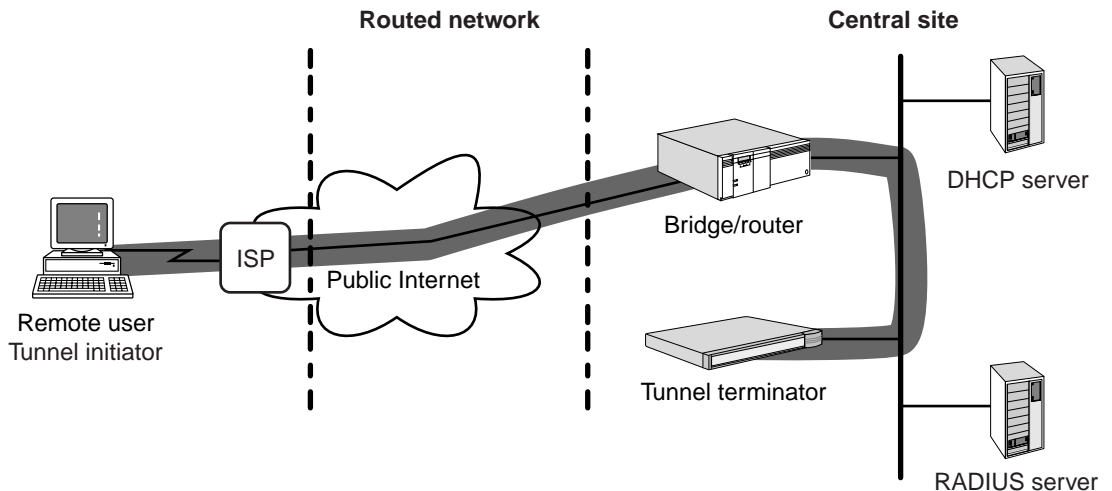
Site-to-site VPNs are also commonly referred to as router-to-router, LAN-to-LAN, and VLL (virtual leased line) VPNs. In this guide, this type of VPN is referred to as site-to-site.

Remote Access Services VPN

The Remote Access Services (RAS) VPN allows an enterprise to replace dedicated dial ports with Internet connectivity through Internet service providers (ISPs), which reduces capital costs and provides access to points of presence across the globe. RAS VPNs ensure that whenever employees travel, they can get onto the corporate intranet by making a local call, which reduces line charges and equipment costs.

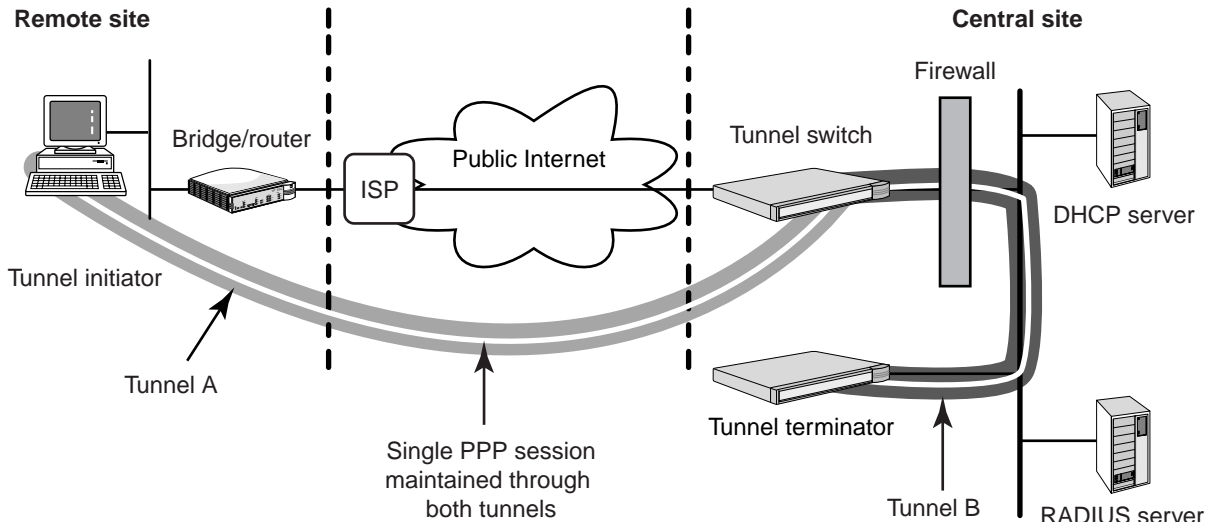
Two types of RAS VPNs are described in this guide. One type of RAS VPN is a remote/mobile client dial-up RAS VPN, shown in Figure 3.

Figure 3 Remote/Mobile Client Dial-Up RAS VPN



Another type of RAS VPN, a RAS extranet VPN, enables corporate employees and partners to access corporate resources from remote LANs as if those users were physically present on the corporate LAN. Figure 4 shows a RAS extranet VPN connection.

Figure 4 RAS Extranet VPNs

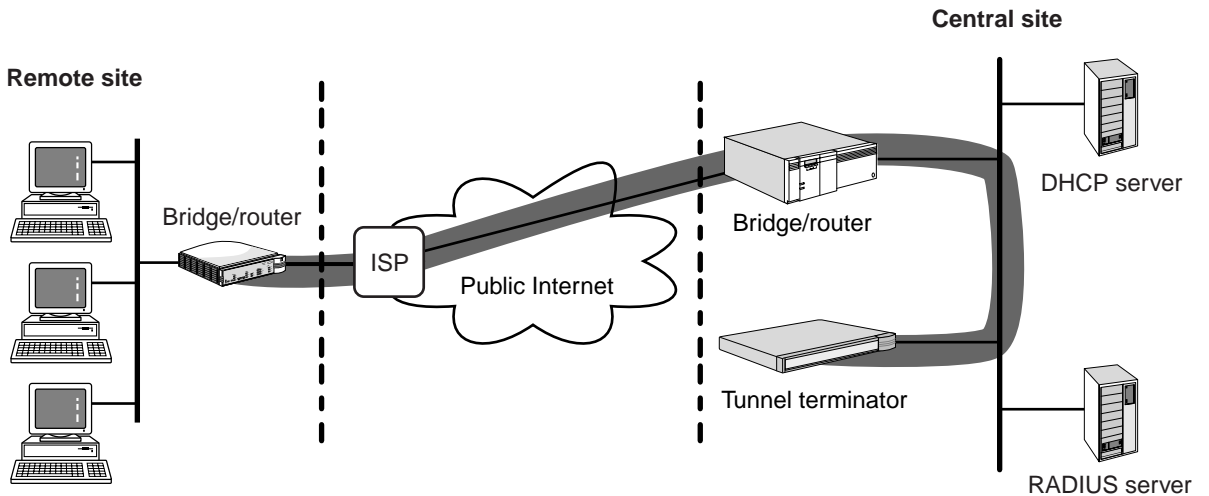


These two types of RAS VPN configurations are similar in that they both require that the tunnel-initiating client be authenticated before the tunnel can be established. The authentication mechanism can be either an external RADIUS server or a database in the tunnel terminator. Also, in both types of RAS VPNs, the tunnel terminator assumes that there is only one device at the tunnel initiator end of the tunnel.

Site-to-Site VPN

In a site-to-site VPN, shown in Figure 5, the configuration of the VPN depends on the type of internet access the remote office has.

Figure 5 Site-to-Site VPN



The remote office can use either:

- A dial-on-demand configuration that accesses the Internet only when users at the remote office require a connection to the central site.
- A virtual leased line (VLL) configuration where the ISP connection is persistent at both ends.

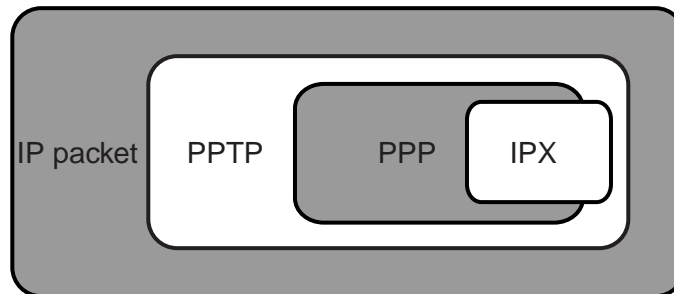
How Do VPNs Work?

VPNs are based on familiar networking technology and protocols.

In the case of some RAS VPNs, the remote access client is still sending a stream of Point-to-Point Protocol (PPP) packets to a remote access server. Similarly, in the case of site-to-site virtual leased lines, a router on one LAN is still sending PPP packets to a router on another LAN. What is new is that in each case instead of going across a dedicated line, the PPP packets are going across a tunnel over a shared network.

The effect of VPNs is like that of pulling a serial cable across a WAN cloud. PPP protocol negotiations set up a direct connection from the remote user to the tunnel termination device.

The most widely accepted method of creating industry-standard VPN tunnels is by encapsulating network protocols such as IP, IPX, and AppleTalk inside the PPP packet and then encapsulating the entire package inside a tunneling protocol, which is typically IP but could also be ATM or Frame Relay. This approach is called "Layer 2 tunneling," because the passenger is a Layer 2 protocol.



Monitoring and Configuring VPN Performance

There are several options available for monitoring the performance of your VPN. You can use the Web Link applet, the Secure VPN Manager application, or InfoVista.

Web Link Health Monitor

The Health Monitor is a part of Web Link, the web-based network management application that is part of all Enterprise OS products. The Health Monitor provides Java graphs that present performance data in a browser.

In addition to system performance graphs, interface performance graphs, and protocol performance graphs, path performance graphs indicate the performance of the physical interface bandwidth usage. Graphs that show total IPX packets and IPX packets per interface appear in the protocol performance graph group.

Secure VPN Manager

Transcend® Secure VPN Manager is a graphical web-based network management tool that presents key information about your virtual private network (VPN). Secure VPN Manager provides the assistance necessary to monitor the VPN tunnels terminated by the Enterprise OS device. Current and historical data is collected, which allow administrators to perform the following functions:

- Quality of service analysis
- Tunnel usage analysis
- Tunnel security analysis
- Capacity utilization analysis

These analyses are possible through the monitoring of the VPN tunnel between two or more 3Com routers, such as an OfficeConnect NETBuilder® bridge/router located at a company's branch office and a NETBuilder II® bridge/router or PathBuilder™ switch located at headquarters.

InfoVista

InfoVista is a comprehensive, flexible service level management and conformance solution for information technology (IT) organizations, telcos, outsourcers, and network service providers. As an enterprise-oriented solution, InfoVista renders a uniform view of service-level achievements across every component within an information system. Unlike other more narrowly focused products, InfoVista collects

and interprets data from every facet of the IT infrastructure, including network, device, applications, and systems.

InfoVista collects data from standard and nonstandard devices, such as servers, workstations, and applications, and measures and reports on user-selected metrics required for Service Level Agreement conformance. Its easy-to-use interface enables IT managers and nontechnical users alike to analyze resource activity and trends, anticipate future demands, and prepare customized Quality of Service reports for distribution to customers.

Tunneling Concepts

This section provides an overview of the concepts and you need to understand and decisions you need to make when configuring tunnels.

Authentication Mechanisms

When creating a virtual port, you can choose one of two authentication mechanisms: proprietary SysCallerID or standards-based PPP.

SysCallerID Authentication

When all sites in your VPN use Enterprise OS products, you can configure SysCallerID as the authentication mechanism. If SysCallerID is used, PPP uses that identification parameter as a “caller ID” to identify itself to its peer when establishing a PPP Link Control Protocol (LCP) link. This identification allows the central site router to map incoming calls from the remote sites. The SysCallerID parameter is an Enterprise OS proprietary PPP authentication mechanism.



SysCallerID is required when using virtual leased line (VLL) configurations.

For more information about configuring a port to use SysCallerID, see the Configuring Port Bandwidth chapter in *Using Enterprise OS Software* and the SYS Service Parameters chapter in *Reference for Enterprise OS Software*.

Standards-based PPP Authentication

When all sites in your VPN are not using Enterprise OS products, you need to use the AuthLocalUser parameter and optionally, the AuthRemoteUser parameter in the PPP service to support standards-based PAP, CHAP, and MS-CHAP authentication.

The AuthLocalUser (ALU) parameter is used to certify the router to a PPP peer. In a dial scenario, the calling router defines the ALU parameter. The

AuthRemoteUser (ARU) parameter identifies the user and password used by the PPP peer. The information entered in this router's ARU parameter is the same as that entered in the calling party's ALU.

For more information about configuring PAP, CHAP, and MS-CHAP, see the Configuring Wide Area Networking Using PPP chapter in *Using Enterprise OS Software* and the PPP Service Parameters chapter in *Reference for Enterprise OS Software*.

Multiprotocol Tunneling

Multiprotocol tunnels require IP connectivity. Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) both use IP as their carrier protocol. If the tunnel endpoints cannot establish IP connectivity between them, they will not be able to establish tunnels.

VPN tunnels carry PPP links. Anything that can be accomplished with PPP links can be accomplished over PPTP and L2TP tunnels. This includes multiprotocol routing, bridging, and bandwidth-on-demand, dial-on-demand and protocol reservation.

PPTP/L2TP defines a method for transferring Point-to-Point Protocol (PPP) datagrams through a tunnel over IP. Tunneling PPP does not change PPP, but provides a vehicle by which PPP data units (PDUs) can be carried between two peers.

A PPTP/L2TP connection is defined by two parallel components: a control connection and a data pipe. For PPTP, the control connection operates over TCP and passes call control and management packets over the TCP session. The data pipe operates over IP to transfer data packets encapsulated using Generic Routing Encapsulation Protocol Version 2 (GRE V2). For L2TP, both the control connection and the data pipe operate over the UDP session.

You can configure PPTP/L2TP tunnel connections between an Enterprise OS device and a VPN enabled access concentrator such as a Total Control™ hub. In this scenario, the Enterprise OS device is acting as a tunnel terminator, which only receives inbound calls. An Enterprise OS device can also receive inbound calls from VPN-capable RAS clients (Windows 98/NT) to provide remote access services.

In addition, an Enterprise OS device expands the use of PPTP/L2TP so a tunnel can be established between two peer Enterprise OS devices. In this scenario, the Enterprise OS device is able to issue outbound calls so either

side can be the tunnel initiator or tunnel terminator. This is a router-to-router configuration, and both peers play the same role.

For more information about configuring PPTP and L2TP tunnels, see the Configuring L2Tunnel Connections chapter in *Using Enterprise OS Software* and the L2Tunnel Service Parameters chapter in *Reference for Enterprise OS Software*.

Tunnel Peers

Of the two tunnel peers, the tunnel terminator must have a fixed, publicly accessible IP address. If both tunnel peers have fixed public IP addresses, then the `-L2T Service AccessList` parameter can be used at both ends to explicitly limit who can access tunnels. This can provide additional security by preventing unauthorized tunnels from connecting in. If both peers have fixed public IP addresses, the tunnel can be initiated from either end.

Encryption Neither PPTP nor L2TP by themselves provide for encryption of their data streams. Encryption can be accomplished at the PPP layer (via MPPE), at the IP layer (via IPsec), or both.

To encrypt the PPP datastream across an IP network, Microsoft provides the Microsoft Point to Point Encryption (MPPE) protocol.

Microsoft does not support L2TP at this time, however, in an ISP-initiated tunnel scenario, the Microsoft Dial-Up client can use MPPE to encrypt the PPP datastream and the Total Control hub can tunnel that PPP datastream. This results in an L2TP tunnel across the Internet that is carrying an encrypted MPPE data stream even though Microsoft did not create the L2TP tunnel.

Key Encryption Key

Key Encryption Key (KEK) is an encryption key that is entirely inside the Enterprise OS platform. When entering a root user name or password, it is not desirable to store the entry in clear text in the CCS form inside a router. It is not a good idea to store it in clear text form in RAM. It is also not desirable to define user names and passwords for RAS users and store them in clear text either in flash or RAM.

KEK provides a mechanism for storing user names and passwords in a uniquely encrypted form. A sufficiently strong hash algorithm is used, so

that is unlikely that anyone would be to create a similar string that hashes to the same value.

KEK immediately hashes an entered user name or password and stores the hashed value only in flash and in RAM. The hashed value is then used to determine whether or not an entered user name or password is correct.

Until recently, all 3Com bridge/routers used the same key and value. So you could copy the CCS file from one router to another. Now by default, 3Com routers use a string and one of the MAC addresses in that particular router together as a key, which is combined with the entered user name or password, thereby making all hashing unique to the router.

For more information about configuring encryption, see the Configuring Wide Area Networking Using PPP chapter in *Using Enterprise OS Software* and the PPP Service Parameters chapter in *Reference for Enterprise OS Software*.

IPSec Security

IPSec can be used to provide security at the IP layer. Because IPSec is integrated into IP itself, IPSec adds security to any link, regardless of the application used.

IPSec can be used in conjunction with the tunneling protocols PPTP and L2TP or as a tunneling mechanism by itself.

IKE

Internet Key Encryption (IKE) protocols provide a mechanism for establishing security associations. The IKEProfile parameter defines a group of settings for IPSec to use when establishing an IKE security association. These settings include authentication method, encryption algorithm, hash algorithm, and optionally the lifetime and Diffie-Hellman group to use in negotiations.

For more information about configuring IPSec, see the Configuring IPSec chapter in *Using Enterprise OS Software* and the IPSec Service Parameters chapter in *Reference for Enterprise OS Software*.

Compression

Site-to-site tunnels can be compressed with the 3Com proprietary implementation of the Stac LZS algorithm. Attempting to enable compression between Win32 (Win95/Win98/WinNT) clients and RAS concurrently with encryption leads to time-outs during the PPP option

negotiation. You may enable compression on the Win32 client, or enable encryption, or neither, but not both.

The standards-based Compression Control Protocol is available in Enterprise OS software version 11.3 or later.

Network Address Translation

Tunneling is frequently used to connect two or more private networks across a public network. Network Address Translation (NAT) applied on the public interface of the tunnel endpoint can prevent the advertisement of the private network's IP address(es) to the public network.

If session establishment occurs only from the tunnel initiators' site(s) to a central tunnel termination site, then the remote branches may use the same LAN address range, tunnel into RAS at the central site, and perform NAT from their private addresses to the address dynamically acquired from RAS.

For more information about configuring Network Address Translation, see the Configuring Network Address Translation chapter in *Using Enterprise OS Software* and the NAT Service Parameters chapter in *Reference for Enterprise OS Software*.

2

CONFIGURING REMOTE ACCESS SERVICES VPNs

This chapter provides configuration procedures for Remote Access Services (RAS) VPNs.

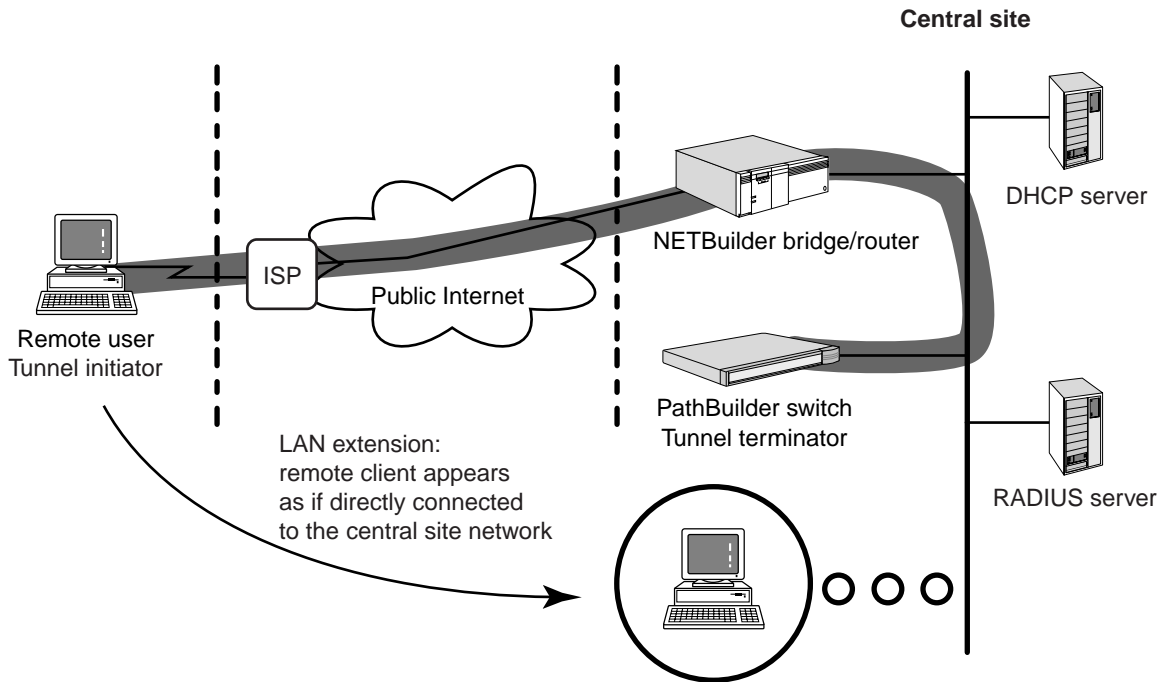
This chapter contains the following configuration information:

- “Configuring the Central Site” on page 27 contains procedures for establishing basic system settings, setting up DHCP support, configuring RAS authentication, and configuring tunnel switching.
- “Configuring the Client” on page 38 contains procedures for setting up and using Microsoft Dial-Up Networking to establish a tunnel to the central site tunnel terminator.

Two Types of RAS VPNs

Two types of RAS VPNs are described in this chapter: the remote/mobile client dial-up RAS VPN and the extranet/partner access RAS VPN. These two types of VPN configurations are similar in that they both require that the tunnel initiating client be authenticated before the tunnel can be established. The authentication mechanism can be either an external RADIUS server or a database in the tunnel terminator.

In the configuration shown in Figure 6, the remote client is set up to dial an Internet service provider (ISP) to gain access to the shared IP network. This remote client can be a mobile user with a laptop computer or a user at a relatively permanent location, such as a home office.

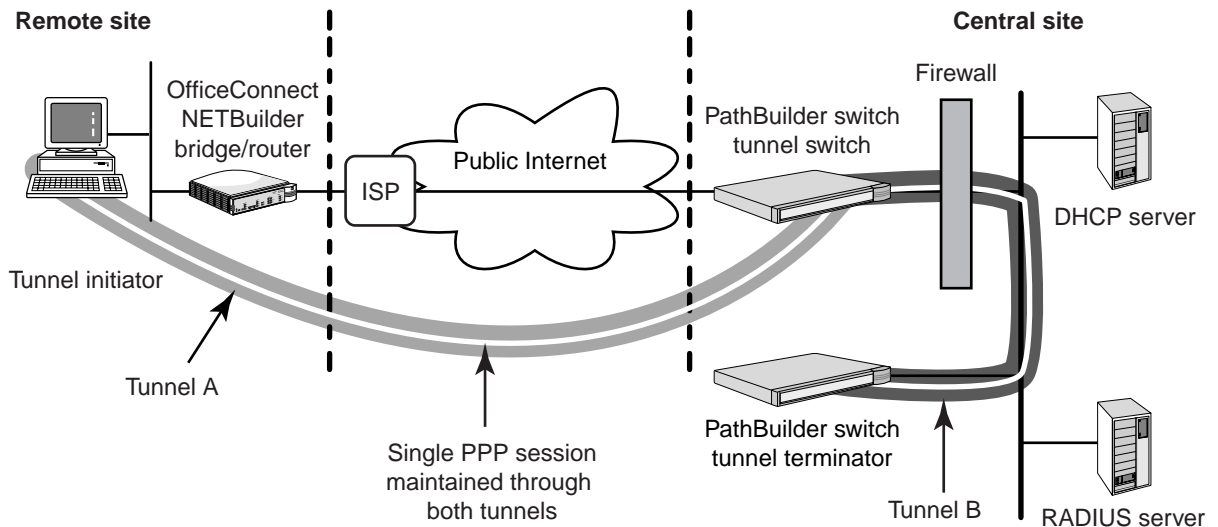
Figure 6 Remote/Mobile Client Dial-Up RAS VPN Configuration

Using a client application such as Microsoft Dial-Up Networking, the user first opens a connection (dials up) to the ISP. Then again using the Dial-Up Networking application, the user establishes a tunnel to the tunnel terminator. When the tunnel is established, the remote user appears to be directly attached to the local network. The mechanism for establishing this appearance is called “LAN extension.”

RAS tunnels can be authenticated using a local user database that resides in the tunnel terminator or an external RADIUS user database that resides on the same LAN as the tunnel terminator. When a relatively few number of users needs to be supported, using an internal database of users within the tunnel terminator is adequate.

Another RAS VPN setup is shown in Figure 7. In this setup, the remote office connects (extranet/partner access) to the Internet (ISP) through a bridge/router. The remote site can have either a dial-on-demand connection to the Internet or a permanent connection to the internet via a leased line.

Figure 7 RAS Extranet VPN Configuration



The user employs an application such as Microsoft's Dial Up Networking to initiate a tunnel with the tunnel terminator at the central site.

Again, the user is authenticated via a RADIUS server or an internal database. When the tunnel is established, the LAN extension mechanism makes the user appear to be directly attached to the local network.



In all of these configurations, the central site must be IP accessible to the ISP. That is, the ISP must be able to reach the tunnel terminator via the tunnel terminator's IP address.

Configuring the Central Site

This section contains general information and procedures for setting up the central site. The central site configuration is the same for both types of RAS VPNs described in this chapter.

At the central site, the tunnel terminator needs to be configured. A central site router may also be in the configuration. If this router protects the central site network using a firewall, you may need to configure the firewall to allow the tunnel traffic to reach the tunnel terminator. It is possible for the tunnel terminator to also be the central site router. However, in the examples in this guide, a NETBuilder II bridge/router is the central site router and a PathBuilder S500 switch is the tunnel terminator.

The procedures in this section describe configuring the PathBuilder S500 switch tunnel terminator.

Configuring the central site tunnel terminator requires that you complete the following tasks:

- Configuring IP and IPX Connectivity
- Configuring RAS
- Provisioning IP Addresses
- Configuring SNMP
- Setting Up System Basics
- Configuring RAS User Authentication

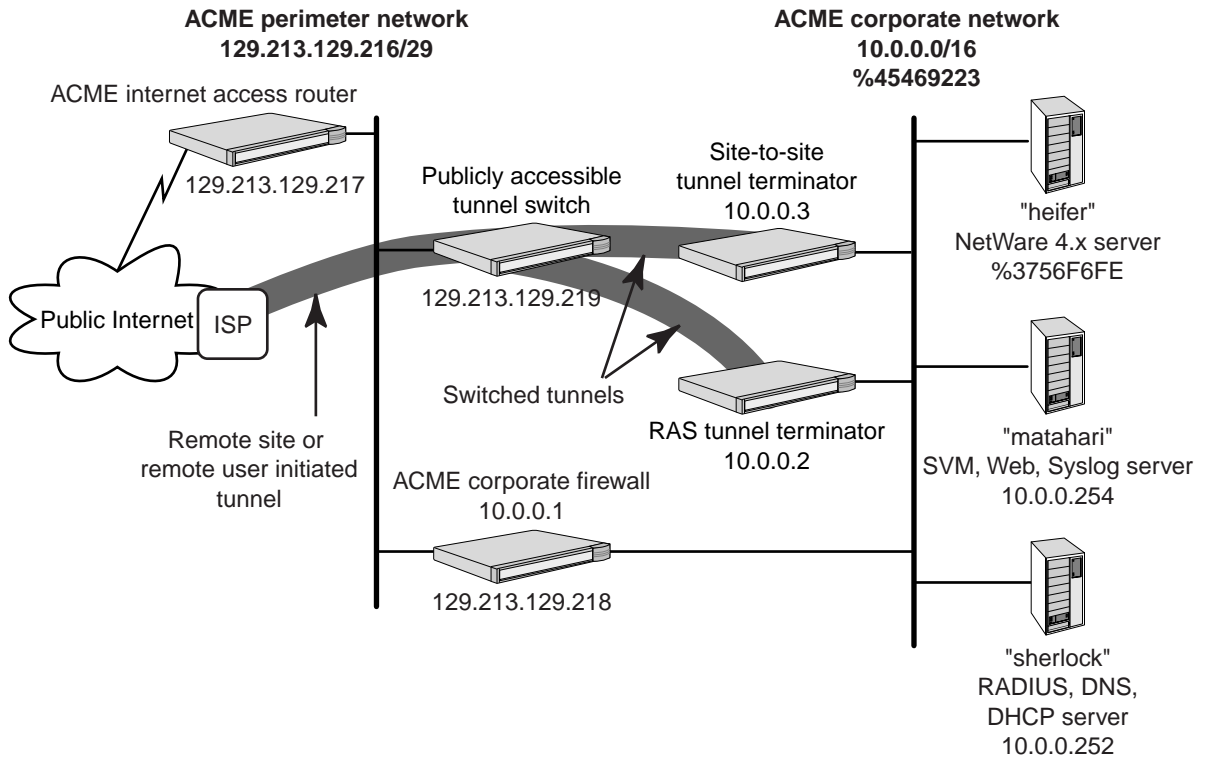


“Configuring Tunnel Switching,” an optional central site configuration, is described on page 37.

The procedures in the remainder of this chapter describe the configuration of the ACME Corporate VPN, shown in Figure 8.

The ACME Corporation VPN site has been set up by 3Com Marketing as a live VPN demonstration site. This site is accessible from anywhere in the world through the Internet. You can use the procedures in “Configuring the Client” on page 38 to set up the Microsoft Dial-Up Networking application to tunnel in to “ACME Corporation.”

Figure 8 ACME Corporation VPN Demonstration Site



The examples in the following sections show the commands used to configure the various components of the demo site. You can use the procedures in "Configuring the Client" to set up your client software and connect to the demo site.

In the following procedure, basic IP and IPX connectivity is set up with LAN IP and IPX addresses and subnet masks.



The ports have been given alphanumeric names so that they can be referred to by name.

Configuring IP and IPX Connectivity

To set up IP and IPX connectivity for the RAS tunnel terminator, follow these steps:

- 1 Name the port by entering:

```
SETDefault !1 -PORT Name = "public"
```

- 2 Establish basic IP and IPX connectivity by entering:

```
SETDefault !public -IP NETaddr = 10.0.0.2 255.255.0.0
SETDefault !public -IPX NETnumber = %45469223
SETDefault -IPX InternalNET = &DEADBEEF
```

- 3 Enable IP and IPX routing globally by entering:

```
SETDefault -IP CONTROL = ROute
SETDefault -IPX CONTROL = ROute
```

- 4 Set up a static override default route to allow this device to reach the Internet by sending any frames for "unknown" networks to another router which knows how to forward them appropriately by entering:

```
ADD -IP ROute 0.0.0.0 0.0.0.0 10.0.0.1 2 Override
```

Configuring RAS

To configure RAS, follow these steps:

- 1 Attach the IPNET address directly to a LAN port by entering:

```
SETDefault -RAS IPNetwork = 10.0.0.0
```

- 2 Make sure the IPXNETWORK does NOT exist elsewhere in the intranet and set up RAS by entering:

```
SETDefault -RAS IPXNETWORK = %DEADBEE0
SETDefault -RAS IPAddrPool = RemoteDhcpServer
SETDefault -RAS SecurityType = RADIUS
SETDefault -RAS PrimAuthSrvr = 10.0.0.252
SETDefault -RAS PrimACntSrvr = 10.0.0.252
SETDefault -RAS Secret = "secret"
SETDefault -RAS Log = (Syslog, ConSOLE, Connect, AuthFail, RsrcFail)
SETDefault -RAS CONTROL = Enable
```

Provisioning IP Addresses

To provision IP addressing, you have two major choices:

- The RAS tunnel terminator can proxy on behalf of RAS clients to a DHCP server on the corporate LAN.
- Or, you can enable a RAS address pool in the tunnel terminator.

When you enable DHCP support for tunnels on a DHCP server on the corporate LAN, LAN clients and tunnel clients are provided IP addresses by the DHCP server. There is no way of differentiating which addresses are assigned to which type of user. Address management for large networks can become quite cumbersome.

When you choose to use the RAS address pool alternative, IP addresses are provided to tunnel clients from the assigned pool of addresses. You can use this technique for logging and auditing purposes because tunnel users are provided well-known addresses, which are easily tracked and monitored.

Configuring DHCP Support Using a DHCP Server

To configure the internal DHCP server support for your remote clients and private LAN clients, you will create an address pool from which the DHCP server will offer addresses. Make sure the ProfDNS and/or ProfNetBiosNs settings matches the actual DNS or WINS (NETBios Name server) addresses. After it is configured, the DHCP service must be enabled and configured to use the defined AddressPool and not the default address pool.

If there is no need for DHCP services for LAN clients on the network, use the internal RAS Address Pool parameter in the DHCP service to provide addresses to RAS clients. No actual DHCP services need to be provided on that LAN. The RAS address pool needs only to be defined.

To configure a RAS address pool, follow these steps:

- 1 Define the RAS address pool by entering:

```
ADD !public -DHCP RasAddressPool 10.0.248.1 - 10.0.255.254 !P1
SETDefault -RAS IPAddrPool = LocalDhcpServer
SETDefault -DHCP CONTROL = Disable
```

- 2 Enable L2T service so that tunnels can be accepted by this bridge/router by entering:

```
SETDefault -L2T CONTROL = Enabled Protocol=ALL
```

Configuring SNMP To configure SNMP, follow these steps:

- 1 Configure SNMP to send traps to and be polled by the Secure VPN Manager application, Transcend Network Control Services, or another network management application, by entering:

```
ADD -SNMP COMMunity "acme" RW ALL
ADD -SNMP MANager "acme" 10.0.0.253 "ALL"
```

Where, 10.0.0.253 is the IP address of the network management application.

Setting Up System Basics To establish basic system settings, follow these steps:

- 1 Set up system information by entering:

```
SETDefault -SYS NMPrompt = "HQ RAS TT#"
SETDefault -SYS PROMpt = "HQ RAS TT>"
SETDefault -SYS SysCONTACT = "ACME Corp 408-555-1215"
SETDefault -SYS SysLOCation = "ACME Santa Clara, B200.2.029"
SETDefault -SYS SysNAME = "ACME VPN Demo Net - HQ RAS TT"
SETDefault -SYS WelcomeString = "Welcome to the VPN ACME site
router!"
SETDefault -SYS BannerString = "WARNING!!!^J^J^J^M^IThis is an
Access Controlled and Monitored Device.^J^M^IUnauthorized access
is prohibited!!^J^J^M"
```



Setting up system information is an optional step. You can use the Web Link application to establish and revise system identification information to suit your installation.

- 2 Establish the Primary and Secondary Name server to be used by this tunnel terminator to resolve names for PING and other services by entering:

```
SETDefault -IPName DomainName = "ACME.com"
SETDefault -IPName PrimaryNameServer = 129.213.129.1
SETDefault -IPName SecondaryNameServer = 139.87.48.242
```

Where IP addresses are those of the domain name servers on your company's network.

- 3 Establish the polling interval by entering:

```
SETDefault -WEblink StatPollInt = 1
```



If the ASCII boot feature is in use (you created a boot.cfg file in the configuration directory), all of these configuration changes will be lost after a system reboot. However, the configuration commands will have

been captured in the capture.cfg file in the configuration directory. By appending the contents of that file to the boot.cfg file, these configuration changes will not be lost. The configuration changes will also not be lost if the ASCII boot feature is disabled by changing the name of the boot.cfg file.

- 4 Rename the boot.cfg file so that any changes made to the system configuration will not be lost after a system reboot by entering:

```
REName boot.cfg boot.org
```

All changes will be logged to capture.cfg, but protected parameters will be replaced with asterisks.

Configuring RAS User Authentication

You can configure either an external RADIUS user database or a local user authentication database, which is a database of users that resides within the tunnel terminator.

When you use an external RADIUS user database you configure an external RADIUS support for RAS.

When you intend to use a local (within the tunnel terminator) user database you must do the following:

- Configure RAS tunnels with a local user authentication database.
- Define the remote users in a local database.
- Create virtual ports and associate user names with those virtual ports.

Configuring an External RADIUS Support for RAS

If an external RADIUS server is used, the security type parameter needs to be set to RADIUS. When RADIUS is set to support RAS authentication, the IP addresses for the primary authentication and accounting servers must be set to that server. Then you will need to configure the external RADIUS server with the user names and passwords for the clients that are allowed access to the tunnel terminator. Follow these steps:

- 1 To configure the SecurityType for an external RADIUS server use:

```
SETDefault -RAS SecurityType = [ Internal | RADIUS | EapRadius ]
```

- 2 Set the accounting and authorization servers to the IP address of the RADIUS server using:

```
SETDefault -RAS PrimACntSrvr = [<IP Address>]
SETDefault -RAS PrimAuthSrvr = [<IP Address>]
```

- 3 Optionally, a secondary authentication and accounting server can be designated using:

```
SETDefault -RAS SecACntSrvr = [<IP Address>]
SETDefault -RAS SecAuthSrvr = [<IP Address>]
```

- 4 The Secret parameter specifies the secret text string used for encryption between the router and the RADIUS server. Set the secret string on the router to match the RADIUS server's Radius Client using:

```
SETDefault -RAS Secret = <"string">
```

- 5 Make sure the UDP ports for authentication (default value 1645) and accounting (default value 1646) match the values defined in the RADIUS server. If these values do not match, you can change the values using:

```
SETDefault -RAS AuthUdpport = <UDP port number>
SETDefault -RAS ACntUdpport = <UDP port number>
```



When using an external user database, such as a RADIUS server, ports are created dynamically as they are needed. You do not need to create any RAS virtual ports.

- 6 Enable the RAS service using:

```
SETDefault -RAS CONTROL = [ Enabled | Disabled ]
```

- 7 Enable the L2T service so this router can accept the tunnels using:

```
SETDefault -L2T CONTROL = <Enabled | Disabled> protocol=<pptp |
l2tp | all>
```

Example RAS Services Configuration The following procedure is an example of how to configure RAS services for an external RADIUS database. An external DHCP server is used in this example.

To configure RAS services for an external RADIUS database on the tunnel terminator, follow these steps.

- 1 Set up the RAS services by entering:

```
SETDefault -RAS IPNetwork = 10.0.0.1
SETDefault -RAS IPAddrPool = RemoteDhcpServer
SETDefault -RAS SecurityType = Radius
SETDefault -RAS PrimAuthSrvr = 10.0.0.252
SETDefault -RAS PrimACntSrvr = 10.0.0.252
SETDefault -RAS Secret = "secret"
SETDefault -RAS Log (NoSyslog,ConSole,CoNnect,AuthFail,RsrcFail)
```

Where the IP addresses of the primary authentication and accounting servers are the IP address of the RADIUS server on your company's network.

- 2 Enable RAS by entering:

```
SETDefault -RAS CONTrol = Enabled
SETDefault -L2T CONTrol = Enabled
```



When -L2T is enabled, the protocol defaults to PPTP.

- 3 Create a port for one remote user, in case RADIUS cannot be reached, by entering:

```
ADD !V1 -Port VirtualPort RAS
ADD !V1 -PPP AuthRemoteUser ("root", "poot")
SETDefault !V1 -Port CONT = Enable
```

Configuring RAS Tunnels with a Local User Authentication Database



It is possible to add more than one user per port. However, when more than one user per port is configured, if both users attempt to gain access at the same time, only one user will be permitted. This configuration is keyboard intensive and may not be a practical method for supporting a large number of remote users.

To create a virtual port for each RAS user and then define the encryption type for the virtual port, follow these steps:

- 1 Define the default authentication using:

```
SETDefault -PPP AuthProToCol = [None | Pap | Chap | MS-Chap]
```

To ensure that the system uses MS-Chap for encryption, enter:

```
SETDefault -PPP AuthProToCol = MS-Chap
```

- 2 Create RAS a virtual ports for users by entering:

```
ADD !V1 -PORT VirtualPort RAS
ADD !V2 -PORT VirtualPort RAS
ADD !V3 -PORT VirtualPort RAS
```

- 3 Define the encryption type for each remote user. In this example, user 1 is assigned the factory default configure, user 2 is forced to use 128-bit encryption, and user 3 is allowed to use 40 bit, 128 bit or no encryption. Define an encryption policies by entering:

```
SETDefault !V1 -PPP ENcryptCONTROL = (NoMPPE40, NoMPPE128)
SETDefault !V2 -PPP ENcryptCONTROL = (NoMPPE40, MPPE128)
SETDefault !V3 -PPP ENcryptCONTROL = (MPPE40, MPPE128)
SETDefault !V1 -PPP ENcryptPolicy = None
SETDefault !V2 -PPP ENcryptPolicy = Required
SETDefault !V3 -PPP ENcryptPolicy = Allowed
```



The Encryption Policy parameter is available in Enterprise OS software version 11.3 and later.

Defining the Remote Users in a Local Database The AuthRemoteUser parameter controls access to a central host by multiple sites.

To add users to the local database, follow these steps:

- 1 For each remote user, specify the user ID and password by adding an AuthRemoteUser. The port must be re-enabled if this parameter is modified. PPP authenticates users prior to handing off requests to the RAS services. Enter:

```
ADD !V1 -PPP AuthRemoteUser ("user1", "password")
ADD !V2 -PPP AuthRemoteUser ("user2", "password")
ADD !V3 -PPP AuthRemoteUser ("user3", "password")
```

- 2 Enable the virtual ports by entering:

```
SETDefault !V1 -Port cont = Enable
SETDefault !V2 -Port cont = Enable
SETDefault !V3 -Port cont = Enable
```

- 3 Enable the RAS service by entering:

```
SETDefault -RAS CONTROL = Enable
```

- 4 Enable the L2T service so this router can accept the tunnels by entering:

```
SETDefault -L2T CONTROL = Enabled
```



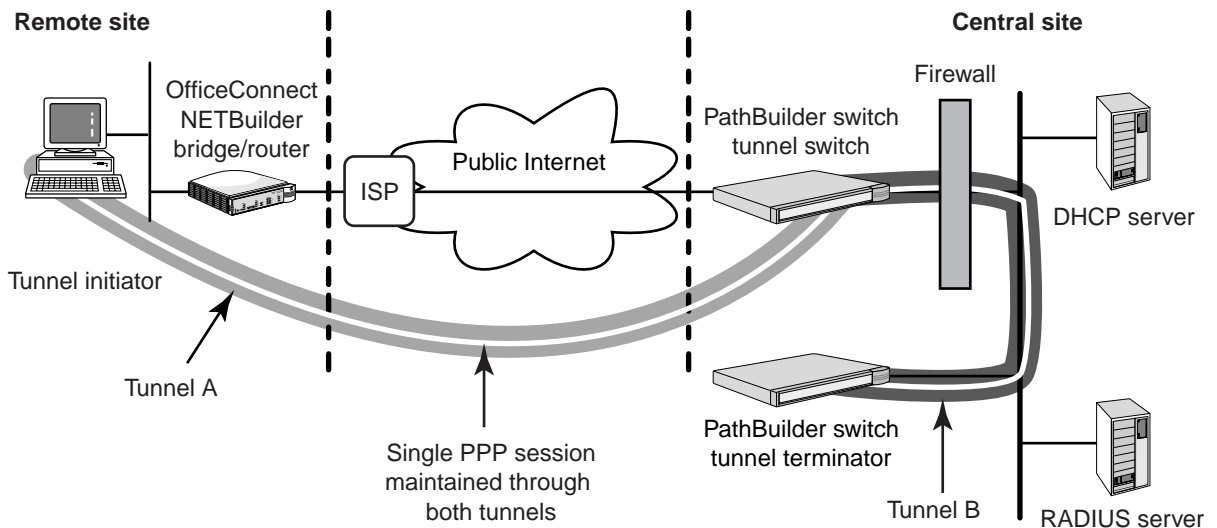
When -L2T is enabled, the protocol defaults to PPTP.

Configuring Tunnel Switching

Tunnel switching can be configured at the central site to enhance the security of the firewall operation and protect the corporate network. In Figure 9, one PathBuilder switch is the tunnel terminator and another is the tunnel switch. In this configuration, both PathBuilder switches use a RADIUS server for authentication.

After the RADIUS server authenticates user names that were submitted by the tunnel switch, it instructs the tunnel switch where to build the outgoing tunnel (to the tunnel terminator). You do not need to create virtual ports on the tunnel switch, because this is accomplished automatically based on the information received from the RADIUS server.

Figure 9 Tunnel Switching Example



This procedure assumes that both PathBuilder S500 switches are running Enterprise OS software version 11.3 or later, PW package.

The PathBuilder switch acting as the tunnel switch is connected through !1 Ethernet interface to the corporate perimeter network.

To configure the PathBuilder switch that is functioning as the tunnel switch, follow these steps:

- 1 Set up IP networking and enable tunneling by entering:

```
SETDefault !1 -IP NETaddr 129.213.129.219 255.255.255.192
ADD -IP ROUTe 0.0.0.0 129.213.129.217 1
SETDefault -L2T CONTrol = Enabled Protocol=ALL
```

- 2 Establish system settings by entering:

```
SETDefault -SYS NMPrompt = "PB500#"
SETDefault -SYS PROMpt = "PB500>"
SETDefault -SY SysCONTACT = "Operator"
SETDefault -SYS SysLOCation = "ACME Corporation"
SETDefault -SYS SysNAME = "ACME PB500"
SETDefault -SYS WelcmeString = "ACME Marketing Tunnel Switch"
SETDefault -SYS BannerString = "Welcome to ACME Tunnel Switch"
```

- 3 Set up the RADIUS service by entering:

```
SETDefault -RAS IPNetwork = 129.213.129.0
SETDefault -RAS SecurityType = Radius
SETDefault -RAS PrimauthSrvr = 10.0.0.252
SETDefault -RAS PrimACntSrvr = 10.0.0.252
SETDefault -RAS Secret = "secret"
SETDefault -RAS Log =(NoSyslog,ConSole,CoNnect,AuthFail,RsrcFail)
SETDefault -RAS CONTrol = Enable
```

Configuring the Client

In a RAS configuration, whether the client is a mobile or remote single user or a user on an extranet in a partner access situation, the client system is typically a PC running the Window 95/98 or Windows NT operating systems.

In addition, this client system must have an application that can perform the functions of a tunnel initiator and access the tunnel terminator. For example, you can use the Microsoft Dial-Up Networking application to create tunnel connections to the PathBuilder tunnel switch.



If you use Microsoft Dial-Up Networking on a Windows 95 machine, you must use version 11.3 or later. Windows NT requires service pack 3 or later. Do not enable compression on the tunnel link.

Configuring the Client Workstation

To configure Microsoft Dial-Up Networking on your PC, follow these steps:

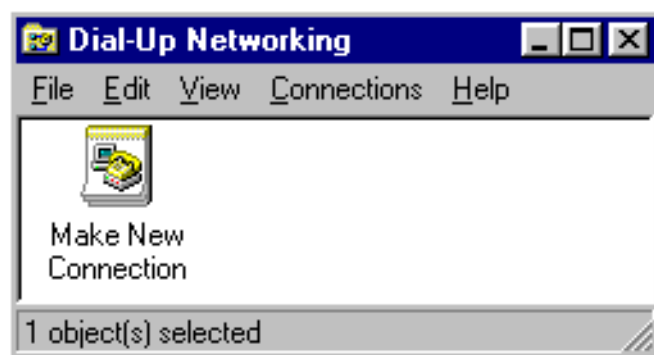
- 1 Download PPTP client software for your Windows 95/98 or NT workstation from the Microsoft web site. This software forms part of Dial-Up Networking (DUN) 1.3 or later and is a free download. Install the software on each PC that needs VPN connectivity.
- 2 If you are a single remote user, configure your modem to connect to the ISP as you normally would. Refer to the modem's user guide for instructions on how to do this. It is best to verify your connection to the Internet before trying to establish a VPN. Try to ping the PPTP server configured to be your tunnel terminator. Make sure your ISP does not block GRE traffic.



You can use Microsoft Dial-Up Networking to connect to your ISP. If you do, click the Make New Connection icon to create a connection object to use to connect to your ISP.

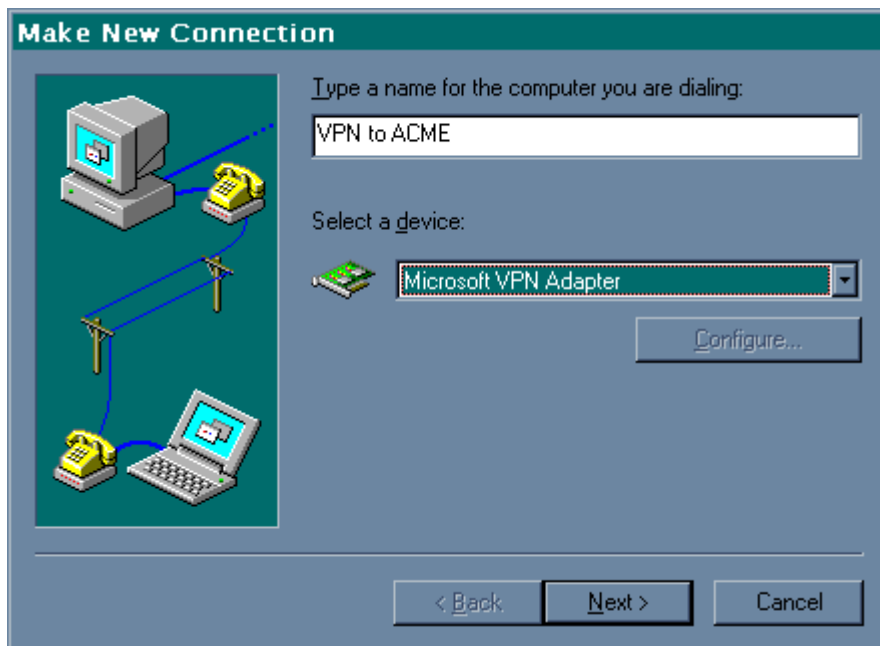
If you are operating in an extranet situation where your internet connection is maintained by your network router, you will not need to perform any user actions to make an ISP connection.

- 3 Locate and open the Dial-Up Networking folder.

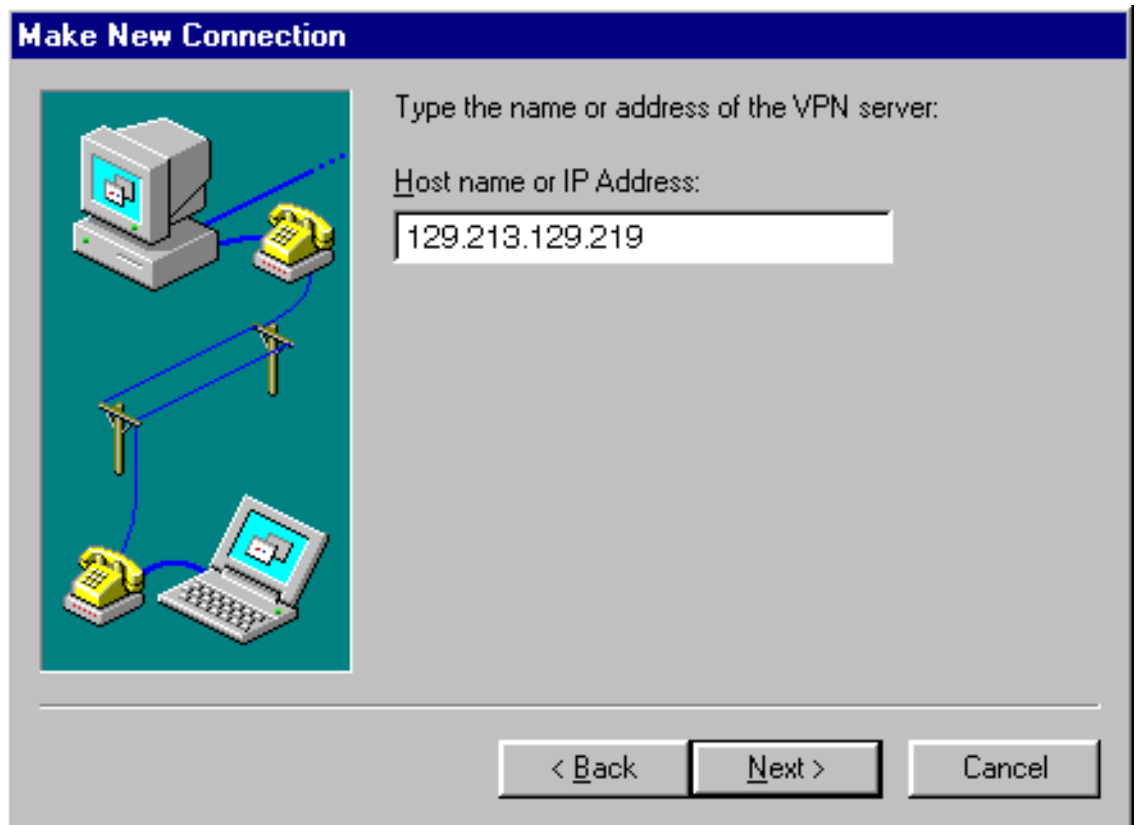


- 4 Double-click the Make New Connection icon.

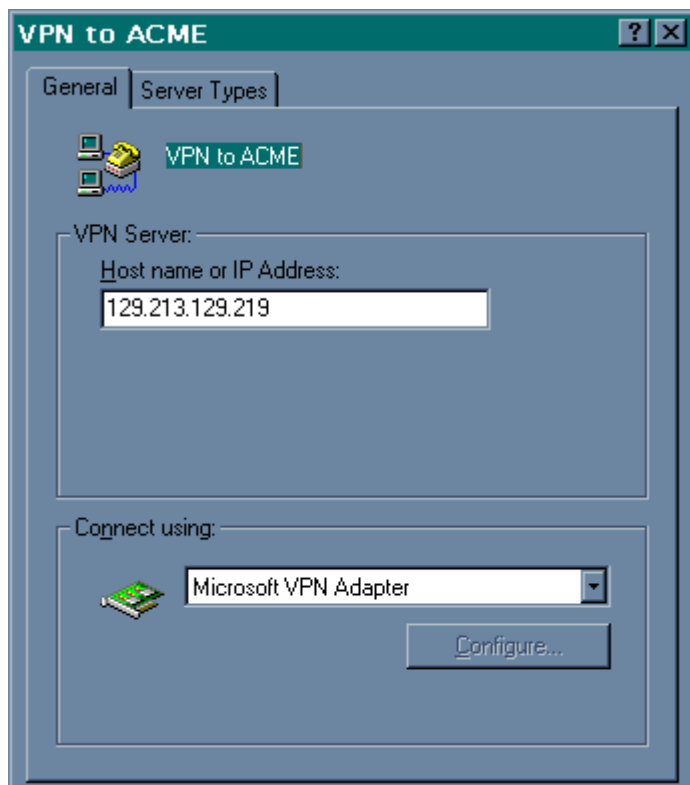
- 5 Type a name for the new dial-up profile, change the physical device from your default modem to the "Microsoft VPN Adapter," and click Next.



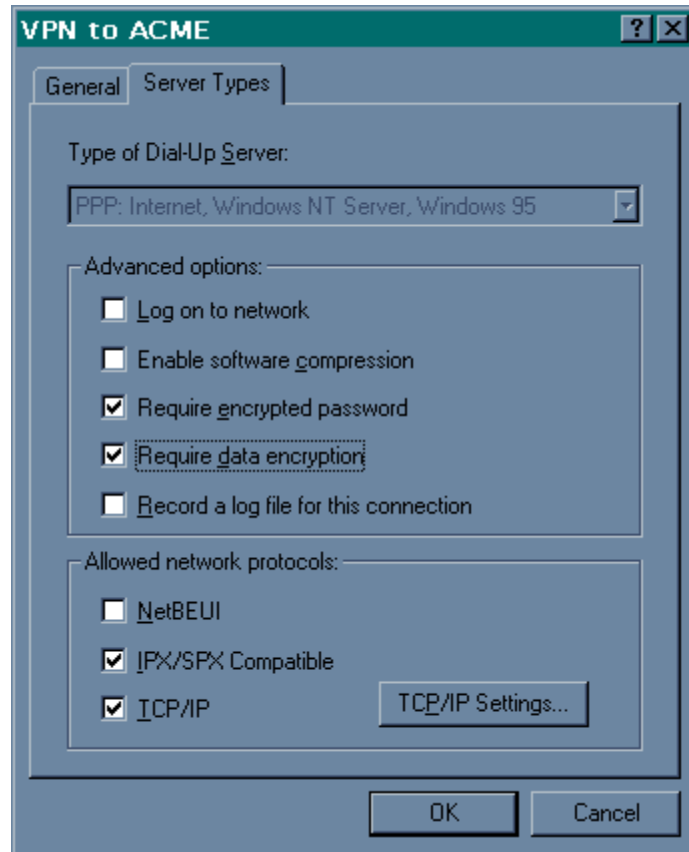
- 6 Enter the IP address (or DNS name, if one is defined) of the device your client will tunnel to. If your corporation only has a tunnel terminator, enter that tunnel terminator's IP address, and click Next. If your corporation has a tunnel switch and one or more tunnel terminators, enter the IP address (or DNS name) of the tunnel switch, and click Next.



- 7 Click Finish to complete the creation of this profile.
- 8 Right-click the new profile in the Dial-Up Networking folder and select Properties from the pop-up menu to configure this connection.



- 9 Click the Server Types tab.



- 10 In the Advanced options section, deselect (click to remove the checkmark) the Enable software compression box. If you do not have a Windows NT domain to log in to, you can deselect the Log on to network box as well. You will still have access to Windows network resources, but will be prompted for your username and password every time you attempt to access one of these resources.

11 If your corporate policy is to require encryption on VPN links and this policy is enforced at the central site, then you should also check the Require data encryption box. If a local user database is defined in the Enterprise OS platform then, this is controlled by the –PPP service EncryptCONTRol parameter. With RADIUS user databases this may or may not be an option in the RADIUS server. Please consult with your RADIUS server documentation for guidelines on defining and enforcing the encryption policy.

12 If you want to ensure that passwords are never exchanged with the tunnel terminator in clear text, which is readable by anyone, then you should check the box labeled Require encrypted password.

By default, the Microsoft Dial-Up Networking software configures your PC to use the most-recently connected dial-up connection as the default gateway for all IP traffic. Any traffic not destined for the directly-attached LAN (if there is one, otherwise all IP traffic) is sent to the tunnel terminator. In other words, traffic destined for somewhere else on the Internet travels across the Internet (inside the tunnel) to the tunnel terminator, then if corporate policy supports it, is sent back out to the Internet. Replies travel across the Internet to the tunnel terminator, then back across the Internet (inside the tunnel) to your PC. Each request and reply packet travels across the corporate Internet connection twice.

13 In the Allowed network protocols section, make sure that only the specific protocol(s) you want to use or are allowed to use for this VPN are checked. Enterprise OS platforms only support IP and IPX RAS, and the ACME demo site has both IP and IPX enabled. Leaving protocols checked that you cannot or will not use unnecessarily prolongs the login phase.

- 14 If you want Internet traffic to travel directly to the Internet and you want only traffic destined for the corporation to travel through the tunnel, click the TCP/IP settings button on the server types tab to open the TCP/IP Settings dialog box.

TCP/IP Settings [?] [X]

Server assigned IP address

Specify an IP address

IP address: 0 . 0 . 0 . 0

Server assigned name server addresses

Specify name server addresses

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Primary WINS: 0 . 0 . 0 . 0

Secondary WINS: 0 . 0 . 0 . 0

Use IP header compression

Use default gateway on remote network

OK Cancel

- 15 Deselect the box labeled Use default gateway on remote network. If your corporation has more than one subnetwork, you will need to explicitly add routes to those subnets to your PC after establishing the VPN connection. The gateway IP address to use will be the IP address you acquire from the tunnel terminator:

```
ROUTE [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]
```

Setting this option can be somewhat automated via a batch file. For example, assume you have two other subnets at the central site, 129.213.0.0/16 and 139.87.0.0/16. You can create a batch file that has the following two statements. Assume this batch file is called ACME.BAT:

```
ROUTE ADD 129.213.0.0 MASK 255.255.0.0 %1 METRIC 2
ROUTE ADD 139.87.0.0 MASK 255.255.0.0 %1 METRIC 2
```

Now, after completing the VPN connection, you can use the WINIPCFG program to determine your acquired IP address, and then issue the DOS command ACME <address>.

Connecting to the Tunnel Terminator

This section describes how to establish a tunnel connection with a tunnel terminator. To set up a connection to the ACME Corporation demo site, use the user names and passwords provided.

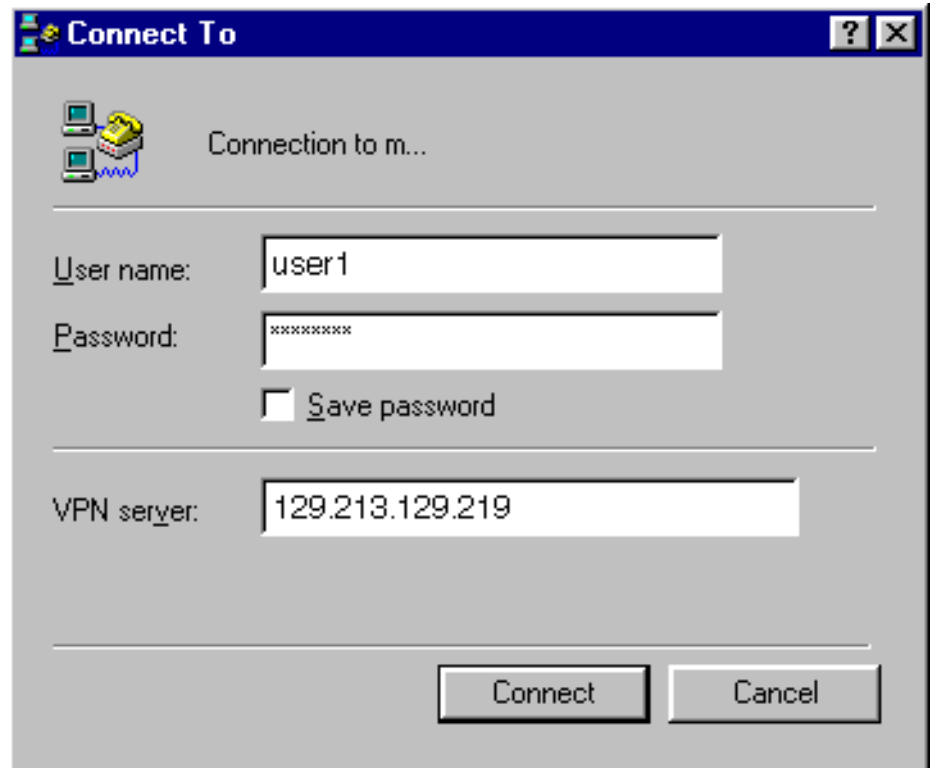
To establish a connection with the tunnel terminator, follow these steps:

- 1 Initiate a call to your ISP as you normally would.



If you are a user on a remote office LAN that has an internet connection, you do not need to open a connection to your ISP. Your network router opens and maintains this connection for you.

- From the Dial-Up Networking window, double-click the icon for your connection to the tunnel terminator that you have just created. The Connect To dialog box opens.



- Enter the user name and password configured for you at the central site.



To access the ACME demo site, use the following user names and password:

- User Names: user1 through user2000
- Password: password

Enter user names and passwords for the ACME demo site in lower case. When you type the password, asterisks instead of characters are displayed.

- 4 When Dial-Up Networking and your PPTP server have negotiated a tunnel between them, you are free to pass data to the remote LAN, access resources on the remote LAN, and use applications as if you were directly connected to that LAN.



Each workstation on a remote (extranet) LAN that wants to connect to the VPN must run Dial-Up Networking 1.3. Each workstation creates its own tunnel, even though it may share the same physical connection to the ISP.

For more information about PPTP, see article 162847 (Troubleshooting PPTP Connectivity Issued in Windows NT 4.0) on the Microsoft web site.

3

CONFIGURING SITE-TO-SITE VPNs

This chapter describes configuring site-to-site VPNs. In a site-to-site VPN, the configuration of the VPN depends on the type of internet access employed by the remote office.

The remote office can use either:

- A dial-on-demand configuration that accesses the internet only when users at the remote office require a connection to the central site, or
- A virtual leased line (VLL) configuration where the Internet service provider (ISP) connection is persistent at both ends.

Dial-up tunnels can be used as a primary connection mechanism when usage is noncontinuous.

Dial-up tunnels can also be used for disaster recovery and backup to existing private network configurations.

The virtual leased line configuration should not be used when the Internet service provider (ISP) connection is paid for in units of time. When the ISP is paid in units of time, a dial-on-demand configuration makes more economic sense.

When the ISP is paid at a fixed rate, the virtual leased line configuration can be used economically.



No specific user actions are required to connect to the central site. After configuration is complete, the applications that require a connection to the central site determine how to make that connection. In a dial-up configuration, the dial-up and connection process occurs without user intervention.

This chapter contains the following configuration procedures:

- Configuring the VLL Central Site Router
- Configuring the VLL Remote Site
- Configuring the Dial-Up Central Site Router
- Configuring Tunnel Switching
- Adding IPSec Security
- Configuring Internet Key Exchange (IKE)

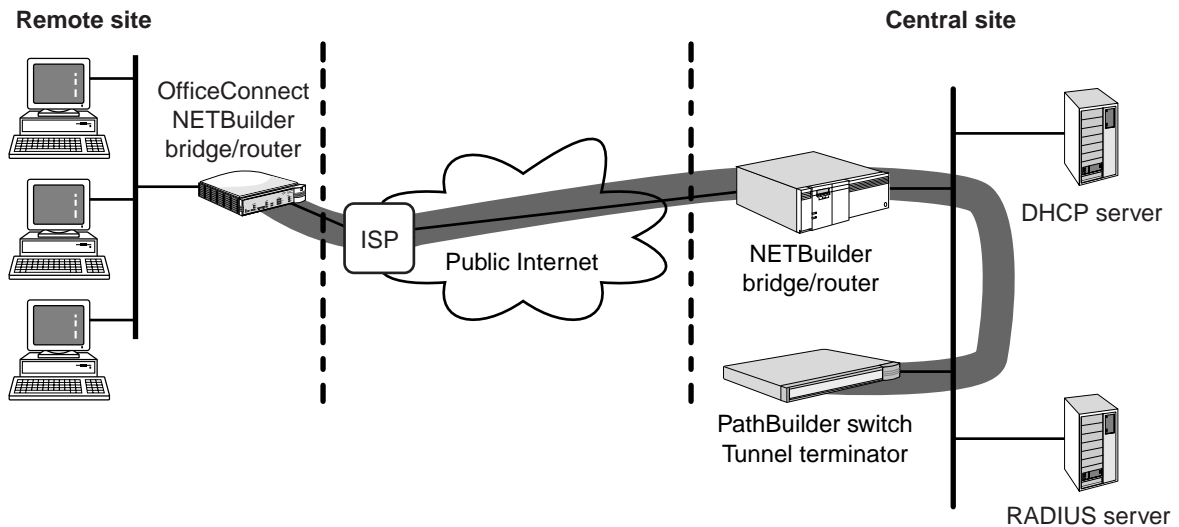
Configuring the VLL Central Site Router

This section describes configuring the central site router in a site-to-site VPN. Figure 10 is an example configuration.



The VLL tunneling configuration described below is an example only. You cannot use VLL tunnels to access the ACME demonstration site at this time. However, the VLL tunneling configuration files are available on the demonstration site for your use if you need them.

Figure 10 VLL Tunnels



Configuring the Central Site Router

To configure the central site PathBuilder switch tunnel terminator, follow these steps:

- 1 Assign the SCID by entering:

```
SETDefault -SYS SysCallerID = "HQ"
```

- 2 Set up public (!1) and private (!2) LAN IP addresses and subnet masks by entering:

```
SETDefault !1 -IP NETaddr = 139.87.37.205 255.255.252.0
```

```
SETDefault !2 -IP NETaddr = 10.0.0.1 255.255.255.0
```

- 3 Create virtual ports for site-to-site tunnels from remote offices. Use SCID as authentication mechanism for these peers.

```
ADD !V11 -PORT VirtualPort SysCallerID"demo1"
```

```
ADD !V12 -PORT VirtualPort SysCallerID"demo2"
```

```
ADD !V13 -PORT VirtualPort SysCallerID"demo3"
```

```
ADD !V14 -PORT VirtualPort SysCallerID"demo4"
```

```
ADD !V15 -PORT VirtualPort SysCallerID"demo5"
```

- 4 Define UnNumbered IP addresses for tunnels by entering:

```
SETDefault !V11 -IP NETaddr = UnNumbered
```

```
SETDefault !V12 -IP NETaddr = UnNumbered
```

```
SETDefault !V13 -IP NETaddr = UnNumbered
```

```
SETDefault !V14 -IP NETaddr = UnNumbered
```

```
SETDefault !V15 -IP NETaddr = UnNumbered
```

- 5 Enable IP routing globally on this router by entering:

```
SETDefault -IP CONTROL = ROute
```

- 6 Configure dynamic routing for tunnels. No dynamic routing protocol is used on the Ethernet interface (!1), which is the public port, to prevent advertising private addresses onto the public network. There is no need for advertising anything onto private net !2, to prevent the private net from being advertised to tunnel peer routers, use the -OSPF DirectPolicy. In addition, all remote offices must go through the central site to reach the Internet so they will abide by whatever corporate firewall policies are in place (no browsing <http://www.games.com> between hours of 8am and 5pm).

```
SETDefault -OSPF DefaultMetric = 1 Type1
```

```
SETDefault !2 -OSPF DirectPolicy = (Advertise,Type1)
```

```
SETDefault !V11 -OSPF CONTROL = Enable
```

```
SETDefault !V12 -OSPF CONTROL = Enable
```

```
SETDefault !V13 -OSPF CONTROL = Enable
```

```
SETDefault !V14 -OSPF CONTROL = Enable
```

```
SETDefault !V15 -OSPF CONTROL = Enable
```

- 7 Statically override the default route to allow this router to reach the Internet by entering:

```
ADD -IP ROUTE 0.0.0.0 0.0.0.0 139.87.36.1 2 Override
```

- 8 So that all private subnetworks can reach the rest of the Internet, all private addresses are translated to a single public address. Note that this is an outbound translation only and happens at session establishment going out this port. Session establishment attempts coming in to this port will fail with "wrong direction" errors. Because these session establishment attempts include tunnel setups, change the default translation failure action to PassThrough. Enter:

```
ADD !1 -NAT AddressMap 10.0.0.0/8 139.87.37.205/32 OutBound
SETDefault !1 -NAT CONTROL = Enabled
SETDefault !1 -NAT XlateFailAction = PassThrough
```

- 9 Enable L2T service so that tunnels can be accepted by this box. VLL peers can not be explicitly defined since they use dynamic addresses. Define dynamic tunnel peers for each expected tunnel initiator by entering:

```
ADD -L2T VLL 0.0.0.0
ADD -L2T VLL 0.0.0.0
ADD -L2T VLL 0.0.0.0
ADD -L2T VLL 0.0.0.0
ADD -L2T VLL 0.0.0.0
SETDefault -L2T CONTROL = Enabled
```

- 10 Name ports and set up the name service by entering:

```
SETDefault !1 -PORT NAME = "corp_net"
SETDefault !2 -PORT NAME = "priv_net"
SETDefault !3 -PORT NAME = "ISDN_B1"
SETDefault !4 -PORT NAME = "ISDN_B2"
SETDefault !5 -PORT NAME = "flexwan1"
SETDefault !6 -PORT NAME = "flexwan2"
SETDefault !V11 -PORT NAME = "remote01"
SETDefault !V12 -PORT NAME = "remote02"
SETDefault !V13 -PORT NAME = "remote03"
SETDefault !V14 -PORT NAME = "remote04"
SETDefault !V15 -PORT NAME = "remote05"
SETDefault -SYS NMPrompt = "HQ#"
SETDefault -SYS PROMpt = "HQ>"
SETDefault -SYS SysCONTACT = "yourname@yourcompany.com"
SETDefault -SYS SysLOCation = "Second Floor"
SETDefault -SYS SysNAME = "HQ"
SETDefault -SYS WelcomeString = "Welcome to the VPN central site!"
```

- 11 Set up the primary and secondary name servers used by this PathBuilder switch to resolve names for PING by entering:

```
SETDefault -IPName DomainName = "mycompany.com"
SETDefault -IPName PrimaryNameServer = 139.87.48.242
SETDefault -IPName SecondaryNameServer = 139.87.52.10
```

- 12 Allow this PathBuilder switch to act as DHCP server for private LAN clients. ProfDNS should be changed to match actual DNS servers. Enter:

```
ADD !2 -DHCP AddressPool 10.0.0.2 - 10.0.0.127 !P1
SETDefault !P1 -DHCP ProfDNS = 139.87.48.242, 139.87.52.10
SETDefault !2 -DHCP CONTROL = AddressPool
SETDefault !2 -DHCP CONTROL = Enabled
```

Configuring the VLL Remote Site

The following configuration example assumes an OfficeConnect NETBuilder model 142 bridge/router with (NW package) software version 11.0 or later with no encryption places ISDN calls into an ISP, acquires an IP address dynamically, and tunnels in to the central site.

To configure the remote site OfficeConnect NETBuilder model 142 bridge/router, follow these steps:

- 1 Configure basic system parameters by entering:

```
SETDefault -SYS NMPrompt = "demol#"
SETDefault -SYS PROMpt = "demol>"
SETDefault -SYS SysCallerID = "demol"
SETDefault -SYS SysCONTACT = "SystemAdmin"
SETDefault -SYS SysLOCation = "Second floor"
SETDefault -SYS SysNAME = "demol"
SETDefault -SYS WelcomeString = "Welcome to the VPN demonstration OCNB!!"
```

- 2 Configure the ISDN interface by entering:

```
SETDefault !2.1 -PAtH LocalDialNo = "4085551212"
SETDefault !2.2 -PAtH LocalDialNo = "4085551212"
```

- 3 If you are in North America, run SpidWIZard by entering:

```
SETDefault !2 -PAtH SpidWIZard = Trigger
SETDefault !2 -PAtH CONTROL = Enabled
```

- 4 If you are not in North America, explicitly configure the ISDN switch type by entering:

```
SETDefault !2 -PAtH SwitchType = ETSI
SETDefault !2 -PAtH CONTROL = Enabled
```

- 5 Put both ISDN paths into a dynamic dial pool personal preference, which is not mandatory, but is necessary if dialing more than one ISP is ever needed, by entering:

```
SETDefault !2.1 -PATH DialCONTRol = DYnamic
SETDefault !2.2 -PATH DialCONTRol = DYnamic
SETDefault !2 -PATH PhantomPower = Disable
```

- 6 Name ports and set up the name service by entering:

```
SETDefault !1 -PORT NAmE = "eth"
SETDefault !4 -PORT NAmE = "flexwan"
SETDefault !V1 -PORT NAmE = "MCI"
SETDefault !V2 -PORT NAmE = "HQ_PPTP"
```

- 7 Create virtual ports. It is not necessary to use a virtual port for a connection to an ISP. In this example, MCI = Internet Service Provider and HQ_PTP = PPTP tunnel to headquarters. Enter:

```
ADD !MCI -PORT VirtualPort SysCallerID"ISP"
ADD !HQ_PPTP -PORT VirtualPort SysCallerID"HQ"
```

- 8 Set up DoD/BoD for ISP access on VP1 by entering:

```
SETDefault !MCI -PORT OWNEr = PPP
SETDefault !MCI -PORT NORMAlBandwidth = 64
SETDefault !MCI -PORT BODIncrLimit = 64
SETDefault !MCI -PORT DialInitStat = DialOnDemand
SETDefault !MCI -PORT BODThreshhold = 1
SETDefault !MCI -PORT DialSamplPeriod = 1, 300
SETDefault !MCI -PORT DialIdleTime = 600
```



To achieve MLPPP two separate dial number list entries are needed. If the ISP only has one phone number, add a nondialing character into the string(s) to make them unique by entering:

```
ADD !MCI -PORT DialNoList "1 408 555 1212 A" Baud=64 Type=Bri
ADD !MCI -PORT DialNoList "1 408 555 1212 B" Baud=64 Type=Bri
SETDefault !MCI -PPP MlpCONTRol = Enabled
SETDefault !MCI -PPP AuthLocalUser = ("username_at_isp",
"password")
SETDefault !MCI -PORT COMPRESSType = PerPacket
```

- 9 Set up IP addresses and routing. The V1 IP address is acquired through IPCP negotiation with the ISP, and V2 can be unnumbered. Enter:

```
SETDefault !1 -IP NETaddr = 10.1.0.1 255.255.255.0
SETDefault !MCI -IP NETaddr = IPCPA
SETDefault !QH_PPTP -IP NETaddr = UnNumbered
SETDefault -IP CONTROL = ROute
SETDefault !1 -OSPF DirectPolicy = (Advertise,Type1)
SETDefault !QH_PPTP -OSPF DemandInterface = Enabled
SETDefault !QH_PPTP -OSPF CONTROL = Enabled
ADD -IP ROute 0.0.0.0 0.0.0.0 !V1 2 Override
```

- 10 Reinitialize the paths and ports by entering:

```
SETDefault !2.1 -PATH CONTROL = Enabled
SETDefault !2.2 -PATH CONTROL = Enabled
SETDefault !MCI -PORT CONTROL = Enabled
```

- 11 Primary and Secondary Name servers are used by this NETBuilder bridge/router to resolve names for PING. Enter:

```
SETDefault -IPName DomainName = "mycompany.com"
SETDefault -IPName PrimaryNameServer = 198.41.0.4
SETDefault -IPName SecondaryNameServer = 192.33.4.12
```

- 12 Allow this bridge/router to act as DHCP server for LAN clients. ProfDNS should be changed to match actual DNS servers by entering:

```
ADD !1 -DHCP AddressPool 10.1.0.3 - 10.1.0.50 !P1
SETDefault !P1 -DHCP ProfDNS = 198.41.0.4, 192.33.4.12
SETDefault !1 -DHCP CONTROL = AddressPool
SETDefault !1 -DHCP CONTROL = Enabled
```

- 13 Enable L2T service so that tunnels can be initiated by this router, and add the VLL entry for the central site by entering:

```
SETDefault -L2T CONTROL = Enabled
ADD -L2T VLL 139.87.37.205
```

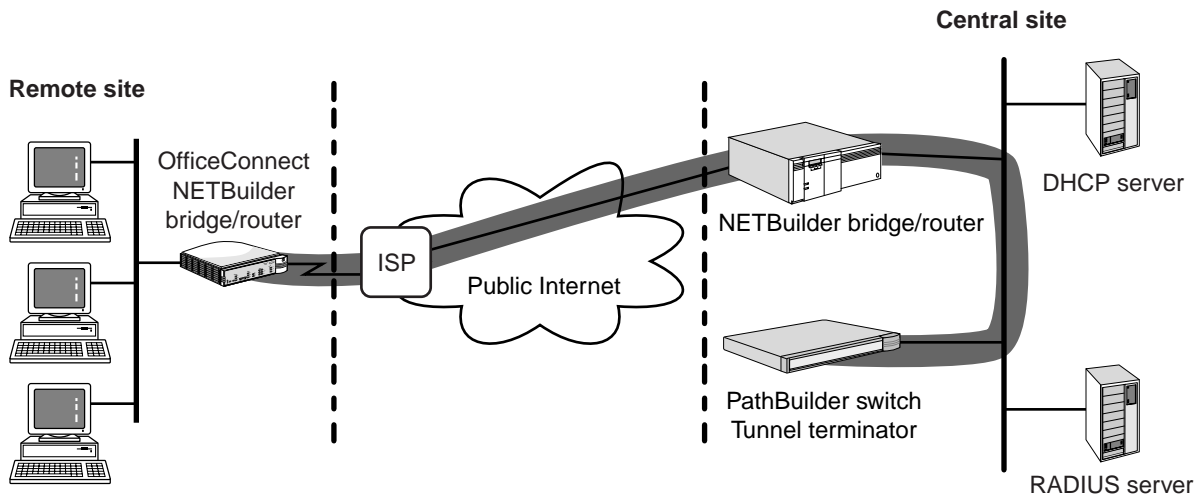
- 14 Finally, make sure that NAT is converting the private LAN addresses to the public address acquired through IPCP from the access concentrator we called by entering:

```
SETDefault !MCI -NAT IPCPAddressMap = Enable 0.0.0.0/0
SETDefault !MCI -NAT CONTROL = Enable
```

Configuring the Dial-Up Central Site Router

This section describes configuring the central site tunnel terminator in a site-to-site VPN with dial-up access shown in Figure 11. The following procedure shows configuring a PathBuilder S5xx tunnel switch running Enterprise OS software version 11.3 or later, PE or PS package. It is connected through port the !1 Ethernet interface to the Corporate network and terminates PPTP and L2TP tunnels from remote routers. Tunnels are all UnNumbered, and OSPF and NLSP are run over those tunnels to dynamically exchange routes.

Figure 11 Site-to-Site Dial-Up Configuration



To configure the central site PathBuilder tunnel terminator, follow these steps:

- 1 Set up LAN IP and IPX addresses by entering:



The port is first named so that it can be referred to by name.

```
SETDefault !1 -PORT NAME = "public"
SETDefault !public -IP NETaddr = 10.0.0.3 255.255.0.0
SETDefault !public -IPX NETnumber = %45469223
SETDefault -IPX InternalNET = &DEADBEE1
```

- 2 Enable IP and IPX routing globally on this bridge/router by entering:

```
SETDefault -IP CONTROL = RRoute
SETDefault -IPX CONTROL = RRoute
```

- 3 Create virtual ports for router to router dial tunnels from remote offices. Use PAP/CHAP as authentication mechanism for these peers by entering:

```
ADD !V1 -PORT VirtualPort PPP
ADD !V2 -PORT VirtualPort PPP
ADD !V3 -PORT VirtualPort PPP
ADD !V4 -PORT VirtualPort PPP
```

- 4 Define AuthRemoteUser values for PPP virtual ports by entering:

```
ADD !V1 -PPP AuthRemoteUser ("remote1", "password")
ADD !V2 -PPP AuthRemoteUser ("remote2", "password")
ADD !V3 -PPP AuthRemoteUser ("remote3", "password")
ADD !V4 -PPP AuthRemoteUser ("remote4", "password")
```

This allows you to determine which virtual ports to bind incoming connections to. Since you are not calling out to the remote sites, you do not need to define DialNoList entries for these virtual ports. PPTP and L2TP connections are accepted on these virtual ports.

- 5 Define UnNumbered IP addresses for tunnels by entering:

```
SETDefault !V1-!V256 -IP NETaddr = UnNumbered
```

- 6 Enable OSPF on LAN and tunnels by entering:

```
SETDefault !1 -OSPF CONTROL = Enable
SETDefault !V1-!V256 -OSPF CONTROL = Enable
```

- 7 Enable L2T service so that tunnels can be accepted by this bridge/router by entering:

```
SETDefault -L2T CONTROL = Enabled Protocol = All
```

- 8 Configure SNMP to send traps to and be polled by the Secure VPN Manager application by entering:

```
ADD -SNMP COMMunity "acme" RW ALL
ADD -SNMP MANager "acme" 10.0.0.253 "ALL"
```

Where the IP address is that of the SNMP trap recipient such as the Transcend Secure VPN Manager or Transcend Network Control Services applications.

- 9 Set up system information and define strings to be shown before and after user logs in to console or telnet by entering:

```
SETDefault -SYS NMPrompt = "HQ R2R TT#"
SETDefault -SYS PROMpt = "HQ R2R TT>"
SETDefault -SYS SysCONTACT = "manager@ACME.com 555-555-1215"
SETDefault -SYS SysLOCation = "ACME Santa Clara"
SETDefault -SYS SysNAME = "VPN Demo Net - HQ R2R TT"
SETDefault -SYS WelcomeString = "Welcome to the VPN router!"
SETDefault -SYS BannerString = "^J^I^I^IWARNING!!!^J^J^J^M^IThis
is an Access Controlled and Monitored Device.^J^M^IUnauthorized
access is prohibited!!!^J^J^M"
```

- 10 Establish the Primary and Secondary Name servers to be used by this bridge/router to resolve names for PING by entering:

```
SETDefault -IPName DomainName = "ACME.com"
SETDefault -IPName PrimaryNameServer = 129.213.129.1
SETDefault -IPName SecondaryNameServer = 139.87.48.242
SETDefault -WEblink StatPollInt = 1
```



If the ASCII boot feature is in use (you created a boot.cfg file in the configuration directory), all of these configuration changes will be lost after a system reboot. However, the configuration commands will have been captured in the capture.cfg file in the configuration directory. By appending the contents of that file to the boot.cfg file, these configurative changes will not be lost. The configuration changes will also not be lost if the ASCII boot feature is disabled by changing the name of the boot.cfg file.

- 11 Rename boot.cfg so that any changes made to the system configuration will not be lost after a system reboot. Enter:

```
REName boot.cfg boot.org
```



All changes are logged to capture.cfg, but protected parameters are replaced with asterisks.

Configuring the Dial-Up Remote Site

This section contains a configuration example for a remote site to central site VPN using a dial-up method.

The remote office site-to-site tunnel configuration assumes an OfficeConnect NETBuilder model 142 bridge/router is running (NW, NE, or NS package) Enterprise OS software version 11.2 or later. The remote site router places ISDN calls into an ISP, obtains a dynamic IP address from the ISP, performs many-to-one NAT outbound to ISP tunnels to the central site as a routed connection over an UnNumbered tunnel, and runs OSPF over a tunnel.

To configure the remote site bridge/router for site-to-site dial-up tunnels, follow these steps:

- 1 Configure ISDN by entering:

```
SETDefault !2.1 -PAth LocalDialNo = "4089860448"  
SETDefault !2.2 -PAth LocalDialNo = "4089860540"
```

- 2 If you are in North America, run SpidWIZard by entering:

```
SETDefault !2 -PAth SpidWIZard = Trigger
```

- 3 If SPID Wizard fails, or if you are not in North America enter:

```
SETDefault !2 -PAth SwitchType = NI1  
SETDefault !2.1 -PAth SPIDdn1 = "408986044800"  
SETDefault !2.2 -PAth SPIDdn2 = "408986054000"
```

- 4 Add both ISDN paths to the dial pool so that any logical port that needs an ISDN BRI B channel can dynamically claim and use them by entering:

```
SETDefault !2.1 -PAth DialCONTRol = DYnamic  
SETDefault !2.2 -PAth DialCONTRol = DYnamic  
SETDefault !2 -PAth CONTRol = Enabled
```

- 5 Create a virtual port for ISP dial connection by entering:

```
ADD !V1 -PORT VirtualPort ppp
```

- 6 Create virtual port for tunnel to headquarters (central site) by entering:

```
ADD !V2 -PORT VirtualPort ppp
```



The port(s) are named so that we can thereafter refer to the port(s) by name.

```
SETDefault !1 -PORT NAmE = "lan"  
SETDefault !V1 -PORT NAmE = "ISP"  
SETDefault !V2 -PORT NAmE = "tunnel"
```

- 7 Set up IP addressing for the LAN by entering:

```
SETDefault !lan -IP NETaddr = 10.1.0.1 255.255.255.0
```
- 8 Define IP addressing for the ISP dial connection by entering:

```
SETDefault !ISP -IP NETaddr = IPCPAddress
```
- 9 Define IP addressing for the tunnel to the central site by entering:

```
SETDefault !tunnel -IP NETaddr = UnNumbered
```
- 10 Allow this router to act as a DHCP server for LAN clients by entering:

```
ADD !lan -DHCP AddressPool 10.1.0.2 - 10.1.0.254 !P1  
SETDefault !P1 -DHCP ProfDNS = 10.0.0.252, 129.213.128.9  
SETDefault !P1 -DHCP ProfNetbios = 10.0.0.252  
SETDefault !P1 -DHCP ProfDomainName = "acme.com"  
SETDefault !1 -DHCP CONTROL = (Enabled, AddressPool, IcmpCheck)
```
- 11 Enable IP routing globally by entering:

```
SETDefault -IP CONTROL = Route
```
- 12 Create a static host route for the tunnel destination that points to the ISP. This ensures that traffic comprising the tunnel is routed across the internet and not pushed into the tunnel itself. Enter:

```
ADD -IP ROUTe 129.213.129.219 !ISP 1
```
- 13 Enable OSPF on tunnel so we can learn "corporate" networks. A direct policy for local Ethernet allows us to advertise our LAN into the OSPF domain without sending unnecessary Hellos onto our LAN. Enter:

```
SETDefault !tunnel -OSPF CONTROL = Enable  
SETDefault !lan -OSPF DirectPolicy = (Advertise, Type1)
```
- 14 Add a static default route to allow this device to reach the Internet by sending any frames for "unknown" networks to the ISP, which knows how to forward them appropriately. Enter:

```
ADD -IP ROUTe 0.0.0.0 !ISP 1
```

Or, create a static default route to the tunnel terminator so that all traffic sourced from this LAN must travel through tunnel and abide by corporate firewall policies. This remote office is then prevented from using ISP for anything except connectivity to central site. Enter:

```
ADD -IP ROUTe 0.0.0.0 !tunnel 2
```

- 15 Set up dial-on-demand/bandwidth-on-demand (DoD/BoD) for the ISP dial-up connection by entering:

```
SETDefault !ISP -PORT OWner = PPP
SETDefault !ISP -PORT NORMAlBandwidth = 64
SETDefault !ISP -PORT BODIncrLimit = 64
SETDefault !ISP -PORT DialInitStat = DialOnDemand
SETDefault !ISP -PORT BODThreshhold = 1
SETDefault !ISP -PORT DialSamplPeriod = 1, 300
SETDefault !ISP -PORT DialIdleTime = 600
```

- 16 To achieve MLPPP, two separate dialnolist entries are needed. If the ISP only has one phone number, add a nondialing character into the string(s) to make them unique by entering:

```
ADD !ISP -PORT DialNoList "1 408 380 1100 A" Baud=64 Type=Bri
ADD !ISP -PORT DialNoList "1 408 380 1100 B" Baud=64 Type=Bri
```

- 17 Send an endpoint discriminator, so the central site does not incorrectly bundle multiple instances of the same "user" logging in into one MLP bundle by entering:

```
SETDefault !ISP -PPP TxEndpointDisc = Enabled
SETDefault !ISP -PPP MlpCONTRol = Enabled
```

- 18 Define user id and password for ISP dialup connection by entering:

```
SETDefault !ISP -PPP AuthLocalUser = ("ISP_username",
"ISP_password")
```

- 19 Enable NAT on the tunnel dial-up connection, to convert private LAN addresses to dynamically-learned public RAS IP address by entering:

```
SETDefault !ISP -NAT IPCPAddressMap = Enable 0.0.0.0/0
SETDefault !ISP -NAT CONTRol = Enable
```

- 20 Define user ids and passwords for tunnel connection by entering:

```
SETDefault !tunnel -PPP AuthLocalUser = ("remotel" "password")
```

Where user names Remote1 through Remote127 can be used for PPTP tunnels and Remote128 to Remote254 for L2TP tunnels.

- 21 Set up BoD/DoD for the tunnel by entering:

```
SETDefault !tunnel -PORT OWner = PPP
SETDefault !tunnel -PORT NORMAlBandwidth = 64
SETDefault !tunnel -PORT BODIncrLimit = 128
SETDefault !tunnel -PORT BODThreshhold = 1
SETDefault !tunnel -PORT DialSamplPeriod = 1, 300
SETDefault !tunnel -PORT DialIdleTime = 600
ADD tunnel -PORT DialNoList "@129.213.129.219" Type=PPTP
SETDefault !tunnel -PORT DialInitState = DialOnDemand
```

- 22 Enable L2T service so that tunnels can be initiated by this bridge/router by entering:

```
SETDefault -L2T CONTrol = Enabled Protocol=ALL
```

- 23 Establish system setting and define strings to be shown before and after user logs in to console or telnet by entering:

```
SETDefault -SYS NMPrompt = "remote01#"
SETDefault -SYS PROMpt = "remote01>"
SETDefault -SYS SysCONtact = "your_name@your_com.com"
SETDefault -SYS SysLOCation = "somewhere in space and time"
SETDefault -SYS SysNAME = "remote01"
SETDefault -SYS WelcmeString = "Welcome to remote01 - a VPN
router!"
SETDefault -SYS BannerString "^J^I^I^IWARNING!!!^J^J^J^M^IThis is
an Access Controlled and Monitored Device.^J^M^IUnauthorized
access is prohibited!!^J^J^M"
```

- 24 Establish Primary and Secondary Name servers that are to be used to resolve names for PING etc. by entering:

```
SETDefault -IPName DomainName = "ACME.com"
SETDefault -IPName PrimaryNameServer = 129.213.129.1
SETDefault -IPName SecondaryNameServer = 139.87.48.242
SETDefault -WEBLink StatPollInt = 1
```



If the ASCII boot feature is in use (you created a boot.cfg file in the configuration directory), all of these configuration changes will be lost after a system reboot. However, the configuration commands will have been captured in the capture.cfg file in the configuration directory. By appending the contents of that file to the boot.cfg file, these configuration changes will not be lost. The configuration changes will also not be lost if the ASCII boot feature is disabled by changing the name of the boot.cfg file.

- 25 Rename the boot.cfg file so that any changes made to the system configuration are not lost after a system reboot. All changes are logged to capture.cfg, but protected parameters are replaced with asterisks. Enter:

```
REName boot.cfg boot.org
```

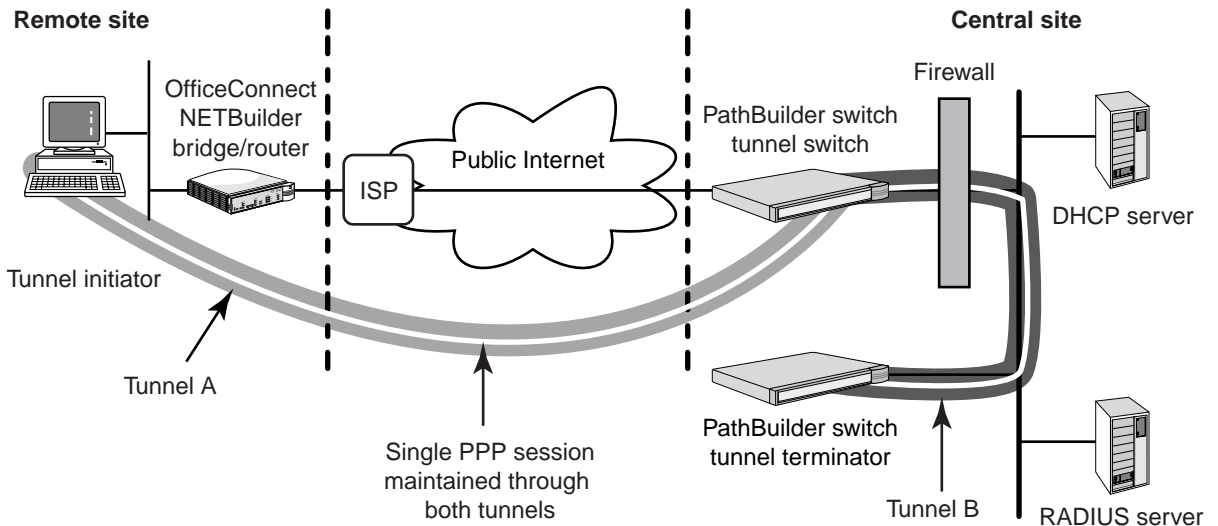
Configuring Tunnel Switching

In Figure 12, one PathBuilder switch is the tunnel terminator, another PathBuilder switch is the tunnel switch. In this configuration, the tunnel terminator uses a RADIUS server for authentication for a single defined user.



Tunnel switching cannot be used in a VLL configuration because in a VLL configuration authentication must be accomplished using the SysCallerId mechanism.

Figure 12 Tunnel Switching



This procedure assumes the PathBuilder S5xx tunnel switch is running Enterprise OS software version 11.2, PS package, and is connected through the Ethernet interface (!1) to the Corporate network.

An external RADIUS server is being used for authentication and accounting of RAS users, and an internal user database is used for router-to-router tunnel switching.



The port(s) are named they can be referred to by that name.

To set up the tunnel switch configuration, follow these steps:

- 1 Set up LAN IP addresses and subnet masks. Enter:

```
SETDefault !1 -PORT Name = "public"
SETDefault !public -IP NETaddr = 129.213.129.219 255.255.255.248
```

- 2 Enable IP routing globally by entering:

```
SETDefault -IP CONTROL = RRoute
```

- 3 Establish a static override default route to allow this device to reach the Internet by sending any frames for "unknown" networks to another router that knows how to forward them appropriately by entering:

```
ADD -IP ROUTE 0.0.0.0 0.0.0.0 129.213.129.218 2 Override
```

- 4 RAS is configured to allow RAS user authentication against the RADIUS server and get back tunnel attributes for those usernames. The IPNETaddress must be a directly attached LAN port. Enter:

```
SETDefault -RAS IPNetwork = 129.213.129.216
SETDefault -RAS IPAddrPool = RemoteDhcpServer
SETDefault -RAS SecurityType = RADIUS
SETDefault -RAS PrimAuthSrvr = 10.0.0.252
SETDefault -RAS PrimACntSrvr = 10.0.0.252
SETDefault -RAS Secret = "secret"
SETDefault -RAS Log = (Syslog,ConSole,CoNnect,AuthFail,RsrcFail)
SETDefault -RAS CONTROL = Enable
```

- 5 Create virtual ports for site-to-site dial tunnels from remote offices. Use PAP/CHAP as the authentication mechanism for these peers. Enter:

```
ADD !V1 -PORT VirtualPort TunnelSwitch
ADD !V2 -PORT VirtualPort TunnelSwitch
ADD !V3 -PORT VirtualPort TunnelSwitch
ADD !V4 -PORT VirtualPort TunnelSwitch
```

- 6 Define AuthRemoteUser values for PPP virtual ports which allows us to determine which virtual ports to bind incoming connections to. Enter:

```
ADD !V1 -PPP AuthRemoteUser ("remote1", "password")
ADD !V2 -PPP AuthRemoteUser ("remote2", "password")
ADD !V3 -PPP AuthRemoteUser ("remote3", "password")
ADD !V4 -PPP AuthRemoteUser ("remote4", "password")
```


- 12 Rename `boot.cfg` so that any changes made to the system configuration are not lost after a system reboot. All changes are logged to `capture.cfg`, but protected parameters are replaced with asterisks. Enter:

```
REName boot.cfg boot.org
```

Adding IPsec Security

This section provides procedures for using IPsec to secure the IP connection by encrypting the data.

Central Site IPsec Configuration

This procedure adds IPSEC encryption support to an existing PPTP tunnel and assumes the tunnel is on physical port !1. The general sequence of configuration is:

- Define a policy.
- Create a KeySet.
- Add ManualKeyInfo.
- Enable the IPSEC service.

- 1 On the central site bridge/router, define a policy using:

```
ADD !<portlist> manualPOLicy <policy_name> <action> (Default |
  {<filters> <src_ipaddr/mask> (<dst_ipaddr/mask> | DYNamic)})
  [<encrypt_alg>] [<auth_alg>]

<action>:      AhEspXport | AhTunnel | AhXport |
  EspAuthTunnel | EspAuthXport | EspTunnel | EspXport
<filters>:     ANY | (GRE, ICMP, OSPF,
  TCP[(<port>,<port>)...up to 16 pairs],
  UDP[(<port>,<port>)...up to 16 pairs])
<encrypt_alg>: 3DES | 3DES2key | DES | RC5 | NULL
<auth_alg>:    MD5 | SHA
<port>:        1-65535 | * | Archie | DNS | Finger | FTP | FTPData |
  Gopher | HTTP | NFS | NNTP | NTP | POP2 | POP3 |
  PortMap | RIP | SMTP | SNMP | SNMPtrap | Syslog | Telnet | WAIS
```

For example, enter:

```
ADD !1 -IPSEC manualPOLicy pptp EspXport GRE,TCP 139.87.37.205
DYNamic 3DES
```

2 Create a KeySet using:

```
ADD -IPSEC KeySet <key_set_name> [EncryptKey ("<encrypt_key>"
| "%<encrypt_key>") ] [AuthKey ("<auth_key>" | "%<auth_key>") ]
```

For example, enter:

```
ADD -IPSEC KeySet simple_key EncryptKey "12345678abcdefgh12345678"
```

3 Add ManualKeyInfo using:

```
SETDefault !<portlist> ManualKeyInfo = <policy_name>
[<peer_ipaddr>] NONE | (<keyset_name> [SpiEsp <spi_in> <spi_out>]
[SpiAh <spi_in> <spi_out>]) <spi_in>: 256-2000 <spi_out>:
256-2147483647
```

For example, enter:

```
SETDefault !1 -IPSEC ManualKeyInfo = pptp_policy NONE simple_key
SpiEsp 1001 1001
```

4 Enable IPSEC service by entering:

```
SETDefault !1 -IPSEC CONTROL = Enable
```

Remote Site IPsec Configuration

This procedure adds IPSEC encryption support to an existing PPTP tunnel and assumes the tunnel is on logical port !V1. The general sequence of configuration is:

- Define a policy.
- Create a KeySet.
- Add ManualKeyInfo.
- Enable the IPSEC service.

1 On the remote site bridge/router define a policy using:

```
ADD !<portlist> manualPOLICY <policy_name> <action> (DEFAULT |
{<filters> <src_ipaddr/mask> (<dst_ipaddr/mask> | DYNAMIC)})
[<encrypt_alg>] [<auth_alg>]
```

```
<action>:      AhEspXport | AhTunnel | AhXport | EspAuthTunnel |
EspAuthXport | EspTunnel | EspXport <filters>:      ANY | (GRE,
ICMP, OSPF, TCP[(<port>,<port>)...up to 16 pairs]
UDP[(<port>,<port>)...up to 16 pairs])
<encrypt_alg>: 3DES | 3DES2key | DES | RC5 | NULL
<auth_alg>:    MD5 | SHA
<port>:       1-65535 | * | Archie | DNS | Finger | FTP | FTPData
| Gopher | HTTP | NFS | NNTP | NTP | POP2 | POP3 | PortMap | RIP
| SMTP | SNMP | SNMPtrap | Syslog | Telnet | WAIS
```

For example, enter:

```
ADD !1 -IPSEC manualPOLICY pptp EspXport GRE,TCP 0.0.0.0/0  
139.87.37.205 3DES
```

2 Create a KeySet using:

```
ADD -IPSEC KeySet <key_set_name> [EncryptKey ("<encrypt_key>" |  
"%<encrypt_key>")] [AuthKey ("<auth_key>" | "%<auth_key>")]
```

For example, enter:

```
ADD -IPSEC KeySet simple_key EncryptKey "12345678abcdefgh12345678"
```

3 Add ManualKeyInfo using:

```
# SETDefault !<portlist> ManualKeyInfo = <policy_name>  
[<peer_ipaddr>] NONE | (<keyset_name> [SpiEsp <spi_in>  
<spi_out>] [SpiAh <spi_in> <spi_out>])  
<spi_in>: 256-2000  
<spi_out>: 256-2147483647
```

For example, enter:

```
SETDefault !1 -IPSEC ManualKeyInfo = pptp_policy 139.87.37.205  
simple_key SpiEsp 1001 1001
```

4 Enable the IPSEC service by entering:

```
SETDefault !1 -IPSEC CONTROL = Enable
```

Configuring Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) protocol is a key management protocol standard defined in RFC 2409. It incorporates the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. It is therefore a hybrid protocol that can be used to negotiate and provide authenticated keying material for security associations in a protected manner.

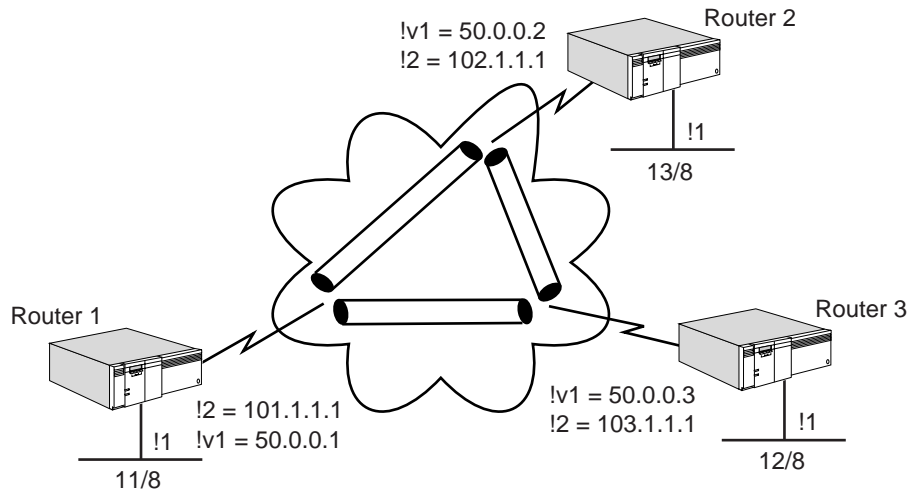
IKE, when used in conjunction with IPSec, provides for Dynamic Key Exchange and additional flexibility. It improves the scalability of IPSec over the broad spectrum of large network deployments over publicly shared infrastructures such as the Internet.

Configuring IKE for Tunnel Mode IPSEC

Figure 13 illustrates using:

- IPsec tunnel mode for the tunnels.
- Dynamic keys using IKE.
- Preshared keys, DES, and MD5 for Phase 1 IKE Profile.
- ESP for encryption (RC5) and authentication (MD5) for Phase 2 TransformList.
- RIP as the routing protocols over the tunnels.

Figure 13 Dynamic Key: Fully Meshed Topology Between Three Routers



Router 1

To configure the router 1 depicted in Figure 13, follow these steps:

- 1 Add an IPIP point-to-multipoint tunnel virtual port by entering:
ADD !v1 -Port Virtual Port IPIP P2MP
- 2 Assign an IP address to the local LAN interface by entering:
SETDefault !1 -IP NETaddress = 11.0.0.1
- 3 Assign an IP network address to the Internet interface by entering:
SETDefault !2 -IP NETaddress = 101.1.1.1
- 4 Assign an IP network address to the IPIP P2MP tunnel interface by entering:
SETDefault !v1 -IP NETaddress = 50.0.0.1

- 5 Specify the mappings of the peer Tunnel IP address to the peer Internet interface IP addresses using the following interface IP addresses:

- a For router 2, enter:

```
ADD -IP ADDRESS 50.0.0.2 ipip 102.1.1.1
```

- b For router 3, enter:

```
ADD -IP ADDRESS 50.0.0.3 ipip 103.1.1.1
```

- 6 Add a default route to the Internet (assuming !2 is a PPP port) by entering:

```
ADD -IP ROUTE 0.0.0.0 !2 1
```

- 7 Enable IP routing by entering:

```
SETDefault -IP CONTROL = ROUTE
```

- 8 Configure ISAKMP information for IKE Phase 1.

Define an IKE profile that describes the Phase 1 SA. This is used by IKE to secure its own negotiation, and is not used to secure the data traffic.
Enter:

```
ADD IKEProfile 10 PreSharedKey des md5
```

- 9 Configure ISAKMP information, for IKE Phase 2.

- a Add a selector list to choose which Traffic the policies will apply to. In this case, all traffic over the tunnel is to be encrypted, so the values of 0.0.0.0/0 are used. Enter:

```
ADD -IPSEC SelectorList s110 10 include any 0.0.0.0/0 0.0.0.0/0
```

- b Add a transform list that specifies the Phase 2 SA. (This is the description of the security for the actual data packets over the tunnel.)
Enter:

```
ADD -IPSEC TransformList t110 10 ESP-RC5 ESP-MD5
```

- c Define a common preshared key shared by all routers that need to communicate with each other. In this case, mask 0.0.0.0/0 is used to select all routers. Enter:

```
ADD -IPSEC PreSharedKey 0.0.0.0/0 "secretkey"
```

- 10 Bind all the information together using a DynamicPOLicy by entering:

```
ADD !v1 -IPSEC DynamicPOLicy pol_ea10 10 Tunnel s110 t110
```

- 11 Enable IPsec Control on the tunnel port by entering:

```
SETDefault !v1 -IPSEC CONTROL = e
```

- 12 Check the IPsec configuration by entering:

```
SHoW -IPSEC CONFIguration
```

- 13 Enable RIP Talk and Listen on the tunnel port by entering:

```
SETDefault !v1 -RIP CONTRol= (ta, li)
```

Router 2

To configure the router 2 depicted in Figure 13, follow steps 1 through 10 in "Router 1" entering the following information:

```
ADD !v1 -Port VirtualPort IPIP P2MP
SETDefault !1 -IP NETaddress = 12.0.0.1
SETDefault !2 -IP NETaddress = 102.1.1.1
SETDefault !v1 -IP NETaddress = 50.0.0.2
ADD -IP ADDRESS 50.0.0.1 IPIP 101.1.1.1
ADD -IP ADDRESS 50.0.0.3 IPIP 103.1.1.1
ADD -IP ROUTe 0.0.0.0 !2 1
SETDefault -IP CONTRol = ROUTe
```

- 14 Configure ISAKMP information for IKE Phase 1.

Define an IKE profile that describes the Phase 1 SA. This is used by IKE to secure its own negotiation and is not used to secure the data traffic.

Enter:

```
ADD IKEProfile 10 PreSharedKey des md5
```

- 15 Configure the IP Security information.

- a Add a SelectorList to choose which traffic the policies will apply to. In this case all traffic over the tunnel is to be encrypted, so the values 0.0.0.0/ are used. Enter:

```
ADD -IPSEC SelectorLIst s110 10 include any 0.0.0.0/0 0.0.0.0/0
```

- b Add a transform list that specifies the Phase 2 SA. This is the description of the security for the actual data packets over the tunnel. Enter:

```
ADD -IPSEC TransformLIst t110 10 ESP-RC5 ESP-MD5
```

- c Define a common preshared key shared by all routers that need to communicate. In this case, the mask 0.0.0.0/0 is used to select all routers. Enter:

```
ADD -IPSEC PreSharedKey 0.0.0.0/0 "secretkey"
```

- d Bind all the information together using a DynamicPOLicy by entering:

```
ADD !v1 DynamicPOLicy pol_ea10 10 Tunnel s110 t110
```

- e Enable IPsec Control on the tunnel port by entering:

```
SETDefault !v1 -IPSEC CONTROL = e
```

- f Check the IPsec configuration by entering:

```
SHOW -IPSEC CONFIGuration
SETDefault !v1 -RIP CONTROL= (ta, li)
```

Router 3

To configure the router 3 depicted in Figure 13, follow steps 1 through 10 in "Router 1" entering the following information:

```
ADD !v1 -PORT VirtualPort IPIP P2MP
SETDefault !1 -IP NETaddress = 13.0.0.1
SETDefault !2 -IP NETaddress = 103.1.1.1
SETDefault !v1 -IP NETaddress = 50.0.0.3
ADD -IP ADDRESS 50.0.0.1 IPIP 101.1.1.1
ADD -IP ADDRESS 50.0.0.2 IPIP 102.1.1.1
ADD -IP ROUTe 0.0.0.0 !2 1
SETDefault -IP CONTROL = ROUTe
```

- 16 Configure the IP security information.

- a Add a SelectorList to choose which traffic the policies will apply to. In this case all traffic over the Tunnel is to be encrypted, so the values 0.0.0.0/ are used. Enter:

```
ADD -IPSEC SelectorList s110 10 include any 0.0.0.0/0 0.0.0.0/0
```

- b Add a transform list that specifies the Phase 2 SA. This is the description of the security for the actual data packets over the tunnel. Enter:

```
ADD TransformList t110 10 ESP-RC5 ESP-MD5
```

- c Define a common preshared key shared by all routers that need to communicate. In this case, the mask 0.0.0.0/0 is used to select all routers. Enter:

```
ADD PreSharedKey 0.0.0.0/0 "secretkey"
```

- d Define an IKE profile that describes the Phase 1 SA. This is used by IKE to secure its own negotiation and is not used to secure the data traffic. Enter:

```
ADD IKEProfile 10 PreSharedKey des md5
```

e Bind all the information together using a DynamicPOLicy by entering:

```
ADD !v1 DynamicPOLicy pol_ea10 10 Tunnel s110 t110
```

f Enable IPsec Control on the tunnel port by entering:

```
SETDefault !v1 -IPSEC CONTROL = e
```

g Check the IPsec configuration by entering:

```
SHow -IPSEC conf
```

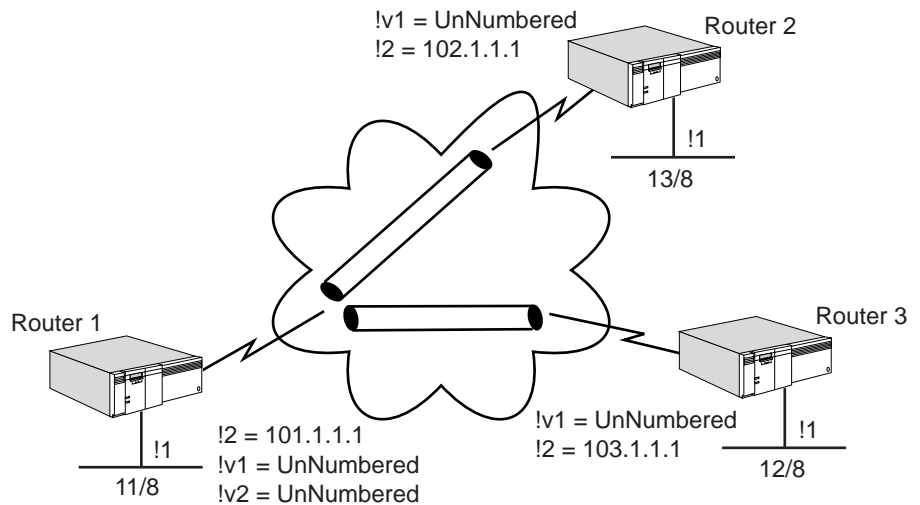
```
SETDefault !v1 -RIP CONTROL = (ta, li)
```

Configuring IKE for Transport Mode

Figure 14 illustrates a hub and spoke topology between three routers, using:

- L2TP or PPTP for tunnels.
- IPsec transport mode.
- Dynamic keys using IKE.
- Phase 1 IKE Profile using preshared keys, DES, MD5.
- Phase 2 TransformList using ESP for encryption (RC5).
- OSPF as the routing protocols over the tunnels.

Figure 14 Dynamic Key: Hub and Spoke Topology Between Three Routers



Router 1, Router 2, and Router 3

To configure the routers depicted in Figure 14, follow these steps:



All three routers should be configured identically, except where noted in the following procedure.

- 1 Configure PPTP or L2TP tunnels for the topology depicted in Figure 14, using the procedure outlined in the Configuring L2Tunnel Connections chapter in *Using Enterprise OS Software*.
- 2 Configure the routing policies.
 - a Add a default route to the Internet (assuming !2 is a PPP port) by entering:

```
ADD -IP ROute 0.0.0.0 !2 1
```
 - b Enable IP routing by entering:

```
SETDefault -IP CONTrol = ROute
```
- 3 Configure ISAKMP information for IKE Phase 1.

Define an IKE profile that describes the Phase 1 SA. This is used by IKE to secure its own negotiation and is not used to secure the data traffic. A lifetime of five hours is assigned to this Phase 1 SA. Enter:

```
ADD IKEProfile 10 PreSharedKey des md5 5hr
```
- 4 Configure the ISAKMP information for IKE Phase 2.

Add a SelectorList to choose that traffic the policies will apply to. In this case all traffic over the Internet port is to be encrypted, so the values 0.0.0.0/ are used. Enter:

```
ADD -IPSEC SelectorLIst s110 10 include any 0.0.0.0/0 0.0.0.0/0
```
- 5 Add a transform list that specifies the Phase 2 SA. This is the description of the security for the actual data packets over the tunnel. Enter:

```
ADD -IPSEC TransformLIst t110 10 ESP-RC5 ESP-MD5
```
- 6 Define a common preshared key shared by all routers that need to communicate. In this case, the mask 0.0.0.0/0 is used to select all routers. Enter:

```
ADD -IPSEC PreSharedKey 0.0.0.0/0 "secretkey1234567"
```

- 7 Bind all the information together using a DynamicPOLicy by entering:

```
ADD !2 DynamicPOLicy pol_ea10 10 Xport s110 t110
```



For PPTP/L2TP using IPSec transport mode, this needs to be configured on the actual physical port, not the virtual port.

- 8 Enable IPSec Control on the IPSec port by entering:

```
SETDefault !2 -IPSEC CONTROL= e
```

- 9 Check the IPSec configuration by entering:

```
SHOW -IPSEC CONFIGuration
```

- 10 Enable OSPF on the virtual ports.

- a For router 1, enter:

```
SETDefault !v1 -Ospf CONTROL = e
```

```
SETDefault !v2 -Ospf CONTROL = e
```

- b For router 2, enter:

```
SETDefault !v1 -Ospf CONTROL = e
```

- c For router 3, enter:

```
SETDefault !v1 -Ospf CONTROL = e
```

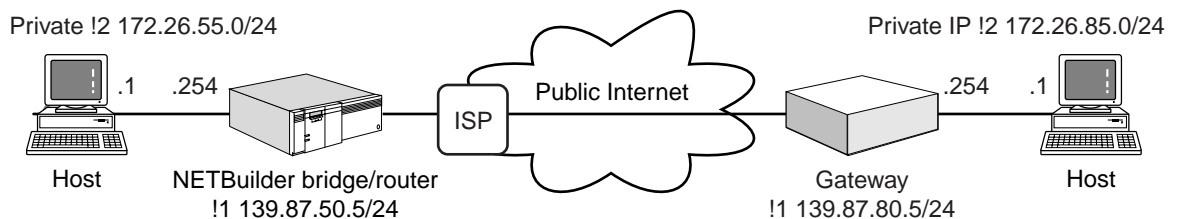


Port !2 should not run OSPF to avoid route-over-route conflicts.

Configuring IKE with a Non-3Com Security Gateway

Most security gateways are not routers as shown in Figure 15. This means that even though they perform tunnel mode IP over IP encapsulation, they do not have the notion of routing over virtual ports.

Figure 15 Non-3Com Security Gateway Configuration



To set up this correct configuration, enter:

```
Setd !1 -ip net=172.26.55.254/24 139.87.80.5/24
Setd -ip control=Route
Add !V1 -Port VirtualPort IPIP 139.87.50.5/24 139.87.80.5/24
Add !V1 -IP NETaddress = Unnumbered
Add !V1 -IP Route 172.26.85.0 255.255.255.0 !V1 1
Add -IPSec PreSharedKey 139.87.80.5 "whatkeyreally"
Add -IPSec IKEProfile 1 DES MD5 Group1 8 hrs
Add -IPSec SelectorList GateWY_SL 10 Include ANY 172.26.55.1
172.26.85.1
Add -IPSec TransformList GateWY_TL 10 ESP-DES ESP-MD5
Setd -IPSec GlobalLifeTime = 4 Hrs
Add -IPSec !V1 DynamicPOLicy GateWY_POL 5 GateWY_SL GateWY_TL
NoPFS GLT*
```

The IKE configurations remains the same.

INDEX

A

ASCII boot feature 58, 65
authentication database, users definition 36
authentication mechanisms 20
authentication with an external RADIUS server 26

B

boot.cfg file 58

C

capture.cfg file 58
CCP (compression control protocol) 24
central site configuration
 RAS VPN 27
CHAP 20
client configuration 38
compression control protocol (CCP) 24
Compression, Stac LZS algorithm 23
configuration
 central site dial-up 56
 central site IPSec 66
 central site VLL 50
 dial-on-demand 49
 ISDN dial-up 59
 RAS central site 27
 remote client 38
 remote site dial-up 59
 remote site IPSec 67
 remote site VLL 53
 site-to-site VPN 49
 tunnel switch 37
 tunnel switching 63
conventions
 notice icons, About This Guide 9
 text, About This Guide 9

D

dial-on-demand configuration 49
dial-up tunnels 49
downloading PPTP client software 39

E

encryption types 35
external RADIUS server 26
 support 33

F

files
 boot.cfg 58
 capture.cfg 58

G

General 14
general routing encapsulation (GRE) 14
Generic Routing Encapsulation Protocol Version 2
 (GRE V2) 21
GRE (general routing encapsulation) 14

I

IKE (Internet Key Encryption) 23
InfoVista 19
Internet Key Encryption (IKE) 23
Internet Service Provider (ISP) 25
IPSec 23
 defining a key set 67
 defining a policy 66
IPSec security
 adding 66, 67
ISDN configuration 59
ISP (Internet Service Provider) 25

K

KEK (Key Encryption Key) 22
Key Encryption Key (KEK) 22

L

L2TP (Layer 2 Tunneling Protocol) 14
LAN extension 26
Layer 2 Tunneling Protocol (L2TP) 14, 21
local user authentication database 26

M

Microsoft Dial-Up Networking 26, 38, 39
Microsoft Point-to-Point Encryption (MPPE)
protocol 22

N

Network Address Translation (NAT)
NAT (Network Address Translation) 24
Network management application
Transcend® Secure VPN Manager 19
Web Link Health Monitor 19
network management application
InfoVista 19

P

Point 14
point of presence (POP) 12
Point-to-Point Tunneling Protocol (PPTP) 14, 21
POP (point of presence) 12
PPTP (Point-to-Point Tunneling Protocol) 14
PPTP client software
downloading 39

R

RAS VPN
central site configuration 27
RAS VPN configuration
remote client 38
remote client configuration 38
renaming boot.cft 58

S

Stac LZS algorithm compression 23
SysCallerID, using 20

T

TI (tunnel initiator) 11
Total Control™ Hub 21
Transcend® Secure VPN Manager 19
TT (tunnel terminator) 11
tunnel components 11
tunnel initiator (TI) 11
tunnel peers 22
tunnel switch
configuration 37
used in a tunnel 11
tunnel switch configuration 63
tunnel terminator (TT) 11

U

user authentication database, setting up 35
user database, local 35

V

virtual leased line (VLL) 49
virtual private network (VPN) 11
virtual private network, definition of 11
VLL (virtual leased line) 49
VPN (virtual private network) 11

W

Web Link Health Monitor 19
