



*Operating System*

## Virtual Private Networking with Windows 2000: Deploying Router-to-Router VPNs

*By Joseph Davies*

*Microsoft Corporation*

*Published: October 2001*

---

### **Abstract**

A virtual private network (VPN) is the extension of a private network that encompasses logical links across shared or public networks such as the Internet. A router-to-router VPN connection allows computers to securely connect the sites of an organization across the Internet. This paper describes the various components and design choices of a deployment of router-to-router VPN connections using the Windows® 2000 platform VPN servers. This paper also includes detailed walkthroughs to deploy Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP)-based router-to-router VPNs, information on firewall configuration, and details of troubleshooting tools and common problems. This paper assumes familiarity with TCP/IP, IP routing, Internet Protocol security (IPSec), and the capabilities of the Windows 2000 Routing and Remote Access service.

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2001. Microsoft Corporation. All rights reserved. Microsoft, Active Directory, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

---

## Contents

<b>Introduction .....</b>	<b>1</b>
Overview of Demand-Dial Routing in Windows 2000 Server	2
Demand-dial routing updates	3
Introduction to Router-to-Router VPN connections	4
On-demand vs. persistent connections	5
Restricting the initiation of demand-dial connections	5
One-way vs. two-way initiated connections	6
<b>Components of Windows 2000 Router-to-Router VPNs .....</b>	<b>7</b>
VPN routers	7
Installing a certificate on a VPN router	10
Design Points: Configuring the VPN router	10
Internet network infrastructure	13
Answering router name resolvability	13
Answering router reachability	13
VPN routers and firewall configuration	13
Design Points: Answering router accessibility from the Internet	13
Authentication protocols	14
Design Point: Which authentication protocol to use?	15
VPN protocols	15
Point-to-Point Tunneling Protocol	15
Layer Two Tunneling Protocol with IPSec	15
Design Point: PPTP or L2TP?	16
Site network infrastructure	16
Name resolution	16
Routing	17
Routing and multi-use VPN routers	18
Design Points: Routing infrastructure	19
AAA Infrastructure	20

Remote access policies	21
Windows domain user accounts and groups	22
One-way initiated connections and static routes on the user account	23
Design Points: AAA infrastructure	24
Certificate infrastructure	24
Computer certificates for L2TP/IPSec	24
User and computer certificates for EAP-TLS authentication	25
Design Points: Certificate infrastructure	26
<b>Deploying a PPTP-based Router-to-Router VPN Connection.....</b>	<b>27</b>
Deploying certificate infrastructure	27
Installing a user certificate on a calling router	27
Configuring EAP-TLS on the calling router	28
Installing a computer certificate on the authenticating server	28
Configuring EAP-TLS on the answering router and remote access policy	28
Deploying Internet infrastructure	29
Placing VPN routers in perimeter network or on the Internet	29
Installing Windows 2000 Server on VPN routers and configuring Internet interfaces	29
Deploying the answering router	29
Configuring the answering router's connection to the site	29
Running the Routing and Remote Access Server Setup Wizard	30
Configuring a demand-dial interface	30
Deploying the calling router	31
Configuring the calling router's connection to the site	31
Running the Routing and Remote Access Server Setup Wizard	31
Configuring a demand-dial interface	32
Deploying AAA infrastructure	33
Configuring Active Directory for user accounts and groups	33
Configuring the primary IAS server on a domain controller	33
Configuring the secondary IAS server on a different domain controller	35
Deploying site network infrastructure	35
Configuring routing on the VPN routers	35

Verifying reachability from each VPN router	36
Configuring routing for off-subnet address pools	36
Deploying intersite network infrastructure	36
<b>Deploying an L2TP-based Router-to-Router VPN Connection .....</b>	<b>38</b>
Deploying certificate infrastructure	38
Certificates for L2TP connections	38
Certificates for EAP-TLS authentication	39
Installing a user certificate on a calling router	39
Configuring EAP-TLS on the calling router	39
Installing a computer certificate on the authenticating server	40
Configuring EAP-TLS on the answering router and remote access policy	40
Deploying Internet infrastructure	40
Placing VPN routers in perimeter network or on the Internet	40
Installing Windows 2000 Server on VPN routers and configuring Internet interfaces	41
Deploying the answering router	41
Configuring the answering router's connection to the site	41
Running the Routing and Remote Access Server Setup Wizard	41
Configuring a demand-dial interface	42
Deploying the calling router	43
Configuring the calling router's connection to the site	43
Running the Routing and Remote Access Server Setup Wizard	43
Configuring a demand-dial interface	44
Deploying AAA infrastructure	44
Configuring Active Directory for user accounts and groups	45
Configuring the primary IAS server on a domain controller	45
Configuring the secondary IAS server on a different domain controller	46
Deploying site network infrastructure	47
Configuring routing on the VPN routers	47
Verifying reachability from each VPN router	47
Configuring routing for off-subnet address pools	47
Deploying intersite network infrastructure	47

<b>Appendix A: Configuring Firewalls with a Windows 2000 VPN Router.....</b>	<b>49</b>
VPN router in front of the firewall	49
Packet Filters for PPTP	50
Packet Filters for L2TP/IPSec	50
VPN router behind the firewall	51
Packet Filters for PPTP	52
Packet Filters for L2TP/IPSec	53
VPN router between two firewalls	54
<b>Appendix B: Alternate Configurations .....</b>	<b>56</b>
Multiple Internet Function VPN Router	56
Single-Adapter VPN Router	57
<b>Appendix C: Troubleshooting.....</b>	<b>58</b>
Troubleshooting tools	58
TCP/IP Troubleshooting Tools	58
Authentication and Accounting Logging	58
Unreachability Reason	59
Event Logging	59
IAS Event Logging	59
PPP logging	59
Tracing	59
Network Monitor	60
Troubleshooting router-to-router VPN connections	61
Connection attempt is rejected when it should be accepted	61
Connection attempt is accepted when it should be rejected	64
Unable to reach locations beyond the VPN router	64
Unable to reach the virtual interfaces of VPN routers	65
On-demand connection is not made automatically	66
Unable to establish tunnel	66
<b>Summary.....</b>	<b>67</b>

**Related Links..... 68**

---

## Introduction

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. With a VPN, you can send data between two computers across a shared or public network in a manner that emulates a point-to-point private link (such as a long haul T-Carrier-based wide area network [WAN] link). Virtual private networking is the act of creating and configuring a virtual private network.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information, which allows the data to traverse the shared or public network to reach its endpoint. To emulate a private link, the data is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The logical link over which the private data is encapsulated and encrypted is a virtual private network (VPN) connection.

Figure 1 shows the logical equivalent of a VPN connection.

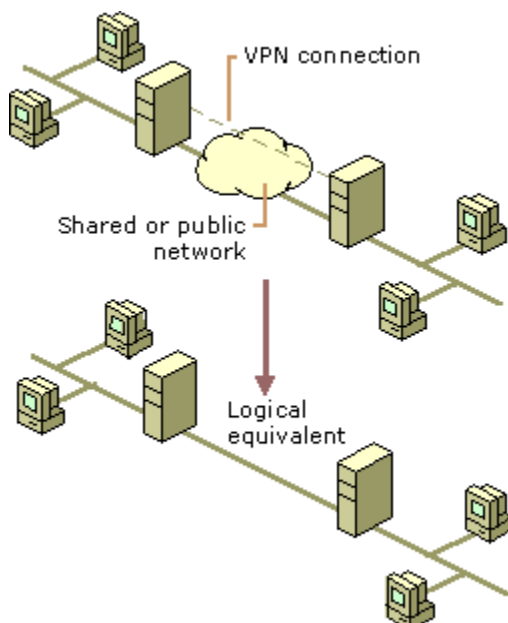


Figure 1 The logical equivalent of a VPN connection

Users working at home or on the road can use VPN connections to establish a remote access connection to an organization server by using the infrastructure provided by a public network such as the Internet. From the user's perspective, the VPN connection is a point-to-point connection between the computer (the VPN client) and an organization server (the VPN server). The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link.

Organizations can also use VPN connections to establish router-to-router connections with geographically separate offices or with other organizations over a public network such as the Internet while maintaining secure communications. A router-to-router VPN connection across the Internet logically operates as a dedicated WAN link.

With both remote access and router-to-router connections, an organization can use VPN connections to trade long-distance dial-up or leased lines for local dial-up or leased lines to an Internet service provider (ISP).

There are two types of PPP-based router-to-router VPN technology in the Windows® 2000 operating system:

1. Point-to-Point Tunneling Protocol (PPTP)  
PPTP uses user-level Point-to-Point Protocol (PPP) authentication methods and Microsoft Point-to-Point Encryption (MPPE) for data encryption.
2. Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPSec)  
L2TP with IPSec (L2TP/IPSec) uses user-level PPP authentication methods and IPSec for computer-level authentication using certificates and data authentication, integrity, and encryption.

---

**Note:** Using IPSec tunnel mode for router-to-router VPN connections is possible using computers running Windows 2000 Server. Because the IPSec tunnel is not represented as a logical interface over which packets can be forwarded and received, routing protocols do not operate over IPSec tunnels. Because the configuration of IPSec tunnels for router-to-router VPN connections is vastly different, it is not discussed here. For more information, see article Q252735, "[How to Configure IPSec Tunneling in Windows 2000](#)," in the [Microsoft Knowledge Base](#).

---

For encryption, you can use either link encryption or end-to-end encryption in addition to link encryption:

- Link encryption encrypts the data only on the link between the routers. For PPTP connections, you must use MPPE in conjunction with MS-CHAP, MS-CHAP v2, or EAP-TLS authentication. For L2TP/IPSec connections, IPSec provides encryption on the link between the routers.
- End-to-end encryption encrypts the data between the source host and its final destination. You can use IPSec after the router-to-router VPN connection is made to encrypt data from the source host to the destination host.

#### Overview of Demand-Dial Routing in Windows 2000 Server

The Windows 2000 Routing and Remote Access service includes support for demand-dial routing (also known as dial-on-demand routing) over both dial-up connections (such as analog phone lines or ISDN) and VPN connections. Demand-dial routing is the forwarding of packets across a Point-to-Point Protocol (PPP) link. The PPP link is represented inside the Windows 2000 Routing and Remote Access service as a demand-dial interface, which can be used to create on-demand connections across dial-up, non-permanent, or persistent media. Demand-dial connections allow you to use dial-up telephone lines instead of leased lines for low-traffic situations and to leverage the connectivity of the Internet to connect branch offices with VPN connections.

Demand-dial routing is not the same as remote access. While remote access connects a single computer to a network; demand-dial routing connects entire networks. However, both use PPP as the protocol through which to negotiate and authenticate the connection and encapsulate the data sent over it. As implemented in the Windows 2000 Routing and Remote Access service, both remote access and demand-dial connections can be enabled separately. However, they still share the same:

- Dial-in properties behavior of user accounts.
- Security (authentication protocols and encryption).
- Remote access policies usage.
- Windows or Remote Authentication Dial-In User Service (RADIUS) usage (for authentication, authorization, and accounting).
- IP and Internetwork Packet Exchange (IPX) address assignment and configuration.

- PPP features usage, such as Microsoft Point-to-Point Compression (MPPC), Multilink PPP, and Bandwidth Allocation Protocol (BAP).
- Troubleshooting facilities, including event logging, Windows or RADIUS authentication and accounting logging, and tracing.

While the concept of demand-dial routing is fairly simple, configuration of demand-dial routing is relatively complex. This complexity is due to the following factors:

- **Connection endpoint addressing.** The connection must be made over public data networks, such as the analog phone system or the Internet. The endpoint of the connection must be identified by a phone number for dial-up connections, and either a fully qualified host name or IP address for VPN connections.
- **Authentication and authorization of the caller**  
Anyone calling the router must be authenticated and authorized. Authentication is based on the caller's set of credentials that are passed during the connection establishment process. The credentials that are passed must correspond to a Windows 2000 account. Authorization is granted based on the dial-in properties of the Windows 2000 account and remote access policies.
- **Differentiation between remote access clients and calling routers.** Both routing and remote access services coexist on the same computer running Windows 2000 Server. Both remote access clients and demand-dial routers can initiate a connection. The computer running Windows 2000 Server that answers a connection attempt must be able to distinguish a remote access client from a demand-dial router. If the user name, which is included in the authentication credentials sent by the router that initiates the connection (the calling router), matches the name of a demand-dial interface on the Windows 2000 Server that answers the connection attempt (the answering router), the connection is a demand-dial connection. Otherwise, the incoming connection is a remote access connection.
- **Configuration of both ends of the connection.** Both ends of the connection must be configured, even if only one end of the connection is initiating a demand-dial connection. Configuring only one side of the connection means that packets are successfully routed in only one direction. Communication typically requires that information travel in both directions.
- **Configuration of static routes.** You should not use dynamic routing protocols over temporary demand-dial connections. Therefore, routes for network IDs that are available across the demand-dial interface must be added, as static routes, to the routing tables of the demand-dial routers. You can add static routes manually or by using auto-static updates.

### Demand-dial routing updates

While demand-dial routing can save connection costs, typical routing protocols rely on a periodic advertising process to communicate routing information. For example, RIP for IP advertises the contents of its routing table every 30 seconds on all interfaces. This behavior is not a problem for permanently connected LAN or WAN lines. For usage-sensitive dial-up WAN lines, this type of periodic behavior could cause the router to call another router every 30 seconds, which may result in an undesirable phone bill. Therefore, you should not run routing protocols across temporary dial-up WAN lines.

If you do not use routing protocols to update the routing tables, then you must enter the routes as static routes. The static routes that correspond to the network IDs available across the interface are entered manually or automatically. The automatic entering of static routes for demand-dial interfaces is known as auto-static updates

and is supported by the Windows 2000 Routing and Remote Access service. Auto-static updates are supported when you use RIP for IP, RIP for IPX, and SAP for IPX, but not OSPF.

When instructed, a demand-dial interface that is configured for auto-static updates sends a request across an active connection to request all of the routes of the router on the other side of the connection. In response to the request, all of the routes of the requested router are automatically entered as static routes in the routing table of the requesting router. The static routes are persistent; they are kept in the routing table even if the interface becomes disconnected or the router is restarted. An auto-static update is a one-time, one-way exchange of routing information.

You can automate and schedule auto-static updates by executing the update as a Windows 2000 scheduled task. For more information, see the topic titled "Scheduling auto-static updates" in Windows 2000 Server online Help.

#### **To find a specific topic in Windows 2000 Server online Help**

1. From the Windows 2000 desktop, click **Start**, and then click **Help**.
2. In the **Windows 2000** dialog box, click the **Search** tab.
3. Clear the **Match similar words** check box and select the **Search titles only** check box.
4. In **Type the keyword to find**, type the topic title, and then click **List topics**.
5. In the list of topics under **Select topic**, double click the topic that exactly matches the typed topic title.

---

**Note:** The "auto" in auto-static refers to the automatic adding of the requested routes as static routes in the routing table. The sending of the request for routes is performed through an explicit action: either through the Routing and Remote Access snap-in or the Netsh utility while the demand-dial interface is in a connected state. Auto-static updates are not automatically performed every time a demand-dial connection is made.

---

#### Introduction to Router-to-Router VPN connections

A router-to-router VPN connection is a demand-dial connection that uses a VPN tunneling protocol such as PPTP and L2TP to connect two portions of a private network. Each VPN router provides a routed connection to the network to which the VPN router is attached. On a router-to-router VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers.

The calling router (the VPN client) initiates the connection. The answering router (the VPN server) listens for connection attempts, receives the connection attempt from the calling router, and responds to the request to create a connection. The calling router authenticates itself to the answering router. When using a mutual authentication protocol such as MS-CHAP v2 or EAP-TLS, the answering router also authenticates itself to the calling router.

Table 1 lists the router-to-router VPN-capable Microsoft operating systems.

**Table 1 Router-to-Router VPN-Capable Microsoft Operating Systems**

VPN Tunneling Protocol	Microsoft Operating System
PPTP	Windows 2000 Server, Windows NT version 4.0 with the Routing and Remote Access Service (RRAS)
L2TP/IPSec	Windows 2000 Server

VPN routers can also be any computer that is capable of creating a routed PPTP connection using MPPE or a routed L2TP connection using IPSec encryption.

### On-demand vs. persistent connections

A router-to-router VPN connection can be on-demand or persistent:

- An on-demand router-to-router connection is a connection that is made when traffic must be forwarded across the connection. The connection is made, the traffic is forwarded, and the connection is terminated after a configured amount of idle time. You can configure idle disconnect behavior for the answering router by setting an idle disconnect on the **Dial-in Constraints** tab on the profile properties of the remote access policy that is used for the router-to-router VPN connection. You can configure idle disconnect behavior for the calling router on the **Options** tab on the properties of the demand-dial interface in the Routing and Remote Access snap-in.
- A persistent router-to-router connection is always connected. If the connection is dropped, it is immediately retried. To configure the answering router for connection persistence, clear the **Disconnect if idle for** and **Restrict maximum session to** check boxes on the **Dial-in Constraints** tab on the profile properties of the remote access policy that is used for the router-to-router VPN connection. To configure the calling router for connection persistence, select **Persistent connection** on the **Options** tab from the properties of the demand-dial interface.

If the calling router connects to the Internet by using a dial-up link such as an analog phone line or ISDN, then you need to configure a dial-up on-demand router-to-router VPN connection consisting of a single demand-dial interface at the answering router and two demand-dial interfaces at the calling router: one to connect to a local Internet service provider (ISP) and one for the router-to-router VPN connection. Dial-up on-demand router-to-router VPN connections also require an additional host route in the IP routing table of the calling router. For more information, see the topic titled "An on-demand router-to-router VPN" in Windows 2000 Server online Help.

For either on-demand or persistent router-to-router VPN connections, the answering router is permanently connected to the Internet.

### Restricting the initiation of demand-dial connections

To prevent the calling router from making unnecessary connections, you can restrict the calling router from making on-demand router-to-router VPN connections in the following ways:

- **Demand-dial filtering.** You can use demand-dial filtering to configure either the types of IP traffic that do not cause a demand-dial connection to be made or the types of IP traffic that cause a connection to be made. You can configure demand-dial filtering by right-clicking the demand-dial interface in the **Routing**

**Interfaces** node in the Routing and Remote Access snap-in, and then clicking **Set IP Demand-dial Filters**.

- **Dial-out hours.** You can use dial-out hours to configure the hours that a calling router is either permitted or denied to make a router-to-router VPN connection. You can configure dial-out hours by right-clicking the demand-dial interface in the **Routing Interfaces** node in the Routing and Remote Access snap-in, and then clicking **Dial-out Hours**.

You can use remote access policies to configure the times when incoming demand-dial routing connections are allowed.

### One-way vs. two-way initiated connections

With one-way initiated connections, one VPN router is always the calling router and one VPN router is always the answering router. One-way initiated connections are well suited to a permanent connection spoke-and-hub topology where the branch office router is the only router that initiates the connection. One-way initiated connections require the following:

- The answering router is configured as a LAN and demand-dial router.
- A user account is added for the authentication credentials of the calling router that is accessed and validated by the answering router.
- A demand-dial interface is configured at the answering router with the same name as the user account that is used by the calling router. This demand-dial interface is not used to dial out, therefore it does not have a host name or IP address or with valid user credentials.

With two-way initiated connections, either VPN router can be the calling router or answering router depending on who is initiating the connection. Both VPN routers must be configured to both initiate and accept a router-to-router VPN connection. You can use two-way initiated connections when the router-to-router VPN connection is not active 24 hours a day and traffic from either router is used to create an on-demand connection. Two-way initiated router-to-router VPN connections require the following:

- Both routers are connected to the Internet by using a permanent WAN link.
- Both routers are configured as LAN and demand-dial routers.
- User accounts are added for both routers so that the authentication credentials for the calling router are accessed and validated by the answering router.
- Demand-dial interfaces, with the same name as the user account that is used by the calling router, must be fully configured at both routers, including settings for the host name or IP address of the answering router and user account credentials.

Table 2 lists a correct example configuration for two-way initiated demand-dial routing between Router 1, a demand-dial router in the Seattle site, and Router 2, a demand-dial router in the New York site.

**Table 2 Correct example configuration for two-way initiated demand-dial routing**

Router	Demand-dial interface name	User account name in user credentials
Router 1	DD_NewYork	DD_Seattle
Router 2	DD_Seattle	DD_NewYork

Notice how the user account name in the user credentials of the demand-dial interface of one router matches the name of a demand-dial interface on the other router.

## Components of Windows 2000 Router-to-Router VPNs

Figure 2 shows the components of Windows 2000 router-to-router virtual private networks.

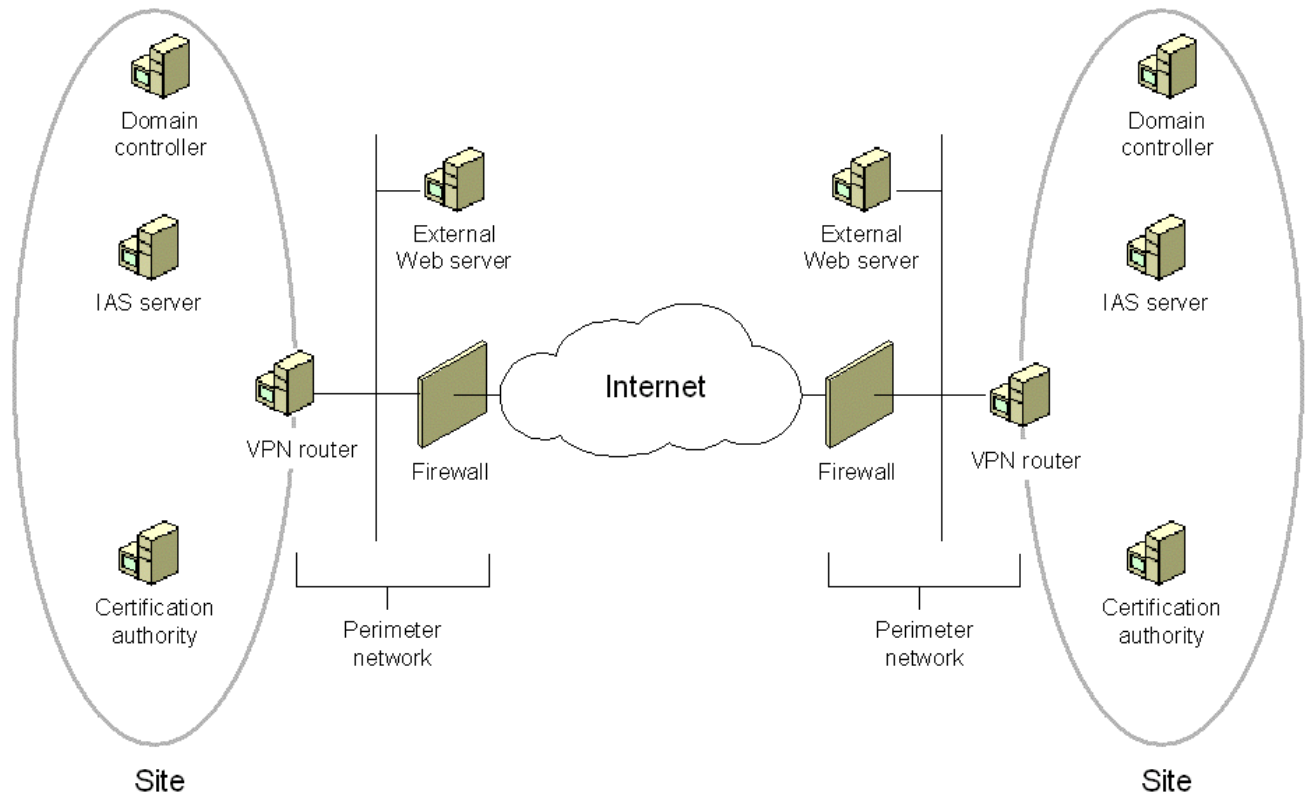


Figure 2 Components of Windows 2000 router-to-router VPNs

The major components are:

- VPN routers
- Internet infrastructure
- Intranet infrastructure
- Authentication, authorization, and accounting (AAA) infrastructure
- Certificate infrastructure

### VPN routers

VPN routers either initiate or receive VPN-based demand-dial connections and consists of the following components:

- **Routing and Remote Access service.** The Routing and Remote Access service on both the calling and answering router is configured as a VPN server using the Routing and Remote Access Server Setup Wizard.
- **Ports.** A port is a logical or physical communications channel capable of supporting a single PPP connection. Physical ports are based on equipment installed in the VPN router. Virtual private network

(VPN) ports are logical ports.

- **Demand-dial interfaces.** A demand-dial interface configured on the calling router represents the PPP connection and contains configuration information such as the type of port to use, the addressing used to create the connection (an IP address or domain name), authentication methods, encryption requirements, and authentication credentials.

For two-way initiated connections, a demand-dial interface configured on the answering router represents the PPP connection to the calling router. For a one-way initiated connection using static routes on the user account of the calling router, a demand-dial interface on the answering router does not need to be configured.

- **User account.** To authenticate the calling router, the credentials of the calling router must be verified by the properties of a corresponding user account. If the answering router is configured for Windows authentication, a user account in the authentication credentials of the calling router must be verifiable using Windows security. If the answering router is configured for RADIUS authentication, then the RADIUS server must have access to the user account in the authentication credentials of the calling router.

The user account must have the following settings:

- On the **Dial-in** tab, remote access permission is set to either **Allow access** or **Control access through Remote Access Policy**. When you create user accounts with the Demand-Dial Interface Wizard, the remote access permission is set to **Allow access**.
- On the **General** or **Account** tab, **User must change password at next logon** is disabled and **Password never expires** is enabled. These settings are configured when you create user accounts with the Demand-Dial Interface Wizard.

For a one-way initiated connection, you can configure static IP routes on the **Dial-in** tab that are added to the answering router's routing table when the demand-dial connection is made.

- **Routes.** To forward traffic across a router-to-router VPN connection, IP routes in the routing tables of the VPN routers is configured to use the correct demand-dial interface.

For one-way initiated connections, configure the calling router normally. For the answering router, you can configure the user account specified in the authentication credentials of the calling router with static IP routes.

- **Remote access policy.** On the answering router or the Internet Authentication Service (IAS) server that is acting as a RADIUS server to the answering router, to specify connection parameters that are specific to demand-dial connections, create a separate remote access policy that uses the Windows-Groups attribute set to the group that has all of the user accounts for calling routers as members. A separate remote access policy for demand-dial connections is not required.

A calling router does the following:

- Initiates VPN connections based on an administrator action or when a packet being forwarded matches a route using a VPN-based demand-dial interface.
- Waits for authentication and authorization before forwarding packets.
- Acts as a router forwarding packets between nodes in its site and the answering router.
- Acts as an endpoint of the VPN connection.

The answering router does the following:

- Listens for VPN connection attempts.
- Authenticates and authorizes VPN connections before allowing data to flow.
- Acts as a router forwarding packets between nodes in its site and the calling router.

- Acts as an endpoint of the VPN connection.

VPN routers typically have two installed network adapters—one network adapter connected to the Internet and one network adapter connected to the intranet.

When you configure and enable the Routing and Remote Access service, the Routing and Remote Access Server Setup Wizard prompts you to select the role that the computer will fulfill. For VPN routers, you should select the **Virtual private network (VPN) server** option. With the **Virtual private network (VPN) server** option, the Routing and Remote Access server operates in the role of a VPN server that supports both remote access and router-to-router VPN connections. For remote access VPN connections, users run VPN client software and initiate a remote access connection to the VPN server. For router-to-router VPN connections, a router initiates a VPN connection to the VPN server. Alternately, the VPN server can initiate a VPN connection to another VPN router.

---

**Note:** Microsoft recommends the choice of **Virtual private network (VPN) server** over **Network router** in the Routing and Remote Access Server Setup Wizard because the **Network router** option does not prompt you to select an Internet interface over which to automatically configure packet filters, does not prompt you to configure RADIUS servers, and only creates 5 PPTP and 5 L2TP ports.

---

When you select the **Virtual private network (VPN) server** option in the Routing and Remote Access Server Setup Wizard:

1. You are first prompted to verify the protocols over which VPN traffic is forwarded. By default, all of the protocols that can be used with a remote access or router-to-router VPN connection are listed.
2. Next, you are prompted to select the interface that is connected to the Internet. The interface that you select will be automatically configured with packet filters that allow only PPTP and L2TP-related traffic. All other traffic is silently discarded. For example, you will no longer be able to ping the Internet interface of the calling router. If you do not want to have VPN packet filters automatically configured, you can select **<No Internet connection>**. If you want to use the calling router computer as a network address translator (NAT), Web server, or other function, see Appendix B.
3. Next, if you have multiple network adapters that are connected to the intranet, you are prompted to select an interface over which DHCP, DNS, and WINS configuration is obtained.
4. Next, you are prompted to determine whether you want to assign IP addresses to either remote access clients or other calling routers by using either DHCP or a specified range of addresses. If you select a specified range of addresses, you are prompted to add one or more address ranges.
5. Next, you are prompted to specify whether you want to use RADIUS as your authentication and accounting provider. If you select RADIUS, you are prompted to configure primary and alternate RADIUS servers and the shared secret.

When you complete the **Virtual private network (VPN) server** option in the Routing and Remote Access Server Setup Wizard, the results are as follows:

1. The Routing and Remote Access service is enabled as both a remote access server and a LAN and demand-dial router, with Windows as the authentication and accounting provider (unless RADIUS was chosen and configured). If there is only one network adapter connected to the site, that network adapter is automatically selected as the IP interface from which to obtain DHCP, DNS, and WINS configuration. Otherwise, the network adapter specified in the wizard is selected to obtain DHCP, DNS, and WINS configuration. If specified, the static IP address ranges are configured.
2. Exactly 128 PPTP and 128 L2TP ports are created. All of them are enabled for both inbound remote

- access connections and inbound and outbound demand-dial connections.
3. The selected Internet interface is configured with input and output IP packet filters that allow only PPTP and L2TP traffic.
  4. All protocols selected are configured to both allow remote access connections and access the network to which the remote access server is attached.
  5. The DHCP Relay Agent component is added with the **Internal** interface. If the VPN router is a DHCP client at the time the wizard is run, the DHCP Relay Agent is automatically configured with the IP address of a DHCP server. Otherwise, you must manually configure the properties of the DHCP Relay Agent with an IP address of a DHCP server in your site. The DHCP Relay Agent forwards DHCPInform packets between VPN remote access clients and a site DHCP server.
  6. The IGMP component is added. The **Internal** interface and all other LAN interfaces are configured for IGMP router mode. This allows VPN remote access clients to send and receive IP multicast traffic.

### Installing a certificate on a VPN router

If VPN routers are making L2TP connections or using EAP-TLS authentication, certificates must be installed on the VPN router computers. For L2TP connections, a computer certificate must be installed on both the calling and answering router computer to provide authentication for establishing an IPsec security association (SA). For EAP-TLS authentication, a computer certificate must be installed on the authenticating server (either the answering router or a RADIUS server) and a user certificate must be installed on the calling router.

For more information about installing certificates on calling routers, answering routers, and authentication server computers, see “Certificate infrastructure” in this paper.

### Design Points: Configuring the VPN router

Consider the following before running the Routing and Remote Access Server Setup Wizard:

- Which protocols will be supported over the VPN connection?  
The Routing and Remote Access service can forward IP or IPX packets over a PPTP or L2TP connection.
- Which connection of the VPN router is connected to the Internet?  
Typical Internet-connected VPN routers have at least two LAN connections: one connected to the Internet (either directly or connected to a perimeter network) and one connected to the site. To make this distinction easier to see for the Routing and Remote Access Server Setup Wizard, rename the connections with their purpose or role using Network and Dial-up Connections. For example, rename the connection connected to the Internet, default name **Local Area Connection 2**, to **Internet**.
- Can the VPN router be a DHCP client?  
The VPN router must have a manual TCP/IP configuration for its Internet interface. While technically possible, it is not recommended that the VPN router be a DHCP client for its site interface(s). Due to the routing requirements of the VPN router, manually configure an IP address, subnet mask, DNS server(s), and WINS server(s), but do not configure a default gateway.  
  
Note that it is possible for the VPN router to have a manual TCP/IP configuration and still use DHCP to obtain IP addresses for remote access VPN clients and other calling routers.
- How will IP addresses be allocated to remote access VPN clients and other calling routers?  
The VPN router can be configured to obtain IP addresses from DHCP or from a manually configured set of

address ranges. Using DHCP to obtain IP addresses simplifies the configuration, however, you must ensure that the DHCP scope for the subnet to which the site connection of the calling router is attached has enough addresses for all the computers physically connected to the subnet and the maximum number of PPTP and L2TP ports. For example, if the subnet to which the site connection of the VPN router is attached contains 50 DHCP clients, then, for the default configuration of the VPN router, the scope should contain at least 307 addresses (50 computers + 128 PPTP clients + 128 L2TP clients + 1 address for the VPN router). If there are not enough IP addresses in the scope, remote access VPN clients and calling routers that connect after all the addresses in the scope are allocated will be assigned an address in the Automatic Private IP Addressing (APIPA) range of 169.254.0.0/16.

If you configure a static pool of addresses, ensure that the pool has enough addresses for all your PPTP and L2TP ports, plus an additional address for the VPN router. If there are not enough addresses in your static pool, remote access VPN clients and Windows NT® 4.0 RRAS calling routers will not be able to connect. Windows 2000 calling routers, however, will still be able to connect. Windows 2000 calling and answering routers still request an IP address from each other during the connection establishment process. But if one of the routers does not have an address to assign, both routers continue with the connection establishment process. The logical interface on the point-to-point connection does not have an assigned IP address. This is known as an unnumbered connection. While Windows 2000 VPN routers support unnumbered connections, the routing protocols included with Windows 2000 do not work over an unnumbered connection.

If you are configuring a static pool of addresses, there might be additional routing considerations. For more information, see “Site network infrastructure” in this paper.

- What is the authentication and accounting provider?

The VPN router can use Windows or RADIUS as its authentication or accounting provider.

When Windows is used as the authentication and accounting provider, the VPN router uses Windows 2000 security to validate the credentials of a calling router and access the calling router's user account dial-in properties. Locally configured remote access policies authorize the VPN connection and locally written accounting log files log VPN connection accounting information.

When RADIUS is used as the authentication and accounting provider, the VPN router uses a configured RADIUS server to validate the credentials of a calling router, authorize the connection attempt, and store VPN connection accounting information.

- Are you making L2TP connections?

If so, you must install a computer certificate on both the calling router and answering router computers.

- Are you using user-level certificate authentication with EAP-TLS?

If so, you must install a user certificate on the calling router computer and a computer certificate on the authenticating server (either the answering router computer [if the answering router is configured for the Windows authentication provider] or the RADIUS server [if the answering router is configured for the RADIUS authentication provider]). If the authenticating server is a Windows 2000 VPN router or a Windows 2000 Internet Authentication Service (IAS) server, EAP-TLS is only available if the authenticating server is a member of an Active Directory™ service domain.

- For on-demand connections, do you want prevent connections from occurring during certain times of the day during the week or for certain types of traffic?

If so, configure dial-out hours or demand-dial filters on the demand-dial interface of the calling router.

- Do you want to match your IP packet filters to the demand-dial filters?

Demand-dial filters are applied before the connection is made. IP packet filters are applied after the connection is made. To prevent the demand-dial connection from being established for traffic that is discarded by the IP packet filters:

- If you have configured a set of output IP packet filters with the **Receive all packets except those that meet the criteria listed below** option, then configure the same set of filters as demand-dial filters with **Initiate connection** set to **For all traffic except**.
- If you have configured a set of output IP packet filters with the **Drop all packets except those that meet the criteria listed below** option, then configure the same set of filters as demand-dial filters with **Initiate connection** set to **Only for the following traffic**.

Consider the following when changing the default configuration of the VPN router for router-to-router VPN connections:

- Do you want to support remote access VPN connections?  
By default, all the PPTP and L2TP ports are configured to allow both remote access connections (inbound only) and demand-dial routing connections (inbound and outbound). To disable remote access connections and create a dedicated router-to-router VPN connection server, clear the **Remote access connections (inbound only)** check box from the properties of the **WAN miniport (PPTP)** and **WAN miniport (L2TP)** devices from the properties of the **Ports** object in the Routing and Remote Access snap-in.
- Do you need to install a computer certificate?  
If the VPN router is supporting L2TP connections or is authenticating connections using the EAP-TLS authentication protocol and configured to use the Windows authentication provider, you must install a computer certificate. If the VPN router is a calling router using the EAP-TLS authentication protocol, you must install a user certificate. For more information, see "Certificate infrastructure" in this paper.
- Do you need custom remote access policies for VPN connections?  
If you configure the VPN router for Windows authentication or for RADIUS authentication and the RADIUS server is an IAS server, the default remote access policy rejects all types of connection attempts unless the remote access permission of the user account's dial-in properties is set to **Allow access**. If you want to manage authorization and connection parameters by group or by type of connection, you must configure custom remote access policies. For more information, see "Remote Access Policies" in this paper.
- Do you want separate authentication and accounting providers?  
The Routing and Remote Access Server Setup Wizard configures both authentication and accounting providers to be the same. After the Wizard is complete, however, you can configure the authentication and accounting providers separately (for example, if you want to use Windows authentication and RADIUS accounting). You can configure authentication and accounting providers on the **Authentication** tab from the properties of the VPN router in the Routing and Remote Access snap-in.

After the VPN router is configured, you can begin creating demand-dial interfaces and configuring routes using the Routing and Remote Access snap-in. For more information, see "Deploying a PPTP-based Router-to-Router VPN Connection" and "Deploying an L2TP-based Router-to-Router VPN Connection" in this paper.

Internet network infrastructure

To create a router-to-router VPN connection to an answering router across the Internet:

- The answering router's name must be resolvable.
- The answering router must be reachable.
- VPN traffic must be allowed to and from the answering router.

### **Answering router name resolvability**

While it is possible to configure demand-dial interfaces with the names of the answering routers to which a connection is made, it is recommended that you use IP addresses rather than names. If you use a name and the name resolves to the public IP address of the answering router, traffic sent to services running on the VPN router will be sent in clear text across the Internet. For more information, see "Routing and multi-use VPN routers" in this paper.

### **Answering router reachability**

To be reachable, the answering router must be assigned a public IP address to which packets are forwarded by the routing infrastructure of the Internet. If you have been assigned a static public IP address from an ISP or an Internet registry, this is typically not an issue. In some configurations, the answering router is actually configured with a private IP address and has a published static IP address by which it is known on the Internet. A device between the Internet and the answering router translates the published and actual IP addresses of the answering router in packets to and from the answering router.

While the routing infrastructure might be in place, the answering router might be unreachable due to the placement of firewalls, packet filtering routers, network address translators, security gateways, or other types of devices that prevent packets from either being sent to or received from the answering router computer.

### **VPN routers and firewall configuration**

There are two approaches to using a firewall with a VPN router:

1. The VPN router is attached directly to the Internet and the firewall is between the VPN router and the site. In this configuration, the VPN router must be configured with packet filters that only allow VPN traffic in and out of its Internet interface. The firewall can be configured to allow specific types of inter-site traffic.
2. The firewall is attached to the Internet and the VPN router is between the firewall and the site. In this configuration, both the firewall and the VPN router are attached to a network segment known as the perimeter network (also known as a demilitarized zone [DMZ] or a screened subnet). Both the firewall and the VPN router must be configured with packet filters that allow only VPN traffic to and from the Internet. Figure 2 shows this configuration.

For the details of configuring packet filters for the VPN router and the firewall for both of these configurations, see Appendix A.

### **Design Points: Answering router accessibility from the Internet**

Consider the following when configuring your Internet infrastructure for router-to-router VPN connections:

- Wherever possible, configure your demand-dial interfaces with the IP addresses of answering routers. If you are using names, ensure that the DNS names of your answering routers are resolvable by either

placing an appropriate DNS record in your Internet DNS server or the DNS server of your ISP. Test the resolvability by using the Ping tool to ping the name of each of your answering routers. Due to packet filtering, the result of the ping command may be "Request timed out", but check to ensure that the name specified was resolved by the Ping tool to the correct IP address.

- Ensure that the IP addresses of your answering routers are reachable from the Internet by using the Ping tool to ping the name or address of your answering router with a 5 second timeout (using the -w command line option) when directly connected to the Internet. If you see a "Destination unreachable" error message, the answering router is not reachable.
- Configure packet filtering for PPTP traffic, L2TP traffic, or both types of traffic on the appropriate firewall and answering router interfaces connecting to the Internet and the perimeter network. For more information, see Appendix A.

### Authentication protocols

To authenticate the calling router who is attempting to create a PPP connection, Windows 2000 supports a wide variety of PPP authentication protocols including:

- Password Authentication Protocol (PAP)
- Shiva Password Authentication Protocol (SPAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- MS-CHAP version 2 (MS-CHAP v2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Level Protocol (EAP-TLS)

For PPTP connections, you must use MS-CHAP, MS-CHAP v2, or EAP-TLS. Only these three authentication protocols provide a mechanism to generate the same encryption key on both the calling router and the answering router. MPPE uses this encryption key to encrypt all PPTP data sent on the VPN connection. MS-CHAP and MS-CHAP v2 are password-based authentication protocols.

In the absence of user certificates, MS-CHAP v2 is highly recommended as it is a stronger authentication protocol than MS-CHAP and provides mutual authentication. With mutual authentication, the calling router is authenticated by the answering router and the answering router is authenticated by the calling router.

---

**Note:** If you must use a password-based authentication protocol, enforce the use of strong passwords on your network. Strong passwords are long (greater than 8 characters) and contain a random mixture of upper and lower case letters, numbers, and punctuation. An example of a strong password is f3L\*q02~>xR3w#4o. In an Active Directory™ service domain, use Group Policy settings to enforce the use of strong user passwords.

---

EAP-TLS is designed to be used in conjunction with a certificate infrastructure and user certificates. With EAP-TLS, the calling router sends a user certificate for authentication and the answering router or RADIUS server sends a computer certificate for authentication. This is the strongest authentication method as it does not rely on passwords. If the authenticating server is a Windows 2000 VPN router or an IAS server, EAP-TLS is only available if the authenticating server is a member of an Active Directory domain.

---

**Note:** You can use third-party CAs as long as the certificate in the computer store of the answering router or RADIUS server contains the Server Authentication certificate purpose (also known as a certificate usage, certificate issuance policy, or Enhanced Key Usage [EKU]). A certificate purpose is identified using an object identifier (OID). The OID for Server Authentication is "1.3.6.1.5.5.7.3.1". Additionally, the user certificate installed on the Windows 2000 calling router must contain the Client Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.2").

---

For L2TP/IPSec connections, any PPP authentication protocol can be used because the user authentication occurs after the calling router and answering router have established a secure channel of communication known as an IPSec security association (SA). However, the use of either MS-CHAP v2 and EAP-TLS are recommended to provide mutual user authentication.

### **Design Point: Which authentication protocol to use?**

Consider the following when choosing an authentication protocol for VPN connections:

- If you are using a certificate infrastructure that issues user certificates, use the EAP-TLS authentication protocol for both PPTP and L2TP connections. EAP-TLS is not supported by Windows NT 4.0 RRAS routers.
- If you must use a password-based authentication protocol, use MS-CHAP v2 and enforce strong passwords using Group Policy. MS-CHAP v2 is supported by computers running Windows 2000 and Windows NT 4.0 with RRAS and Service Pack 4 and later.

### VPN protocols

Windows 2000 includes support for two PPP-based router-to-router VPN protocols:

1. Point-to-Point Tunneling Protocol
2. Layer Two Tunneling Protocol

### **Point-to-Point Tunneling Protocol**

Introduced in Windows NT 4.0, PPTP leverages Point-to-Point Protocol (PPP) user authentication and Microsoft Point-to-Point Encryption (MPPE) to encapsulate and encrypt IP and IPX traffic. When MS-CHAP v2 is used with strong passwords, PPTP is a secure VPN technology. For nonpassword-based authentication, EAP-TLS can be used in Windows 2000 to support user certificates. PPTP is widely supported, easily deployed, and can be used across most network address translators (NATs).

### **Layer Two Tunneling Protocol with IPSec**

L2TP leverages PPP user authentication and IPSec Encapsulating Security Payload (ESP) transport mode to encapsulate and encrypt IP and IPX traffic. This combination, known as L2TP/IPSec, uses certificate-based computer identity authentication to create the IPSec security association in addition to PPP-based user authentication. L2TP/IPSec provides data integrity and data authentication for each packet. However, L2TP/IPSec requires a certificate infrastructure to allocate computer certificates and is supported by Windows 2000 VPN routers and other third-party VPN routers.

## Design Point: PPTP or L2TP?

Consider the following when deciding between PPTP and L2TP for router-to-router VPN connections:

- PPTP can be used with Windows 2000 and Windows NT version 4.0 with RRAS. PPTP does not require a certificate infrastructure to issue computer certificates.
- PPTP-based VPN connections provide data confidentiality (captured packets cannot be interpreted without the encryption key). PPTP VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data authentication (proof that the data was sent by the authorized computer).
- PPTP-based calling routers can be located behind a NAT because most NATs include a NAT editor that knows how to properly translate PPTP tunneled data. For example, the Internet connection sharing (ICS) feature of Windows 2000 Network and Dial-up Connections and the NAT routing protocol component of the Windows 2000 Routing and Remote Access service include a NAT editor that translates PPTP traffic from PPTP clients located behind the NAT. Answering routers cannot be behind a NAT unless there are multiple public IP addresses and there is a one-to-one mapping of a public IP address to the private IP address of the answering router or, if there is only one public address, if the NAT is configured to translate and forward the PPTP tunneled data to the VPN router. Most NATs using a single public IP address, including ICS and the NAT routing protocol component, can be configured to allow inbound traffic based on IP addresses and TCP and UDP ports. However, PPTP tunneled data does not use TCP or UDP headers. Therefore, an answering router cannot be located behind a computer using ICS or the NAT routing protocol component when using a single IP address.
- L2TP-based VPN routers cannot be behind a NAT because Internet Key Exchange (IKE), the protocol to negotiate Windows 2000 IPSec security associations, and IPSec-protected traffic is not NAT-translatable.
- L2TP can only be used with Windows 2000 and third-party VPN routers and supports computer certificates as the authentication method for IPSec. Computer certificate authentication requires a certificate infrastructure to issue computer certificates to the answering router computer and all calling router computers.
- By using IPSec, L2TP-based VPN connections provide data confidentiality, data integrity, data authentication, and replay protection.
- PPTP and L2TP is not an either/or choice. By default, a Windows 2000 VPN router supports both PPTP and L2TP connections simultaneously. You can use PPTP for some router-to-router VPN connections (from calling routers that are running Windows NT 4.0 with RRAS or Windows 2000 and do not have an installed computer certificate) and L2TP for other router-to-router VPN connections (from calling routers running Windows 2000 that have an installed computer certificate).
- If you are using both PPTP and L2TP, you can create separate remote access policies that define different connection parameters for PPTP and L2TP connections.

## Site network infrastructure

The network infrastructure of the site is an important element of VPN design. Without proper design, calling routers are unable to obtain proper IP addresses, and packets cannot be forwarded between calling routers and site resources.

## Name resolution

If the calling router is configured with the IP addresses of Domain Name System (DNS) or Windows Internet Name Service (WINS) servers, DNS and WINS server IP addresses are not requested from the answering router during

the PPP connection negotiation. If the calling router is not configured with the IP addresses of DNS and WINS servers, DNS and WINS servers are requested. The answering router never requests DNS and WINS server IP addresses from the calling router.

Unlike Windows 2000 and Windows XP remote access clients, the calling router does not send a DHCPInform message to the answering router to discover additional TCP/IP configuration information.

By default, the calling router does not register itself with the DNS or WINS servers of the answering router. To change this behavior, set the registry value HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\PPP\ControlProtocols\BuiltIn\RegisterRoutersWithNameServers to 1.

## Routing

Each VPN router is an IP router and as such must be properly configured with the set of routes that makes all locations reachable. Specifically, each VPN router needs the following:

- A default route that points to a firewall or router directly connected to the Internet.  
This route makes all of the locations on the Internet reachable.
- One or more routes that summarize the addresses used within the site of the VPN router that points to a neighboring site router.  
These routes make all of the locations within the site of the VPN router reachable from the VPN router. Without these routes, all hosts in the site not connected to the same subnet as the VPN router are unreachable.

To add a default route that points to the Internet, configure the Internet interface with a default gateway and then manually configure the site interface without a default gateway.

To add site routes to the routing table of each VPN router, you can:

- Add static routes using the Routing and Remote Access snap-in. You do not necessarily have to add a route for each subnet in your site. At a minimum, you just need to add the routes that summarize all the possible addresses in your site. For example, if your site uses portions of the private address space 10.0.0.0/8 to number its subnets and hosts, you do not have to add a route for each subnet. Just add a route for 10.0.0.0 with the subnet mask 255.0.0.0 that points to a neighboring router on the site subnet to which your VPN router is attached.
- If you are using the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) routing protocols in your site, you can add and configure the RIP or OSPF routing protocol components of the Routing and Remote Access service so that the VPN router participates in the propagation of routing information as a dynamic router.

If your site has only a single subnet, no further configuration is required.

When a router-to-router VPN connection is made, each router sends traffic using a logical interface that corresponds to the PPTP or L2TP port of the connection. During the PPP negotiation, IP addresses might be assigned to these logical interfaces. Ensuring the reachability of the logical interfaces of VPN routers depends on how you configure each VPN router to obtain IP addresses for remote access clients and calling routers. The IP addresses assigned to VPN routers as they connect can be from:

- An on-subnet address range, which is an address range of the site subnet to which the VPN router is attached.  
An on-subnet address range is used whenever the VPN router is configured to use DHCP to obtain IP

addresses and when the manually configured pool(s) of IP addresses are within the range of addresses of the attached subnet.

- An off-subnet address range, which is an address range that represents a different subnet that is logically attached to the VPN router.

An off-subnet address range is used whenever the VPN router is manually configured with a pool of IP addresses for a separate subnet.

### **On-subnet address range**

If you are using an on-subnet address range, no additional routing configuration is required as the VPN router acts as a proxy for all packets destined to the logical interfaces of the other connected VPN routers. Routers and hosts on the VPN router subnet forward packets destined to the logical interfaces of connected VPN routers to the VPN router and the VPN router relays them to the appropriate connected VPN routers.

### **Off-subnet address range**

If you are using an off-subnet address range, you must add the route(s) that summarize the off-subnet address range to the site routing infrastructure so that traffic destined to the logical interfaces of connected VPN routers are forwarded to the VPN router and then sent by the VPN router to the appropriate connected VPN router. You can add the routes that summarize the off-subnet address range to the routing infrastructure of the site through the following:

- Add static routes to the neighboring router for the off-subnet address range that point to the VPN router's site interface. Configure the neighboring router to propagate this static route to other routers in the site using the dynamic routing protocol used in your site.
- If the VPN router is using OSPF and participating as a dynamic router, the VPN router must be configured as an autonomous system boundary router (ASBR) so that the static routes of the off-subnet address range are propagated to the other OSPF routers in the site.

If your site consists of a single subnet, then you must either configure each site host for persistent route(s) of the off-subnet address range that point to the VPN router's site interface or configure each site host with the VPN router as its default gateway. Because routing for off-subnet address ranges requires additional host configuration, it is recommended that you use an on-subnet address pool for a small office/home office (SOHO) network consisting of a single subnet.

### **Routing and multi-use VPN routers**

If you want to access services running on the VPN router, whether or not the traffic to those services is sent on the Internet in an encrypted or clear text form depends on which address the node is using to access the VPN router service:

- If the node accesses the service running on the VPN router using its site IP address, all traffic is sent encrypted inside the tunnel of the VPN connection.
- If the node accesses the service running on the VPN router using its public IP address, all traffic is sent as clear text outside the tunnel of the VPN connection.

Due to the way in which routes are created on calling routers when making a VPN connection, it may be possible to connect to services running on an answering router, however, the traffic might not be sent across the VPN

connection. When a calling router creates a VPN connection with an answering router, it creates a host route to the answering router that uses the Internet connection. The host route for the answering router's address is created so that it is reachable using the Internet connection. If the host route is not present, VPN traffic to the answering router cannot be sent.

The result of having the host route for the calling router is that all traffic that is sent by nodes in the calling router's site to the answering router's public IP address are not sent across the VPN connection, and are instead sent in an unencrypted form across the network between the calling router and answering router.

For example, when a calling router creates a VPN connection with an answering router and then a node in the calling router's site accesses a file share on the VPN router computer using the VPN router's public IP address, the file sharing traffic is not sent using the router-to-router VPN connection, but is sent in clear text over the network between the calling router and answering router.

Additionally, if packet filters are configured on the answering router that only allow VPN connection traffic, all other traffic sent to the answering router is discarded. In this typical configuration, all attempts to connect to services running on the answering router will fail because traffic attempting to connect to those services are not sent over the VPN connection.

The key to which address is used by the VPN client to access services running on each VPN router lies in the way that the name of the VPN router is resolved. Typical users and applications refer to network resources using names, rather than IP addresses. The name must be resolved to an IP address using either DNS or WINS. If the site DNS and WINS infrastructures never contain a record mapping the VPN router's name to the VPN router's public IP address, traffic to services running on the VPN router is always sent across the VPN connection.

To prevent a VPN router from dynamically registering the public IP address of its Internet interface in the site DNS, obtain properties of the **Internet Protocol (TCP/IP)** component of the Internet connection in Dial-up and Network Connections. Click **Advanced**. In the **Advanced TCP/IP Settings** dialog box, click the **DNS** tab, and then clear the **Register this connection's addresses in DNS** check box.

To prevent a VPN router from registering the public IP address of its Internet interface with site WINS servers, obtain properties of the **Internet Protocol (TCP/IP)** component of the Internet connection in the Dial-up and Network Connections folder. Click **Advanced**. In the **Advanced TCP/IP Settings** dialog box, click the **WINS** tab, and then click **Disable NetBIOS over TCP/IP**.

### **Design Points: Routing infrastructure**

Consider the following when configuring the routing infrastructure for router-to-router VPN connections:

- Configure the Internet interface of the VPN router with a default gateway. Do not configure the site interface of the VPN router with a default gateway.
- Add static IP routes to the VPN router that summarize the addresses used in the site in which the VPN router is located. Alternately, if you use either RIP or OSPF as your dynamic routing protocol, configure and enable RIP or OSPF on the VPN router. If you use a routing protocol other than RIP or OSPF, such as Interior Gateway Routing Protocol (IGRP), configure the neighboring router for RIP or OSPF on the interface connected to the subnet containing the VPN router, and then configure IGRP on all other interfaces.
- If the VPN router is hosting other services, ensure that the name of the VPN router is always resolved to the private or site IP address of the VPN router. To do this, disable DNS dynamic update and NetBIOS

over TCP/IP on the Internet interface(s) of the VPN router.

- Configure the VPN router with an on-subnet address range by obtaining IP addresses through DHCP or by manually configuring on-subnet address pools.

### AAA Infrastructure

The authentication, authorization, and accounting (AAA) infrastructure exists to:

- Authenticate the credentials of calling routers.
- Authorize the VPN connection.
- Record the VPN connection creation and termination for accounting purposes.

The AAA infrastructure consists of:

- The answering router computer
- RADIUS server computers
- Domain controllers

As previously discussed, a Windows 2000 answering router can be configured with either Windows or RADIUS as its authentication or accounting provider. RADIUS provides a centralized AAA service when you have multiple answering routers and remote access VPN servers or a mix of heterogeneous dial-up and VPN equipment.

When you configure Windows as the authentication provider, the answering router performs the authentication of the VPN connection by communicating with a domain controller using a secure remote procedure call (RPC) channel and authorization of the connection attempt through the dial-in properties of the user account and locally configured remote access policies.

When you configure RADIUS as the authentication provider, the answering router relies on a RADIUS server to perform both the authentication and authorization. When a VPN connection is attempted, the calling router credentials and other connection parameters are sent by the answering router to the configured RADIUS server in a RADIUS Access-Request message. If the connection attempt is both authenticated and authorized, the RADIUS server sends back a RADIUS Access-Accept message. If the connection attempt is either not authenticated or not authorized, the RADIUS server sends back a RADIUS Access-Reject message.

When you configure Windows as the accounting provider, the answering router logs VPN connection information in a local log file (*SystemRoot\System32\Logfiles\Logfile.log* by default) based on settings on the **Settings** tab of the properties of the **Local File** object in the **Remote Access Logging** folder in the Routing and Remote Access snap-in. By default, all types of logging are disabled.

When you configure RADIUS as the authentication provider, the answering router sends RADIUS accounting messages for VPN connections on a RADIUS server, which records the accounting information.

If you are using RADIUS and a Windows domain as the user account database for which to verify user credentials and obtain dial-in properties, Microsoft recommends using the Windows 2000 Internet Authentication Service (IAS). IAS is a full-featured RADIUS server that is tightly integrated with Windows 2000, Active Directory, and the Routing and Remote Access service.

When IAS is used as the RADIUS server:

- IAS performs the authentication of the VPN connection by communicating with a domain controller using a secure RPC channel. IAS performs authorization of the connection attempt through the dial-in properties of the user account and remote access policies configured on the IAS server.

- IAS logs all RADIUS accounting information in a local log file (*SystemRoot\System32\Logfiles\Logfile.log* by default) based on settings configured on the properties of the **Local File** object in the **Remote Access Logging** folder in the Internet Authentication Service snap-in.

### Remote access policies

Remote access policies are an ordered set of rules that define how connections are either accepted or rejected. For connections that are accepted, remote access policies can also define connection restrictions. For each rule, there are one or more conditions, a set of profile settings, and a remote access permission setting. Connection attempts are evaluated against the remote access policies in order, trying to determine whether the connection attempt matches all of the conditions of each policy. If the connection attempt does not match all of the conditions of any policy, the connection attempt is rejected.

If a connection matches all the conditions of a remote access policy and is granted remote access permission, the remote access policy profile specifies a set of connection restrictions. The dial-in properties of the user account also provide a set of restrictions. Where applicable, user account connection restrictions override the remote access policy profile connection restrictions.

Remote access policies consist of the following elements:

- Conditions
- Permission
- Profile settings

### Conditions

Remote access policy conditions are one or more attributes that are compared to the settings of the connection attempt. If there are multiple conditions, then all of the conditions must match the settings of the connection attempt in order for it to match the policy. For VPN connections, you commonly use the following conditions:

- **NAS-Port-Type.** By setting the **NAS-Port-Type** condition to **Virtual (VPN)**, you can specify all VPN connections.
- **Tunnel-Type.** By setting the **Tunnel-Type** to **Point-to-Point Tunneling Protocol (PPTP)** or **Layer Two Tunneling Protocol (L2TP)**, you can specify different policies for PPTP and L2TP connections.
- **Windows-Groups.** By setting the **Windows-Groups** to the appropriate groups, you can specify connection parameters based on group membership.

### Permission

You can use the permission setting to either grant to deny remote access for the connection attempt if the remote access permission of the user account is set to **Control access through Remote Access Policy**. Otherwise, the remote access permission setting on the user account determines the remote access permission.

### Profile Settings

A remote access policy profile is a set of properties that are applied to a connection when it is authorized. For VPN connections, you can use the following profile settings:

- Dial-in constraints can be used to define how long the connection can exist or be idle before being terminated by the answering router, among others.

- Authentication settings can define which authentication protocols the calling router can use when sending its credentials and the configuration of EAP types, such as EAP-TLS.
- Encryption settings can define whether encryption is required and the encryption strength. For encryption strengths, Windows 2000 supports **Basic** (40-bit MPPE for PPTP and 56-bit Data Encryption Standard [DES] for L2TP), **Strong** (56-bit MPPE for PPTP and 56-bit DES for L2TP), or **Strongest** (128-bit MPPE for PPTP and 3DES for L2TP). **Strongest** can be used only if the Windows 2000 High Encryption Pack or Service Pack 2 and later is installed.

For example, you can create a Windows 2000 group called VPNRouters whose members are the user accounts of all calling routers. Then, you create a policy with two conditions on the policy: NAS-Port-Type is set to Virtual (VPN) and Windows-Group is set to VPNRouters. Finally, you configure the profile for the policy to select a specific authentication method and encryption strength.

---

**Note:** IP packet filters on the **IP** tab of the profile settings of a remote access policy only apply to remote access VPN connections. They have no effect on demand-dial connections.

---

### Windows domain user accounts and groups

Windows NT version 4.0 domains, Windows 2000 mixed-mode Active Directory domains, and Windows 2000 native-mode domains contain the user accounts and groups used by the Routing and Remote Access service and IAS to authenticate and authorize VPN connection attempts.

User accounts contain the user name and a form of the user's password that can be used for validation of the calling router's user credentials. Additional account properties determine whether the user account is enabled or disabled, locked out, or permitted to logon only during specific hours. If a user account is disabled, locked out, or not permitted to logon during the time of the VPN connection, the router-to-router VPN connection attempt is rejected. Additionally, if the user account of the calling router is configured to change the password at the next login, the router-to-router VPN connection attempt will fail because changing the password while attempting to make the connection is an interactive process. Demand-dial routers need to be able to make connections as needed without requiring human intervention. Therefore, all user accounts for calling routers must be configured with the **User must change password at next logon** checkbox cleared and the **Password never expires** checkbox selected for the account options on the **Account** tab on the properties of the user account. When you create dial-in accounts with the Demand-Dial Interface Wizard, these account settings are automatically configured.

You should use a separate user account for each site that contains a calling router. Each user account should have a name that matches a demand-dial interface configured on the answering router. When you create dial-in accounts with the Demand-Dial Interface Wizard, this one-to-one relationship between user accounts used by calling routers in separate sites and demand-dial interfaces is automatically maintained.

User accounts also contain dial-in settings. The dial-in setting most relevant for VPN connections is the remote access permission setting, which has the following values:

- Allow access
- Deny access
- Control access through Remote Access Policy

The **Allow access** and **Deny access** settings explicitly allow or deny remote access and are equivalent to the remote access permission setting of Windows NT 4.0 domain accounts. When you use the **Control access**

**through Remote Access Policy** setting, the remote access permission is determined by the remote access permission setting of the matching remote access policy. If the user account is in a mixed-mode domain, the **Control access through Remote Access Policy** setting is not available and you must manage remote access permission on a per-user basis. If the user account is in a native-mode domain, the **Control access through Remote Access Policy** setting is available and you can manage remote access permission on a per-user basis or using groups. When a dial-in account is created with the Demand-Dial Interface Wizard, the remote access permission is set to **Allow access**.

When using groups to manage access, you can use your existing groups and create remote access policies that either allow or reject access or restrict access based on the group name. For example, the Employees group has no VPN remote access restrictions, however, the Contractors group can only create VPN connections during business hours. Alternately, you can create groups based on the type of connection being made. For example, you can create a VPNRouters group and add as members all the user accounts allowed to create VPN connections.

Both the Routing and Remote Access service and IAS can use Active Directory universal principal names (UPNs) and universal groups. In a large domain with thousands of users, create a universal group for all of the users for whom you want to allow access, and then create a remote access policy that grants access for this universal group. Do not put all of your user accounts directly into the universal group, especially if you have a large number of them on your network. Instead, create separate global groups that are members of the universal group, and add users to those global groups.

### **One-way initiated connections and static routes on the user account**

With one-way initiated connections, one router is always the answering router and one router is always the calling router. The answering router accepts the connection and the calling router initiates the connection. One-way initiated connections are well suited to a spoke-and-hub topology where the branch office router is the only router that initiates the connection.

To simplify configuration for one-way initiated connections, user accounts on stand-alone Windows 2000 servers or in a native-mode Active Directory domain support the configuration of static routes. The static routes are automatically added to the routing table of the VPN router when a VPN connection using the user account is made. If the VPN router is participating in dynamic routing for the site, the routes are propagated to the other routers in the site using routing protocols such as RIP and OSPF. Static routes on user accounts are configured by selecting the **Apply static routes** check box on the **Dial-in** tab on the properties of a user account, and then adding static routes.

To use static routes on the user account, configure the calling router normally. On the answering router, all you have to do is create a user account that is used by the calling router and configure static routes that correspond to the calling router's site. Because there is no demand-dial interface on the answering router with the same name as the user account of the calling router, the incoming VPN connection is determined to be a remote access connection. The static routes of the calling router's user account are added to the VPN router's routing table and all traffic to the locations implied by the static routes is sent across the logical remote access connection to the calling router.

---

**Note:** Static routes on the user account are only applied to the answering router when the incoming connection is a remote access VPN connection (the user account in the credentials of the calling router does not match the name of a demand-dial interface on the answering router). Static routes on the user account are not applied when the incoming connection is a demand-dial connection.

---

### **Design Points: AAA infrastructure**

Consider the following when configuring the AAA infrastructure for router-to-router VPN connections:

- If you have multiple VPN routers and you want to centralize AAA service or a heterogeneous mixture of dial-up and VPN equipment, use RADIUS servers and configure the VPN router for the RADIUS authentication and accounting providers.
- If your user account database is a Windows domain, use IAS as your RADIUS server. If you use IAS, install IAS on a domain controller for best performance. Install at least two IAS servers for fail-over and fault tolerance of AAA services.
- Whether configured locally or on an IAS server, use remote access policies to authorize VPN connections and specify connection constraints. For example, use the remote access policy profile settings to grant access based on group membership, to enforce the use of encryption and a specific encryption strength, or specify the use of EAP-TLS.
- For a large Active Directory domain, nest global groups within universal groups to manage access based on group membership.
- For one-way initiated connections, you can configure the calling router normally and configure the answering router with a user account that contains the static routes of the calling router's site.
- Sensitive fields of RADIUS messages, such as the user password and encryption keys, are encrypted with the RADIUS shared secret configured on the VPN router and the RADIUS server. Make the shared secret a long (16 characters or longer), random sequence of letters, numbers, and punctuation and change it often to protect your RADIUS traffic. An example of a strong shared secret is 8d#>9fq4bV)H7%a3. To further protect RADIUS traffic, use Windows 2000 IPsec policies to provide data confidentiality for all traffic using the RADIUS UDP ports (1812 and 1645 for RADIUS authentication traffic and 1813 and 1646 for RADIUS accounting traffic).

### Certificate infrastructure

To perform certificate-based authentication for L2TP connections and user certificate-based authentication for router-to-router VPN connections using EAP-TLS, a certificate infrastructure must be in place to issue the proper certificates to submit during the authentication process and to validate the certificate being submitted.

### **Computer certificates for L2TP/IPsec**

If you manually configure the certificate authentication method for a rule of an IPsec policy in Windows 2000, you can specify the list of root certification authorities (CAs) from which a certificate is accepted for authentication. For L2TP connections, the IPsec rule for L2TP traffic is automatically configured and the list of root CAs is not configurable. Instead, each computer in the L2TP connection sends a list of root CAs to its IPsec peer from which it accepts a certificate for authentication. The root CAs in this list correspond to the root CAs that issued certificates that are stored in the computer certificate store. For example, if Computer A was issued computer certificates by

root CAs CertAuth1 and CertAuth2, it notifies its IPsec peer during main mode negotiation that it will accept certificates for authentication from only CertAuth1 and CertAuth2. If the IPsec peer, Computer B, does not have a valid certificate in its computer certificate store issued from either CertAuth1 or CertAuth2, IPsec security negotiation fails.

Ensure one of the following before attempting an L2TP connection:

1. Both the calling router and answering router were issued computer certificates from the same CA.
2. Both the calling router and answering router were issued computer certificates from CAs that follow a valid certificate chain up to the same root CA.

In general, the calling router must have a valid computer certificate installed that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the answering router trusts. Additionally, the answering router must have a valid computer certificate installed that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the calling router trusts.

A single CA commonly issues computer certificates to all computers in an organization. Because of this, all computers within the organization both have computer certificates from a single CA and request certificates for authentication from the same single CA.

For information about installing computer certificates on VPN routers for L2TP connections, see "Deploying an L2TP-based Router-to-Router VPN Connection."

### **User and computer certificates for EAP-TLS authentication**

To perform EAP-TLS authentication for a router-to-router VPN connection in Windows 2000:

- The calling router must be configured to submit a user certificate during the EAP-TLS authentication process.
- The authenticating server must be configured to submit a computer certificate during the EAP-TLS authentication process. The authenticating server is either the answering router (if the answering router is configured to use the Windows authentication provider) or a RADIUS server (if the answering router is configured to use the RADIUS authentication provider).

EAP-TLS authentication is successful when the following conditions are met:

- The calling router submits a valid user certificate that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the answering router trusts.
- The authenticating server submits a valid computer certificate that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the calling router trusts.
- The user certificate of the calling router contains the Client Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.2").
- The computer certificate of the answering router contains the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1").

For a Windows 2000 CA, a Router (Offline Request) certificate, a special type of user certificate for demand-dial connections, is created and mapped to an Active Directory user account. When the calling router attempts a VPN connection, the Router (Offline Request) certificate is sent during the connection negotiation process. If the Router (Offline Request) certificate is valid, it is used to determine the appropriate user account from which dial-in properties are obtained.

For information about configuring user and computer certificates for EAP-TLS authentication, see "Deploying a PPTP-based Router-to-Router VPN Connection" and "Deploying an L2TP-based Router-to-Router VPN Connection."

### **Design Points: Certificate infrastructure**

Consider the following when configuring the certificate infrastructure for router-to-router VPN connections:

- In order to create L2TP/IPSec router-to-router VPN connections using computer certificate authentication for IPSec, you must install a certificate in the computer certificate store of the calling router and the answering router.
- In order to authenticate VPN connections using EAP-TLS, the calling router must have a user certificate installed and the authenticating server (either the answering router or the RADIUS server) must have a computer certificate installed.
- To install a computer or user certificate on a computer across the Internet, make a PPTP connection using a password-based authentication protocol such as MS-CHAP v2. After connecting, use the Certificate Manager snap-in or Internet Explorer to request the appropriate certificates. Once the certificates are installed, disconnect and then reconnect with the appropriate VPN protocol and authentication method. An example of this situation is a computer at a remote branch office without the certificates needed to make L2TP/IPSec or EAP-TLS-authenticated connections.

---

## Deploying a PPTP-based Router-to-Router VPN Connection

The deployment of PPTP-based router-to-router VPN connections using Windows 2000 consists of the following:

- Deploy certificate infrastructure
- Deploy Internet infrastructure
- Deploy the answering router
- Deploy the calling router
- Deploy AAA infrastructure
- Deploy site network infrastructure
- Deploy intersite network infrastructure

### Deploying certificate infrastructure

For PPTP-based VPN connections, a certificate infrastructure is needed only when you are using EAP-TLS authentication. If you are only using a password-based authentication protocol such as MS-CHAP v2, a certificate infrastructure is not required and is not used for the authentication of the VPN connection.

To use EAP-TLS authentication for router-to-router VPN connections, you must:

- Install a user certificate on each calling router computer.
- Configure EAP-TLS on the calling router.
- Install a computer certificate on the authenticating server (the answering router or the RADIUS server).
- Configure EAP-TLS on the answering router and remote access policy.

### Installing a user certificate on a calling router

If you are using a Windows 2000 CA, a Router (Offline Request) certificate is created and mapped to an Active Directory user account. To deploy a Router (Offline Request) certificates for a calling router, the network administrator must:

1. Configure the Windows 2000 CA to issue Router (Offline Request) certificates.
2. Request a Router (Offline Request) certificate.
3. Export the Router (Offline Request) certificate.
4. Map the certificate to the appropriate user account.
5. Send the Router (Offline Request) certificate to the network administrator of the calling router.
6. Import the Router (Offline Request) certificate on the calling router.

For more information about deploying Router (Offline Request) certificates for demand-dial routing, see the topic titled "Branch office demand-dial connection" in Windows 2000 Server online Help.

For a third-party CA, see the documentation for the CA software for instructions about how to create a user certificate with the Client Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.2") and export it so that it can be mapped to an Active Directory user account and sent to the network administrator of the calling router. You must also export the root CA certificate, the certificate of the issuing CA, and the certificates of any intermediate CAs and import them to the proper folder of the computer certificate store of the answering router using the Certificate Manager snap-in.

## Configuring EAP-TLS on the calling router

To configure EAP-TLS for user certificates on the calling router:

- The demand-dial interface must be configured to use EAP with the **Smart Card or other certificate** EAP type by configuring advanced settings on the **Security** tab on the properties of a demand-dial interface. In the properties of the **Smart Card or other certificate** EAP type, select **Use a certificate on this computer**. If you want to validate the computer certificate of the VPN or IAS server, select **Validate server certificate**. If you want to ensure that the server's DNS name ends in a specific string, select **Connect only if server name ends with** and type the string. To require the server's computer certificate to have been issued a certificate from a specific trusted root CA, select the CA in **Trusted root certificate authority**.
- Right-click the demand-dial interface and click **Credentials**. In the **Connect** dialog box, select the proper user or Router (Offline Request) certificate in **User name on certificate**, and then click **OK**.

## Installing a computer certificate on the authenticating server

To install a computer certificate, a certification authority must be present to issue certificates. If the CA is a Windows 2000 CA and the authenticating server is either the answering router or a Windows 2000 Internet Authentication Service (IAS) RADIUS server, you can install a certificate in the computer certificate store of the authenticating server in the following different ways:

1. By configuring the automatic allocation of computer certificates to computers in a Windows 2000 domain. This method allows a single point of configuration for the entire domain. All members of the domain automatically receive a computer certificate through group policy.
2. By using the Certificate Manager snap-in to request a certificate to store in the Certificates (Local Computer)\Personal folder. In this method, each computer must separately request a computer certificate from the CA. You must have administrator permissions to install a certificate using the Certificate Manager snap-in.
3. By using Internet Explorer and web enrollment to request a certificate and store it in local machine store. In this method, each computer must separately request a computer certificate from the CA. You must have administrator permissions to install a certificate using Web enrollment.

Based on the certificate policies in your organization, you only need to perform one of these methods.

For more information about using the Windows 2000 CA to obtain computer certificates, see the topics titled "Machine certificates for L2TP over IPSec VPN connections" and "Submit an advanced certificate request via the Web" in Windows 2000 Server online Help.

For a third-party CA, see the documentation for the CA software for instructions about how to create a certificate with the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1") and export it so that it can be imported using the Certificate Manager snap-in by an administrator on the answering router. Additionally, the root CA certificate, the certificate of the issuing CA, and the certificates of any intermediate CAs must be exported and imported on the calling router.

## Configuring EAP-TLS on the answering router and remote access policy

To configure EAP-TLS authentication on the answering router:

- EAP must be enabled as an authentication type on the **Authentication Methods** dialog box available

from the **Security** tab in the properties of the answering router in the Routing and Remote Access snap-in.

To configure EAP-TLS authentication on the remote access policy or either the answering router or IAS server:

- On the remote access policy that is being used for router-to-router VPN connections, EAP must be enabled with the **Smart Card or other certificate** EAP type selected on the **Authentication** tab on the policy's profile settings. If the computer on which the remote access policy is being configured has multiple computer certificates installed, configure the properties of the **Smart Card or other certificate** EAP type and select the appropriate computer certificate to submit during the EAP-TLS authentication process.

If you are using a third-party RADIUS server, see the RADIUS server documentation for information on how to enable EAP-TLS and configure EAP-TLS to use the correct computer certificate.

### Deploying Internet infrastructure

Deploying the Internet infrastructure for router-to-router VPN connections consists of the following:

- Place VPN routers in the perimeter network or on the Internet.
- Install Windows 2000 Server on VPN router computers and configure Internet interfaces.

#### **Placing VPN routers in perimeter network or on the Internet**

Decide where to place the VPN routers in relation to your Internet firewall. In the most common configuration, the VPN routers are placed behind the firewall on the perimeter network between your site and the Internet. If so, configure packet filters on the firewall to allow PPTP traffic to and from the IP address of the VPN routers' perimeter network interfaces. For more information, see Appendix A.

#### **Installing Windows 2000 Server on VPN routers and configuring Internet interfaces**

Install Windows 2000 Server on VPN router computers and connect it to either the Internet or to perimeter network with one network adapter and connect it to the site with another network adapter. Without running the Routing and Remote Access Server Setup Wizard, the VPN router computer will not forward IP packets between the Internet and the site. For the connection connected to the Internet or the perimeter network, configure the TCP/IP protocol with a public IP address, a subnet mask, and the default gateway of either the firewall (if the router is connected to a perimeter network) or an ISP router (if the router is directly connected to the Internet). Do not configure the connection with DNS server or WINS server IP addresses.

### Deploying the answering router

Deploying the answering router for a router-to-router VPN connection consists of the following:

- Configure the answering router's connection to the site.
- Run the Routing and Remote Access Server Setup Wizard.
- Configure a demand-dial interface.

#### **Configuring the answering router's connection to the site**

Configure the connection connected to the site with a manual TCP/IP configuration consisting of IP address, subnet mask, site DNS servers, and site WINS servers. Note that you must not configure the default gateway on the site

connection to prevent default route conflicts with the default route pointing to the Internet.

### Running the Routing and Remote Access Server Setup Wizard

Run the Routing and Remote Access Server Setup Wizard to configure the Windows 2000 answering router using the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click your server name, and then click **Configure and Enable Routing and Remote Access**.
3. In **Common Configurations**, click **Virtual Private Network (VPN) server** and then click **Next**. If you want to use the answering router computer as a network address translator (NAT), Web server, or other function, see Appendix B.
4. In **Remote Client Protocols**, verify that all data protocols that you want to route over router-to-router VPN connections are present. By default, all of the protocols that can be used with a remote access or router-to-router VPN connection are listed. Click **Next**.
5. In **Internet Connection**, click the connection that corresponds to the interface connected to the Internet or your perimeter network, and then click **Next**.
6. In **IP Address Assignment**, click **Automatic** if the answering router should use DHCP to obtain IP addresses for calling routers. Or, click **From a specified range of addresses** to use one or more static ranges of addresses. If any of the static address ranges is an off-subnet address range, routes must be added to the routing infrastructure in order for the virtual interfaces of calling routers to be reachable. When IP address assignment is complete, click **Next**.
7. In **Managing Multiple Remote Access Servers**, if you are using RADIUS for authentication and authorization, click **Yes, I want to use a RADIUS server**, and then click **Next**.
  - In **RADIUS Server Selection**, configure the primary (mandatory) and secondary (optional) RADIUS servers and the shared secret, and then click **Next**.
8. Click **Finish**.
9. Start the Routing and Remote Access service when prompted.

By default, only 128 PPTP ports are configured on the WAN Miniport (PPTP) device. If you need more PPTP ports, configure the **WAN Miniport (PPTP)** device from the properties of the **Ports** object in the Routing and Remote Access snap-in.

By default, only the MS-CHAP and MS-CHAP v2 protocols are enabled. If you are using user certificates for authentication, select **Extensible Authentication Protocol (EAP)** check box from the **Authentication Methods** dialog box available from the **Security** tab on the properties of the answering router computer in the Routing and Remote Access snap-in.

### Configuring a demand-dial interface

From the Routing and Remote Access snap-in on the answering router, perform the following steps:

1. In the console tree, right-click **Routing Interfaces**, and then click **New Demand-dial Interface**.
2. In the **Welcome to the Demand-Dial Interface Wizard** dialog box, click **Next**.
3. In the **Interface Name** dialog box, type the name of the demand-dial interface, and then click **Next**.
4. In the **Connection Type** dialog box, click **Connect using virtual private networking (VPN)**, and then

click **Next**.

5. In the **VPN Type** dialog box, click **Point to Point Tunneling Protocol (PPTP)**, and then click **Next**.

6. In the **Destination Address** dialog box, type the IP address of the calling router.

For a two-way-initiated router to-router VPN connection, configure the IP address of the calling router. For a one-way initiated router-to-router VPN connection, you can skip this step because the answering router never uses this interface to initiate a connection to the calling router.

7. In the **Protocols and Security** dialog box, select the **Route IP packets on this interface**, **Route IPX packets on this interface** (if needed), and **Add a user account so that a remote router can dial in** check boxes, and then click **Next**.

8. In the **Dial In Credentials** dialog box, type the password of the user account used by the calling router in **Password** and **Confirm password**, and then click **Next**. This step automatically creates a user account with the same name as the demand-dial interface that is being created. This is done so that when the calling router initiates a connection to the answering router, it is using a user account name that matches the name of a demand-dial interface. Therefore, the answering router can determine that the incoming connection from the calling router is a demand-dial connection rather than a remote access connection.

9. In the **Dial Out Credentials** dialog box, type the user name in **User name**, the user account domain name in **Domain**, and the user account password in both **Password** and **Confirm password**.

For a two-way-initiated router to-router VPN connection, configure the name, domain, and password when this router is acting as the calling router. For a one-way initiated router-to-router VPN connection, you can type any name in **User name** and skip the rest of the fields because this router never uses this interface to initiate a connection to the calling router.

10. In the **Completing the demand-dial interface wizard** dialog box, click **Finish**.

The result of this configuration is a PPTP-based demand-dial interface over which IP routing is enabled. A user account with the same name as the demand-dial interface is automatically added with correct account and dial-in settings.

## Deploying the calling router

Deploying the calling router for a router-to-router VPN connection consists of the following:

- Configure the calling router's connection to the site.
- Run the Routing and Remote Access Server Setup Wizard.
- Configure a demand-dial interface.

### Configuring the calling router's connection to the site

Configure the connection connected to the site with a manual TCP/IP configuration consisting of IP address, subnet mask, site DNS servers, and site WINS servers. Note that you must not configure the default gateway on the site connection to prevent default route conflicts with the default route pointing to the Internet.

### Running the Routing and Remote Access Server Setup Wizard

Run the Routing and Remote Access Server Setup Wizard to configure the Windows 2000 calling router using the

following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click your server name, and then click **Configure and Enable Routing and Remote Access**.
3. In **Common Configurations**, click **Virtual Private Network (VPN) server** and then click **Next**. If you want to use the calling router computer as a network address translator (NAT), Web server, or other function, see Appendix B.
4. In **Remote Client Protocols**, verify that all data protocols that you want to route over router-to-router VPN connections are present. By default, all of the protocols that can be used with a remote access or router-to-router VPN connection are listed. Click **Next**.
5. In **Internet Connection**, click the connection that corresponds to the interface connected to the Internet or your perimeter network, and then click **Next**.
6. In **IP Address Assignment**, click **Automatic** if the calling router should use DHCP to obtain IP addresses for other calling routers when it is acting as an answering router. Or, click **From a specified range of addresses** to use one or more static ranges of addresses. If any of the static address ranges is an off-subnet address range, routes must be added to the routing infrastructure in order for the virtual interfaces of routers calling this router to be reachable. When IP address assignment is complete, click **Next**.
7. In **Managing Multiple Remote Access Servers**, if you are using RADIUS for authentication and authorization, click **Yes, I want to use a RADIUS server**, and then click **Next**.
  - In **RADIUS Server Selection**, configure the primary (mandatory) and secondary (optional) RADIUS servers and the shared secret, and then click **Next**.
8. Click **Finish**.
9. Start the Routing and Remote Access service when prompted.

By default, only 128 PPTP ports are configured on the WAN Miniport (PPTP) device. If you need more PPTP ports, configure the **WAN Miniport (PPTP)** device from the properties of the **Ports** object in the Routing and Remote Access snap-in.

By default, only the MS-CHAP and MS-CHAP v2 protocols are enabled. If you are using user certificates for authentication, select **Extensible Authentication Protocol (EAP)** check box from the **Authentication Methods** dialog box available from the **Security** tab on the properties of this router computer in the Routing and Remote Access snap-in.

### Configuring a demand-dial interface

From the Routing and Remote Access snap-in on the calling router, perform the following steps:

1. In the console tree, right-click **Routing Interfaces**, and then click **New Demand-dial Interface**.
2. In the **Welcome to the Demand-Dial Interface Wizard** dialog box, click **Next**.
3. In the **Interface Name** dialog box, type the name of the demand-dial interface. For a two-way initiated connection, this is the same name as the user name in the user credentials used by the answering router when it is acting as a calling router. Click **Next**.
4. In the **Connection Type** dialog box, click **Connect using virtual private networking (VPN)**, and then click **Next**.
5. In the **VPN Type** dialog box, click **Point to Point Tunneling Protocol (PPTP)**, and then click **Next**.

6. In the **Destination Address** dialog box, type the IP address of the answering router.
7. In the **Protocols and Security** dialog box, select the **Route IP packets on this interface**, **Route IPX packets on this interface** (if needed) check boxes. For a two-way initiated connection, select the **Add a user account so that a remote router can dial in** check box. Click **Next**.
8. For a two-way initiated connection, in the **Dial In Credentials** dialog box, type the password of the user account used by the answering router acting as a calling router in **Password** and **Confirm password**, and then click **Next**. This step automatically creates a user account with the same name as the demand-dial interface that is being created. This is done so that when the answering router acting as a calling router initiates a connection to this router, it is using a user account name that matches the name of a demand-dial interface. Therefore, this router can determine that the incoming connection from the answering router acting as a calling router is a demand-dial connection rather than a remote access connection.
9. In the **Dial Out Credentials** dialog box, type the user name in **User name**, the user account domain name in **Domain**, and the user account password in both **Password** and **Confirm password**.
10. In the **Completing the demand-dial interface wizard** dialog box, click **Finish**.

The result of this configuration is a PPTP-based demand-dial interface over which IP routing is enabled. A user account with the same name as the demand-dial interface is automatically added with correct account and dial-in settings.

## Deploying AAA infrastructure

Deploying the AAA infrastructure for router-to-router VPN connections consists of the following:

- Configure Active Directory for user accounts and groups.
- Configure the primary IAS server on a domain controller.
- Configure the secondary IAS server on a different domain controller.

This configuration must be done at each site containing an answering router. For branch offices with few computers and a single answering router, it is easier to configure the Routing and Remote Access service for Windows authentication and use locally configured remote access policies than configuring a separate IAS server computer.

### Configuring Active Directory for user accounts and groups

To configure Active Directory for user accounts and groups, do the following:

1. Ensure that all calling routers have a corresponding user account with the correct account and dial-in settings. This includes calling routers for branch offices and business partners. User accounts with the correct account and dial-in settings are automatically created when you select the **Add a user account so that a remote router can dial in** check box on the **Protocols and Security** dialog box in the Demand-Dial Interface Wizard.
2. Organize user accounts used by calling routers into the appropriate universal and nested groups to take advantage of group-based remote access policies. For more information, see the topic titled "Universal, global, and domain local groups" in Windows 2000 Server online Help.

### Configuring the primary IAS server on a domain controller

To configure the primary IAS server on a domain controller, do the following:

1. On the domain controller, install IAS as an optional networking component. For more information, see the topic titled "Install IAS" in Windows 2000 Server online Help.
2. Configure the IAS server computer (the domain controller) to read the properties of user accounts in the domain. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help.
3. If the IAS server authenticates connection attempts for user accounts in other domains, verify that these domains have a two-way trust with the domain in which the IAS server computer is a member. Next, configure the IAS server computer to read the properties of user accounts in other domains. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help. For more information about trust relationships, see the topic titled "Understanding domain trusts" in Windows 2000 Server online Help.

If the IAS server authenticates connection attempts for user accounts in other domains, and those domains do not have a two-way trust with the domain in which the IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains.

4. Enable file logging for accounting and authentication events. For more information, see the topic titled "Configure log file properties" in Windows 2000 Server online Help.
5. Add the VPN router(s) as RADIUS clients of the IAS server. For more information, see the topic titled "Add RADIUS clients" in Windows 2000 Server online Help. For the IP address of each VPN router, use the site IP address assigned to the VPN router. If you are using names, use the internal name of the VPN router. Use strong shared secrets.
6. Create remote access policies that reflect your remote access usage scenarios. For example, to configure a remote access policy that requires PPTP-based router-to-router VPN connections for members of the VPNRouters group to use MS-CHAP v2 authentication and 128-bit encryption, create a remote access policy with the following settings:

Policy name: Router-to-router VPN connections

Conditions:

**NAS-Port-Type** matches **Virtual (VPN)**

**Tunnel-Type** matches **Point-to-Point Tunneling Protocol**

**Windows-Groups** matches **VPNRouters** (example)

Permission: **Grant remote access permission**

Profile settings, **Authentication** tab:

Select **Microsoft Encrypted Authentication (MS-CHAP v2)**. Clear all other check boxes.

Profile settings, **Encryption** tab:

Select the **Strongest** check box, and then clear all other check boxes.

7. If you have created new remote access policies, either delete the default remote access policy named **Allow access if dial-up permission is enabled**, or move it so that it is the last policy to be evaluated. For more information, see the topics titled "Delete a remote access policy" and "Change the policy evaluation order" in Windows 2000 Server online Help.

---

**Note:** The **Strongest** encryption strength is only available after installing either the Windows 2000 High Encryption Pack or Windows 2000 Service Pack 2 (or later) on the IAS server computer.

---

### Configuring the secondary IAS server on a different domain controller

To configure the secondary IAS server on a different domain controller, do the following:

1. On the other domain controller, install IAS as an optional networking component. For more information, see the topic titled "Install IAS" in Windows 2000 Server online Help.
2. Configure the secondary IAS server computer (the other domain controller) to read the properties of user accounts in the domain. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help.
3. If the secondary IAS server authenticates connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the secondary IAS server computer is a member. Next, configure the secondary IAS server computer to read the properties of user accounts in other domains. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help. For more information about trust relationships, see the topic titled "Understanding domain trusts" in Windows 2000 Server online Help.  
If the secondary IAS server authenticates connection attempts for user accounts in other domains, and those domains do not have a two-way trust with the domain in which the secondary IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains.
4. To copy the configuration of the primary IAS server to the secondary IAS server, type **netsh aaa show config > path\file.txt** at a command prompt on the primary IAS server. This stores the configuration settings, including registry settings, in a text file. The path can be relative, absolute, or a network path.
5. Copy the file created in step 4 to the secondary IAS server. At a command prompt on the secondary IAS server, type **netsh exec path\file.txt**. This imports all the settings configured on the primary IAS server to the secondary IAS server.

### Deploying site network infrastructure

Deploying the network infrastructure of a site for router-to-router VPN connections consists of the following:

- Configure routing on the VPN routers.
- Verify reachability from each VPN router.
- Configure routing for off-subnet address pools.

### Configuring routing on the VPN routers

In order for your VPN routers to properly forward traffic to locations within the site in which they are located, you must configure them with either static routes that summarize all the possible addresses used on in the site or with routing protocols so that the VPN router can participate as a dynamic router and automatically add routes for site subnets to its routing table.

To add static routes, see the topic titled "Add a static route" in Windows 2000 Server online Help. To configure the VPN router as a RIP router, see the topic titled "Configure RIP for IP". To configure the VPN router as an OSPF router, see the topics titled "OSPF design considerations" and "Configure OSPF" in Windows 2000 Server online Help.

### Verifying reachability from each VPN router

From each VPN router, verify that the VPN router computer can resolve names and successfully communicate with resources in the VPN router's site by using the Ping command, Internet Explorer, and making drive and printer connections to known servers within the site.

### Configuring routing for off-subnet address pools

If you configured any of the VPN routers with a static address pool and any of the ranges within the pool are an off-subnet range, you must ensure that the route(s) representing the off-subnet address range(s) are present in your site routing infrastructure to reach the virtual interfaces of calling routers. You can ensure this by adding static route(s) representing the off-subnet address range(s) as static routes to the neighboring router(s) of the VPN router(s) and then using the routing protocol of your site to propagate the route to other routers. When you add the static route(s), you must specify that the gateway or next hop address is the site interface of the VPN router.

Alternately, if you are using RIP or OSPF, you can configure the VPN routers using off-subnet address pools as RIP or OSPF routers. For OSPF, you must configure the VPN router as an autonomous system boundary router (ASBR). For more information, see the topic titled "OSPF design considerations" in Windows 2000 Help.

### Deploying intersite network infrastructure

Deploying the intersite network infrastructure consists of configuring each VPN router with the set of routes for subnets that are available in the other sites (across each router-to-router VPN connection). This can be done in the following ways:

- Manually configure static routes on each VPN router.
- Perform auto-static updates on each VPN router.
- Configure routing protocols to operate over the router-to-router VPN connection.

### Manually configuring static routes on each VPN router

From the Routing and Remote Access snap-in, perform the following steps:

1. In the console tree, click **IP Routing**, and then click **Static Routes**.
2. Right-click **Static Routes**, and then click **New Static Route**.
3. In the **Static Route** dialog box, select the appropriate demand-dial interface name, and type the destination, network mask, and metric.
4. Click **OK** to add the route.
5. For an additional route, go back to step 2.

---

**Note:** Because the demand-dial connection is a point-to-point connection, the **Gateway IP address** field is not configurable.

---

### Performing auto-static updates on each VPN router

If RIP for IP is enabled on the demand-dial interfaces of both VPN routers, you can use auto-static updates to automatically configure static routes when the VPN connection is in a connected state. A demand-dial interface that

is configured for auto-static updates sends a request across an active connection to request all of the routes of the router on the other side of the connection. In response to the request, all of the routes of the requested router are automatically entered as static routes in the routing table of the requesting router.

From the Routing and Remote Access snap-in on a VPN router (assuming the router-to-router VPN connection is active), perform the following steps:

1. In the console tree, click **IP Routing**, and then click **General**.
2. In the details pane, right-click the appropriate demand-dial interface, and then click **Update Routes**.

You can also use the **netsh interface set interface** command to perform an auto-static update. For more information, see the topic titled "Scheduling auto-static updates" in Windows 2000 Server online Help.

### **Configuring routing protocols**

If the router-to-router VPN connection is persistent (always active), you can also configure IP routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) to operate over the VPN connection. For more information, see the topics titled "Setting up a RIP-for-IP routed internetwork" and "Setting up an OSPF routed internetwork" in Windows 2000 Server online Help.

---

## Deploying an L2TP-based Router-to-Router VPN Connection

The deployment of L2TP-based router-to-router VPN connections using Windows 2000 consists of the following:

- Deploy certificate infrastructure
- Deploy Internet infrastructure
- Deploy the answering router
- Deploy the calling router
- Deploy AAA infrastructure
- Deploy site network infrastructure
- Deploy intersite network infrastructure

### Deploying certificate infrastructure

For L2TP-based VPN connections, a certificate infrastructure is required to issue certificates needed to perform IPSec authentication. Additionally, a certificate infrastructure is also needed when you are using EAP-TLS authentication.

### Certificates for L2TP connections

To install a computer certificate, a certification authority must be present to issue certificates. If the CA is a Windows 2000 CA, you can install a certificate in the computer certificate store of the VPN router in the following different ways:

1. By configuring the automatic allocation of computer certificates to computers in a Windows 2000 domain. This method allows a single point of configuration for the entire domain. All members of the domain automatically receive a computer certificate through group policy.
2. By using the Certificate Manager snap-in to request a certificate to store in the Certificates (Local Computer)\Personal folder. In this method, each computer must separately request a computer certificate from the CA. You must have administrator permissions to install a certificate using the Certificate Manager snap-in.
3. By using Internet Explorer and web enrollment to request a certificate and store it in local machine store. In this method, each computer must separately request a computer certificate from the CA. You must have administrator permissions to install a certificate using Web enrollment.

Based on the certificate policies in your organization, you only need to perform one of these methods.

For more information about using the Windows 2000 CA to obtain computer certificates, see the topics titled "Machine certificates for L2TP over IPSec VPN connections" and "Submit an advanced certificate request via the Web" in Windows 2000 Server online Help.

For a third-party CA, see the documentation for the CA software for instructions about how to create a certificate and export it so that it can be imported into the computer certificate store using the Certificate Manager snap-in by an administrator on the calling and answering routers. Additionally, the root CA certificate, the certificate of the issuing CA, and the certificates of any intermediate CAs must be exported and imported on the calling and answering routers.

## Certificates for EAP-TLS authentication

To use EAP-TLS authentication of router-to-router VPN connections, you must:

- Install a user certificate on each calling router computer.
- Configure EAP-TLS on the calling router.
- Install a computer certificate on the authenticating server (the answering router or the RADIUS server)
- Configure EAP-TLS on the answering router and remote access policy.

### Installing a user certificate on a calling router

If you are using a Windows 2000 CA, a Router (Offline Request) certificate (a special type of user certificate for demand-dial connections), is created and mapped to an Active Directory user account. To deploy a Router (Offline Request) certificates for a calling router, the network administrator must:

1. Configure the Windows 2000 CA to issue Router (Offline Request) certificates.
2. Request a Router (Offline Request) certificate.
3. Export the Router (Offline Request) certificate.
4. Map the certificate to the appropriate user account.
5. Send the Router (Offline Request) certificate to the network administrator of the calling router.
6. Import the Router (Offline Request) certificate on the calling router.

For more information about deploying Router (Offline Request) certificates for demand-dial routing, see the topic titled "Branch office demand-dial connection" in Windows 2000 Server online Help.

For a third-party CA, see the documentation for the CA software for instructions about how to create a user certificate with the Client Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.2") and export it so that it can be mapped to an Active Directory user account and sent to the network administrator of the calling router. You must also export the root CA certificate, the certificate of the issuing CA, and the certificates of any intermediate CAs and import them to the proper folder of the computer certificate store of the answering router using the Certificate Manager snap-in.

### Configuring EAP-TLS on the calling router

To configure EAP-TLS for user certificates on the calling router:

- The demand-dial interface must be configured to use EAP with the **Smart Card or other certificate** EAP type by configuring advanced settings on the **Security** tab on the properties of a demand-dial interface. In the properties of the **Smart Card or other certificate** EAP type, select **Use a certificate on this computer**. If you want to validate the computer certificate of the VPN or IAS server, select **Validate server certificate**. If you want to ensure that the server's DNS name ends in a specific string, select **Connect only if server name ends with** and type the string. To require the server's computer certificate to have been issued a certificate from a specific trusted root CA, select the CA in **Trusted root certificate authority**.
- Right-click the demand-dial interface and click **Credentials**. In the **Connect** dialog box, select the proper user or Router (Offline Request) certificate in **User name on certificate**, and then click **OK**.

### Installing a computer certificate on the authenticating server

If the authenticating server is the answering router, you can use the same computer certificate that is installed to authenticate L2TP connections for EAP-TLS authentication provided it contains the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1"). If not, you must install an additional computer certificate that contains the Server Authentication certificate purpose. If the authenticating server is an IAS server, you must install a computer certificate that contains the Server Authentication certificate purpose.

If the CA is a Windows 2000 CA and the authenticating server is either the answering router or a Windows 2000 Internet Authentication Service (IAS) RADIUS server, you can install a certificate in the computer certificate store of the authenticating server using the methods described in the "Certificates for L2TP connections" section of this paper.

For a third-party CA, see the documentation for the CA software for instructions about how to create a certificate with the Server Authentication certificate purpose (OID "1.3.6.1.5.5.7.3.1") and export it so that it can be imported using the Certificate Manager snap-in by an administrator on the answering router. Additionally, the root CA certificate, the certificate of the issuing CA, and the certificates of any intermediate CAs must be exported and imported on the calling router.

### Configuring EAP-TLS on the answering router and remote access policy

To configure EAP-TLS authentication on the answering router:

- EAP must be enabled as an authentication type on the **Authentication Methods** dialog box available from the **Security** tab in the properties of the answering router in the Routing and Remote Access snap-in.

To configure EAP-TLS authentication on the remote access policy of the answering router or IAS server:

- On the remote access policy that is being used for router-to-router VPN connections, EAP must be enabled with the **Smart Card or other certificate** EAP type selected on the **Authentication** tab on the policy's profile settings. If the computer on which the remote access policy is being configured has multiple computer certificates installed, configure the properties of the **Smart Card or other certificate** EAP type and select the appropriate computer certificate to submit during the EAP-TLS authentication process.

If you are using a third-party RADIUS server, see the RADIUS server documentation for information on how to enable EAP-TLS and configure EAP-TLS to use the correct computer certificate.

### Deploying Internet infrastructure

Deploying the Internet infrastructure for router-to-router VPN connections consists of the following:

- Place VPN routers in the perimeter network or on the Internet.
- Install Windows 2000 Server on VPN router computers and configure Internet interfaces.

### Placing VPN routers in perimeter network or on the Internet

Decide where to place the VPN routers in relation to your Internet firewall. In the most common configuration, the VPN routers are placed behind the firewall on the perimeter network between your site and the Internet. If so, configure packet filters on the firewall to allow L2TP/IPSec traffic to and from the IP address of the VPN routers' perimeter network interfaces. For more information, see Appendix A.

## Installing Windows 2000 Server on VPN routers and configuring Internet interfaces

Install Windows 2000 Server on VPN router computers and connect it to either the Internet or to perimeter network with one network adapter and connect it to the site with another network adapter. Without running the Routing and Remote Access Server Setup Wizard, the VPN router computer will not forward IP packets between the Internet and the site. For the connection connected to the Internet or the perimeter network, configure the TCP/IP protocol with a public IP address, a subnet mask, and the default gateway of either the firewall (if the router is connected to a perimeter network) or an ISP router (if the router is directly connected to the Internet). Do not configure the connection with DNS server or WINS server IP addresses.

### Deploying the answering router

Deploying the answering router for a router-to-router VPN connection consists of the following:

- Configure the answering router's connection to the site.
- Run the Routing and Remote Access Server Setup Wizard.
- Configure a demand-dial interface.

### Configuring the answering router's connection to the site

Configure the connection connected to the site with a manual TCP/IP configuration consisting of IP address, subnet mask, site DNS servers, and site WINS servers. Note that you must not configure the default gateway on the site connection to prevent default route conflicts with the default route pointing to the Internet.

### Running the Routing and Remote Access Server Setup Wizard

Run the Routing and Remote Access Server Setup Wizard to configure the Windows 2000 answering router using the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click your server name, and then click **Configure and Enable Routing and Remote Access**.
3. In **Common Configurations**, click **Virtual Private Network (VPN) server** and then click **Next**. If you want to use the answering router computer as a network address translator (NAT), Web server, or other function, see Appendix B.
4. In **Remote Client Protocols**, verify that all data protocols that you want to route over router-to-router VPN connections are present. By default, all of the protocols that can be used with a remote access or router-to-router VPN connection are listed. Click **Next**.
5. In **Internet Connection**, click the connection that corresponds to the interface connected to the Internet or your perimeter network, and then click **Next**.
6. In **IP Address Assignment**, click **Automatic** if the answering router should use DHCP to obtain IP addresses for calling routers. Or, click **From a specified range of addresses** to use one or more static ranges of addresses. If any of the static address ranges is an off-subnet address range, routes must be added to the routing infrastructure in order for the virtual interfaces of calling routers to be reachable. When IP address assignment is complete, click **Next**.
7. In **Managing Multiple Remote Access Servers**, if you are using RADIUS for authentication and authorization, click **Yes, I want to use a RADIUS server**, and then click **Next**.
  - In **RADIUS Server Selection**, configure the primary (mandatory) and secondary (optional) RADIUS servers and the shared secret, and then click **Next**.

8. Click **Finish**.
9. Start the Routing and Remote Access service when prompted.

By default, only 128 L2TP ports are configured on the WAN Miniport (L2TP) device. If you need more L2TP ports, configure the **WAN Miniport (L2TP)** device from the properties of the **Ports** object in the Routing and Remote Access snap-in.

By default, only the MS-CHAP and MS-CHAP v2 protocols are enabled. If you are using user certificates for authentication, select **Extensible Authentication Protocol (EAP)** check box from the **Authentication Methods** dialog box available from the **Security** tab on the properties of the answering router computer in the Routing and Remote Access snap-in.

### Configuring a demand-dial interface

From the Routing and Remote Access snap-in on the answering router, perform the following steps:

1. In the console tree, right-click **Routing Interfaces**, and then click **New Demand-dial Interface**.
2. In the **Welcome to the Demand-Dial Interface Wizard** dialog box, click **Next**.
3. In the **Interface Name** dialog box, type the name of the demand-dial interface, and then click **Next**.
4. In the **Connection Type** dialog box, click **Connect using virtual private networking (VPN)**, and then click **Next**.
5. In the **VPN Type** dialog box, click **Layer 2 Tunneling Protocol (L2TP)**, and then click **Next**.
6. In the **Destination Address** dialog box, type the IP address of the calling router.

For a two-way-initiated router-to-router VPN connection, configure the IP address of the calling router. For a one-way initiated router-to-router VPN connection, you can skip this step because the answering router never uses this interface to initiate a connection to the calling router.

7. In the **Protocols and Security** dialog box, select the **Route IP packets on this interface**, **Route IPX packets on this interface** (if needed), and **Add a user account so that a remote router can dial in** check boxes, and then click **Next**.
8. In the **Dial In Credentials** dialog box, type the password of the user account used by the calling router in **Password** and **Confirm password**, and then click **Next**. This step automatically creates a user account with the same name as the demand-dial interface that is being created. This is done so that when the calling router initiates a connection to the answering router, it is using a user account name that matches the name of a demand-dial interface. Therefore, the answering router can determine that the incoming connection from the calling router is a demand-dial connection rather than a remote access connection.
9. In the **Dial Out Credentials** dialog box, type the user name in **User name**, the user account domain name in **Domain**, and the user account password in both **Password** and **Confirm password**.

For a two-way-initiated router-to-router VPN connection, configure the name, domain, and password when this router is acting as the calling router. For a one-way initiated router-to-router VPN connection, you can type any name in **User name** and skip the rest of the fields because this router never uses this interface to initiate a connection to the calling router.

10. In the **Completing the demand-dial interface wizard** dialog box, click **Finish**.

The result of this configuration is a L2TP-based demand-dial interface over which IP routing is enabled. A user account with the same name as the demand-dial interface is automatically added with correct account and dial-in settings.

## Deploying the calling router

Deploying the calling router for a router-to-router VPN connection consists of the following:

- Configure the calling router's connection to the site.
- Run the Routing and Remote Access Server Setup Wizard.
- Configure a demand-dial interface.

### Configuring the calling router's connection to the site

Configure the connection connected to the site with a manual TCP/IP configuration consisting of IP address, subnet mask, site DNS servers, and site WINS servers. Note that you must not configure the default gateway on the site connection to prevent default route conflicts with the default route pointing to the Internet.

### Running the Routing and Remote Access Server Setup Wizard

Run the Routing and Remote Access Server Setup Wizard to configure the Windows 2000 calling router using the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click your server name, and then click **Configure and Enable Routing and Remote Access**.
3. In **Common Configurations**, click **Virtual Private Network (VPN) server** and then click **Next**. If you want to use the calling router computer as a network address translator (NAT), Web server, or other function, see Appendix B.
4. In **Remote Client Protocols**, verify that all data protocols that you want to route over router-to-router VPN connections are present. By default, all of the protocols that can be used with a remote access or router-to-router VPN connection are listed. Click **Next**.
5. In **Internet Connection**, click the connection that corresponds to the interface connected to the Internet or your perimeter network, and then click **Next**.
6. In **IP Address Assignment**, click **Automatic** if the calling router should use DHCP to obtain IP addresses for other calling routers when it is acting as an answering router. Or, click **From a specified range of addresses** to use one or more static ranges of addresses. If any of the static address ranges is an off-subnet address range, routes must be added to the routing infrastructure in order for the virtual interfaces of routers calling this router to be reachable. When IP address assignment is complete, click **Next**.
7. In **Managing Multiple Remote Access Servers**, if you are using RADIUS for authentication and authorization, click **Yes, I want to use a RADIUS server**, and then click **Next**.
  - In **RADIUS Server Selection**, configure the primary (mandatory) and secondary (optional) RADIUS servers and the shared secret, and then click **Next**.
8. Click **Finish**.
9. Start the Routing and Remote Access service when prompted.

By default, only 128 L2TP ports are configured on the WAN Miniport (L2TP) device. If you need more L2TP ports, configure the **WAN Miniport (L2TP)** device from the properties of the **Ports** object in the Routing and Remote

Access snap-in.

By default, only the MS-CHAP and MS-CHAPv2 protocols are enabled. If you are using user certificates for authentication, select **Extensible Authentication Protocol (EAP)** check box from the **Authentication Methods** dialog box available from the **Security** tab on the properties of this router computer in the Routing and Remote Access snap-in.

### Configuring a demand-dial interface

From the Routing and Remote Access snap-in on the calling router, perform the following steps:

1. In the console tree, right-click **Routing Interfaces**, and then click **New Demand-dial Interface**.
2. In the **Welcome to the Demand-Dial Interface Wizard** dialog box, click **Next**.
3. In the **Interface Name** dialog box, type the name of the demand-dial interface. For a two-way initiated connection, this is the same name as the user name in the user credentials used by the answering router when it is acting as a calling router. Click **Next**.
4. In the **Connection Type** dialog box, click **Connect using virtual private networking (VPN)**, and then click **Next**.
5. In the **VPN Type** dialog box, click **Layer 2 Tunneling Protocol (L2TP)**, and then click **Next**.
6. In the **Destination Address** dialog box, type the IP address of the answering router.
7. In the **Protocols and Security** dialog box, select the **Route IP packets on this interface**, **Route IPX packets on this interface** (if needed) check boxes. For a two-way initiated connection, select the **Add a user account so that a remote router can dial in** check box. Click **Next**.
8. For a two-way initiated connection, in the **Dial In Credentials** dialog box, type the password of the user account used by the answering router acting as a calling router in **Password** and **Confirm password**, and then click **Next**. This step automatically creates a user account with the same name as the demand-dial interface that is being created. This is done so that when the answering router acting as a calling router initiates a connection to this router, it is using a user account name that matches the name of a demand-dial interface. Therefore, this router can determine that the incoming connection from the answering router acting as a calling router is a demand-dial connection rather than a remote access connection.
9. In the **Dial Out Credentials** dialog box, type the user name in **User name**, the user account domain name in **Domain**, and the user account password in both **Password** and **Confirm password**.
10. In the **Completing the demand-dial interface wizard** dialog box, click **Finish**.

The result of this configuration is a L2TP-based demand-dial interface over which IP routing is enabled. A user account with the same name as the demand-dial interface is automatically added with correct account and dial-in settings.

### Deploying AAA infrastructure

Deploying the AAA infrastructure for router-to-router VPN connections consists of the following:

- Configure Active Directory for user accounts and groups.
- Configure the primary IAS server on a domain controller.

- Configure the secondary IAS server on a different domain controller.

This configuration must be done at each site containing an answering router. For branch offices with few computers and a single answering router, it is easier to configure the Routing and Remote Access service for Windows authentication and use locally configured remote access policies than configuring a separate IAS server computer.

### **Configuring Active Directory for user accounts and groups**

To configure Active Directory for user accounts and groups, do the following:

1. Ensure that all calling routers have a corresponding user account with the correct account and dial-in settings. This includes calling routers for branch offices and business partners. User accounts with the correct account and dial-in settings are automatically created when you select the **Add a user account so that a remote router can dial in** check box on the **Protocols and Security** dialog box in the Demand-Dial Interface Wizard.
2. Organize user accounts used by calling routers into the appropriate universal and nested groups to take advantage of group-based remote access policies. For more information, see the topic titled "Universal, global, and domain local groups" in Windows 2000 Server online Help.

### **Configuring the primary IAS server on a domain controller**

To configure the primary IAS server on a domain controller, do the following:

1. On the domain controller, install IAS as an optional networking component. For more information, see the topic titled "Install IAS" in Windows 2000 Server online Help.
2. Configure the IAS server computer (the domain controller) to read the properties of user accounts in the domain. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help.
3. If the IAS server authenticates connection attempts for user accounts in other domains, verify that these domains have a two-way trust with the domain in which the IAS server computer is a member. Next, configure the IAS server computer to read the properties of user accounts in other domains. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help. For more information about trust relationships, see the topic titled "Understanding domain trusts" in Windows 2000 Server online Help.

If the IAS server authenticates connection attempts for user accounts in other domains, and those domains do not have a two-way trust with the domain in which the IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains.

4. Enable file logging for accounting and authentication events. For more information, see the topic titled "Configure log file properties" in Windows 2000 Server online Help.
5. Add the VPN router(s) as RADIUS clients of the IAS server. For more information, see the topic titled "Add RADIUS clients" in Windows 2000 Server online Help. For the IP address of each VPN router, use the site IP address assigned to the VPN router. If you are using names, use the internal name of the VPN router. Use strong shared secrets.
6. Create remote access policies that reflect your remote access usage scenarios. For example, to configure a remote access policy that requires L2TP-based router-to-router VPN connections for members of the VPNRouters group to use MS-CHAP v2 authentication and 128-bit encryption, create a remote access policy with the following settings:

Policy name: Router-to-router VPN connections

Conditions:

**NAS-Port-Type** matches **Virtual (VPN)**

**Tunnel-Type** matches **Layer Two Tunneling Protocol**

**Windows-Groups** matches **VPN Routers** (example)

Permission: **Grant remote access permission**

Profile settings, **Authentication** tab:

Select **Microsoft Encrypted Authentication (MS-CHAP v2)**. Clear all other check boxes.

Profile settings, **Encryption** tab:

Select the **Strongest** check box, and then clear all other check boxes.

7. If you have created new remote access policies, either delete the default remote access policy named **Allow access if dial-up permission is enabled**, or move it so that it is the last policy to be evaluated. For more information, see the topics titled "Delete a remote access policy" and "Change the policy evaluation order" in Windows 2000 Server online Help.

---

**Note:** The **Strongest** encryption strength is only available after installing either the Windows 2000 High Encryption Pack or Windows 2000 Service Pack 2 (or later) on the IAS server computer.

---

### Configuring the secondary IAS server on a different domain controller

To configure the secondary IAS server on a different domain controller, do the following:

1. On the other domain controller, install IAS as an optional networking component. For more information, see the topic titled "Install IAS" in Windows 2000 Server online Help.
2. Configure the secondary IAS server computer (the other domain controller) to read the properties of user accounts in the domain. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help.
3. If the secondary IAS server authenticates connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the secondary IAS server computer is a member. Next, configure the secondary IAS server computer to read the properties of user accounts in other domains. For more information, see the topic titled "Enable the IAS server to read user objects in Active Directory" in Windows 2000 Server online Help. For more information about trust relationships, see the topic titled "Understanding domain trusts" in Windows 2000 Server online Help.  
If the secondary IAS server authenticates connection attempts for user accounts in other domains, and those domains do not have a two-way trust with the domain in which the secondary IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains.
4. To copy the configuration of the primary IAS server to the secondary IAS server, type **netsh aaa show config > path\file.txt** at a command prompt on the primary IAS server. This stores the configuration settings, including registry settings, in a text file. The path can be relative, absolute, or a network path.
5. Copy the file created in step 4 to the secondary IAS server. At a command prompt on the secondary IAS

server, type **netsh exec path\file.txt**. This imports all the settings configured on the primary IAS server to the secondary IAS server.

#### Deploying site network infrastructure

Deploying the network infrastructure of a site for router-to-router VPN connections consists of the following:

- Configure routing on the VPN routers.
- Verify reachability from each VPN router.
- Configure routing for off-subnet address pools.

#### **Configuring routing on the VPN routers**

In order for your VPN routers to properly forward traffic to locations within the site in which they are located, you must configure them with either static routes that summarize all the possible addresses used on in the site or with routing protocols so that the VPN router can participate as a dynamic router and automatically add routes for site subnets to its routing table.

To add static routes, see the topic titled "Add a static route" in Windows 2000 Server online Help. To configure the VPN router as a RIP router, see the topic titled "Configure RIP for IP". To configure the VPN router as an OSPF router, see the topics titled "OSPF design considerations" and "Configure OSPF" in Windows 2000 Server online Help.

#### **Verifying reachability from each VPN router**

From each VPN router, verify that the VPN router computer can resolve names and successfully communicate with resources in the VPN router's site by using the Ping command, Internet Explorer, and making drive and printer connections to known servers within the site.

#### **Configuring routing for off-subnet address pools**

If you configured any of the VPN routers with a static address pool and any of the ranges within the pool are an off-subnet range, you must ensure that the route(s) representing the off-subnet address range(s) are present in your site routing infrastructure to reach the virtual interfaces of calling routers. You can ensure this by adding static route(s) representing the off-subnet address range(s) as static routes to the neighboring router(s) of the VPN router(s) and then using the routing protocol of your site to propagate the route to other routers. When you add the static route(s), you must specify that the gateway or next hop address is the site interface of the VPN router.

Alternately, if you are using RIP or OSPF, you can configure the VPN routers using off-subnet address pools as RIP or OSPF routers. For OSPF, you must configure the VPN router as an autonomous system boundary router (ASBR). For more information, see the topic titled "OSPF design considerations" in Windows 2000 Help.

#### Deploying intersite network infrastructure

Deploying the intersite network infrastructure consists of configuring each VPN router with the set of routes for subnets that are available in the other sites (across each router-to-router VPN connection). This can be done in the following ways:

- Manually configure static routes on each VPN router.
- Perform auto-static updates on each VPN router.

- Configure routing protocols to operate over the router-to-router VPN connection.

#### **Manually configuring static routes on each VPN router**

From the Routing and Remote Access snap-in, perform the following steps:

1. In the console tree, click **IP Routing**, and then click **Static Routes**.
2. Right-click **Static Routes**, and then click **New Static Route**.
3. In the **Static Route** dialog box, select the appropriate demand-dial interface name, and type the destination, network mask, and metric.
4. Click **OK** to add the route.
5. For an additional route, go back to step 2.

---

**Note:** Because the demand-dial connection is a point-to-point connection, the **Gateway IP address** field is not configurable.

---

#### **Performing auto-static updates on each VPN router**

If RIP for IP is enabled on the demand-dial interfaces of both VPN routers, you can use auto-static updates to automatically configure static routes when the VPN connection is in a connected state. A demand-dial interface that is configured for auto-static updates sends a request across an active connection to request all of the routes of the router on the other side of the connection. In response to the request, all of the routes of the requested router are automatically entered as static routes in the routing table of the requesting router.

From the Routing and Remote Access snap-in on a VPN router (assuming the router-to-router VPN connection is active), perform the following steps:

1. In the console tree, click **IP Routing**, and then click **General**.
2. In the details pane, right-click the appropriate demand-dial interface, and then click **Update Routes**.

You can also use the **netsh** commands to perform an auto-static update. For more information, see the topic "Scheduling auto-static updates" in Windows 2000 Server online Help.

#### **Configuring routing protocols**

If the router-to-router VPN connection is persistent (always active), you can also configure IP routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) to operate over the VPN connection. For more information, see the topics titled "Setting up a RIP-for-IP routed internetwork" and "Setting up an OSPF routed internetwork" in Windows 2000 Server online Help.

---

## Appendix A: Configuring Firewalls with a Windows 2000 VPN Router

The following are common configurations of firewalls with a VPN router:

- The VPN router is attached to the Internet and the firewall is between the VPN router and the site.
- The firewall is attached to the Internet and the VPN router is between the firewall and the site.
- Two firewalls are used—one between the VPN router and the site and one between the VPN router and the Internet.

### VPN router in front of the firewall

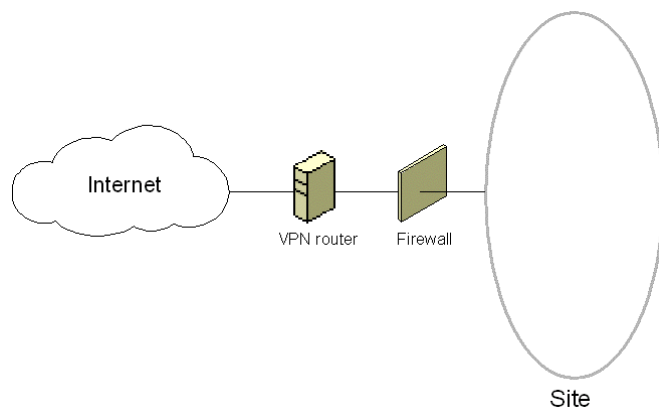
To secure the VPN router from sending or receiving any traffic on its Internet interface except VPN traffic, you need to configure PPTP or L2TP/IPSec input and output filters on the interface that corresponds to the connection to the Internet. Because IP routing is enabled on the Internet interface, if PPTP or L2TP/IPSec filters are not configured on the Internet interface, then any traffic received on the Internet interface is routed, which may forward unwanted Internet traffic to your site.

When the VPN router is in front of the firewall attached to the Internet, you need to add packet filters to the Internet interface that allow only VPN traffic to and from the IP address of the VPN router's Internet interface.

For inbound traffic, when the tunneled data is decrypted by the VPN router, it is forwarded to the firewall. The firewall in this configuration is acting as a filter for site traffic and can prevent specific resources from being accessed, scan data for viruses, perform intrusion detection, and other functions.

Because the only Internet traffic allowed on the site must pass through the VPN router, this approach also prevents the sharing of File Transfer Protocol (FTP) or Web site resources with non-VPN Internet users.

Figure 3 shows the VPN router in front of the firewall.



*Figure 3 The VPN router in front of the firewall*

The firewall is configured for the appropriate rules for site traffic to and from hosts in other sites according to your network security policies.

For the Internet interface on the VPN router, configure the following input and output filters using the Routing and

Remote Access snap-in.

### Packet Filters for PPTP

Configure the following input filters with the filter action set to **Drop all packets except those that meet the criteria below**:

- Destination IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and TCP destination port of 1723.  
This filter allows PPTP tunnel maintenance traffic to the VPN router.
- Destination IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and IP Protocol ID of 47.  
This filter allows PPTP tunneled data to the VPN router.
- Destination IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and TCP [established] source port of 1723.  
This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection. With the TCP [established] filter, traffic is accepted only when the VPN router initiated the TCP connection.

Configure the following output filters with the filter action set to **Drop all packets except those that meet the criteria below**:

- Source IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and TCP source port of 1723.  
This filter allows PPTP tunnel maintenance traffic from the VPN router.
- Source IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and IP Protocol ID of 47.  
This filter allows PPTP tunneled data from the VPN router.
- Source IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and TCP destination port of 1723.  
This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection.

### Packet Filters for L2TP/IPSec

Configure the following input filters with the filter action set to **Drop all packets except those that meet the criteria below**:

- Destination IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and UDP destination port of 500.  
This filter allows Internet Key Exchange (IKE) traffic to the VPN router.
- Destination IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and UDP destination port of 1701.  
This filter allows L2TP traffic to the VPN router.

Configure the following output filters with the filter action set to **Drop all packets except those that meet the criteria below**:

- Source IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and UDP source port of 500.  
This filter allows IKE traffic from the VPN router.
- Source IP address of the VPN router's Internet interface, subnet mask of 255.255.255.255, and UDP source port of 1701.  
This filter allows L2TP traffic from the VPN router.

There are no filters required for IPSec Encapsulating Security Protocol (ESP) traffic for the IP protocol of 50. The Routing and Remote Access service filters are applied after the IPSec components remove the ESP header.

### VPN router behind the firewall

In a more common configuration, the firewall is connected to the Internet and the VPN router is an site resource that is connected to the perimeter network, also known as a demilitarized zone (DMZ) or screened subnet. The perimeter network is an IP network segment that contains resources that are available to Internet users, such as Web and FTP servers. The VPN router has an interface on both the perimeter network and the site. In this approach, the firewall must be configured with input and output filters on its Internet interface that allow the passing of tunnel maintenance traffic and tunneled data to the VPN router. Additional filters can allow the passing of traffic to Web, FTP, and other types of servers on the perimeter network. For an added layer of security, the VPN router can also be configured with PPTP or L2TP/IPSec packet filters on its perimeter network interface.

The firewall in this configuration is acting as a filter for Internet traffic and can confine the incoming and outgoing traffic to the specific resources on the perimeter network, perform intrusion attempt detection, prevent denial of service attacks, and other functions.

Because the firewall does not have the encryption keys for each VPN connection, it can only filter on the plaintext headers of the tunneled data. In other words, all tunneled data passes through the firewall. This is not a security concern, however, because the VPN connection requires an authentication process that prevents unauthorized access beyond the VPN router.

Figure 4 shows the VPN router behind the firewall on the perimeter network.

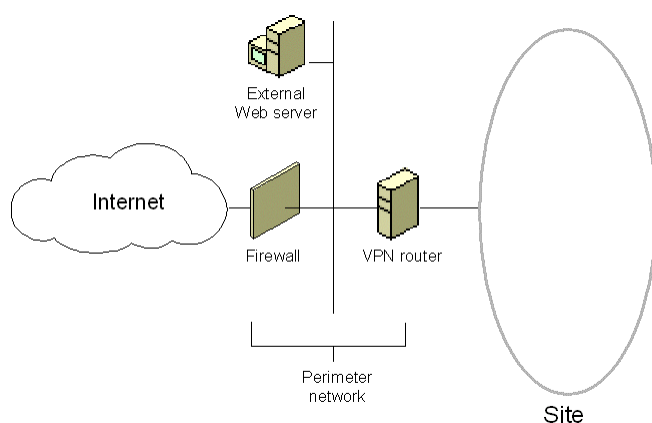


Figure 4 The VPN router behind the firewall on the perimeter network

For both the Internet and network perimeter interfaces on the firewall, configure the following input and output filters

using the firewall's configuration software.

### **Packet Filters for PPTP**

Separate input and output packet filters can be configured on the Internet interface and the perimeter network interface.

#### **Filters on the Internet Interface**

Configure the following input packet filters on the Internet interface of the firewall to allow the following types of traffic:

- Destination IP address of the VPN router's perimeter network interface and TCP destination port of 1723 (0x6BB).  
This filter allows PPTP tunnel maintenance traffic to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and IP Protocol ID of 47 (0x2F).  
This filter allows PPTP tunneled data to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and TCP source port of 1723 (0x6BB).  
This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection. This filter should only be used in conjunction with PPTP packet filters described in "VPN router in front of the firewall" and configured on the VPN router's network perimeter interface. By allowing all traffic to the VPN router from TCP port 1723, there exists the possibility of network attacks from sources on the Internet that use this port.

Configure the following output filters on the Internet interface of the firewall to allow the following types of traffic:

- Source IP address of the VPN router's perimeter network interface and TCP source port of 1723 (0x6BB).  
This filter allows PPTP tunnel maintenance traffic from the VPN router.
- Source IP address of the VPN router's perimeter network interface and IP Protocol ID of 47 (0x2F).  
This filter allows PPTP tunneled data from the VPN router.
- Source IP address of the VPN router's perimeter network interface and TCP destination port of 1723 (0x6BB).  
This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection. This filter should only be used in conjunction with PPTP packet filters described in "VPN router in front of the firewall" and configured on the VPN router's network perimeter interface. By allowing all traffic from the VPN router to TCP port 1723, there exists the possibility of network attacks from sources on the Internet using this port.

#### **Filters on the Perimeter Network Interface**

Configure the following input filters on the perimeter network interface of the firewall to allow the following types of traffic:

- Source IP address of the VPN router's perimeter network interface and TCP source port of 1723 (0x6BB).  
This filter allows PPTP tunnel maintenance traffic from the VPN router.
- Source IP address of the VPN router's perimeter network interface and IP Protocol ID of 47 (0x2F).

This filter allows PPTP tunneled data from the VPN router.

- Source IP address of the VPN router's perimeter network interface and TCP destination port of 1723 (0x6BB).

This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection. This filter should only be used in conjunction with PPTP packet filters described in "VPN router in front of the firewall" and configured on the VPN router's network perimeter interface. By allowing all traffic from the VPN router to TCP port 1723, there exists the possibility of network attacks from sources on the Internet using this port.

Configure the following output packet filters on the perimeter network interface of the firewall to allow the following types of traffic:

- Destination IP address of the VPN router's perimeter network interface and TCP destination port of 1723 (0x6BB).  
This filter allows PPTP tunnel maintenance traffic to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and IP Protocol ID of 47 (0x2F).  
This filter allows PPTP tunneled data to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and TCP source port of 1723 (0x6BB).  
This filter is required only when the VPN router is acting as a calling router in a router-to-router VPN connection. This filter should only be used in conjunction with PPTP packet filters described in "VPN router in front of the firewall" and configured on the VPN router's network perimeter interface. By allowing all traffic to the VPN router from TCP port 1723, there exists the possibility of network attacks from sources on the Internet using this port.

### **Packet Filters for L2TP/IPSec**

Separate input and output packet filters can be configured on the Internet interface and the perimeter network interface.

#### **Filters on the Internet Interface**

Configure the following input packet filters on the Internet interface of the firewall to allow the following types of traffic:

- Destination IP address of the VPN router's perimeter network interface and UDP destination port of 500 (0x1F4).  
This filter allows IKE traffic to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and IP Protocol ID of 50 (0x32).  
This filter allows IPSec ESP traffic to the VPN router.

Configure the following output packet filters on the Internet interface of the firewall to allow the following types of traffic:

- Source IP address of the VPN router's perimeter network interface and UDP source port of 500 (0x1F4).  
This filter allows IKE traffic from the VPN router.
- Source IP address of the VPN router's perimeter network interface and IP Protocol ID of 50 (0x32).

This filter allows IPSec ESP traffic from the VPN router.

There are no filters required for L2TP traffic at the UDP port of 1701. All L2TP traffic at the firewall, including tunnel maintenance and tunneled data, is encrypted as an IPSec ESP payload.

### Filters on the Perimeter Network Interface

Configure the following input packet filters on the perimeter network interface of the firewall to allow the following types of traffic:

- Source IP address of the VPN router's perimeter network interface and UDP source port of 500 (0x1F4). This filter allows IKE traffic from the VPN router.
- Source IP address of the VPN router's perimeter network interface and IP Protocol ID of 50 (0x32). This filter allows IPSec ESP traffic from the VPN router.

Configure the following output packet filters on the perimeter network interface of the firewall to allow the following types of traffic:

- Destination IP address of the VPN router's perimeter network interface and UDP destination port of 500 (0x1F4). This filter allows IKE traffic to the VPN router.
- Destination IP address of the VPN router's perimeter network interface and IP Protocol ID of 50 (0x32). This filter allows IPSec ESP traffic to the VPN router.

There are no filters required for L2TP traffic at the UDP port of 1701. All L2TP traffic at the firewall, including tunnel maintenance and tunneled data, is encrypted as an IPSec ESP payload.

### VPN router between two firewalls

Another configuration is when the VPN router computer is placed on the perimeter network between two firewalls. The Internet firewall, the firewall between the Internet and the VPN router, filters all Internet traffic from all Internet clients. The site firewall, the firewall between the VPN router and the site, filters site traffic from hosts in other sites.

Figure 5 shows the VPN router between two firewalls on the perimeter network.

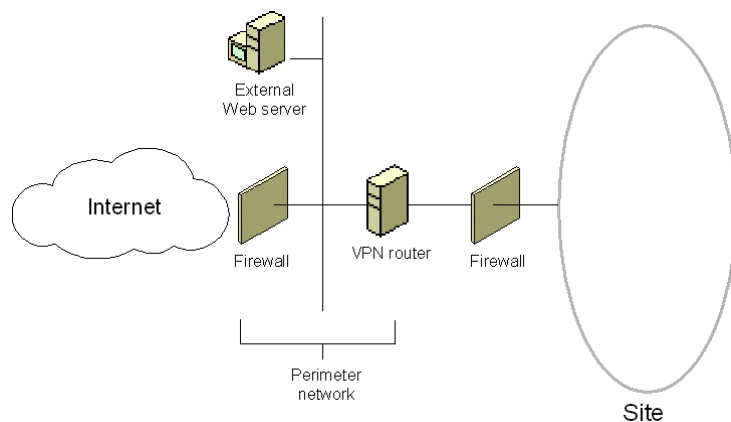


Figure 5 The VPN router between two firewalls on the perimeter network

In this configuration:

- Configure your Internet firewall and VPN router with the packet filters as described in the "VPN router behind the firewall" section.
- Configure your site firewall for the appropriate rules for site traffic to and from calling routers according to your network security policies.

---

## Appendix B: Alternate Configurations

This section provides information about common alternate configurations for a Windows 2000 VPN router. The most common configuration is described in the "Deploying an L2TP-based Router-to-Router VPN Connection " and "Deploying an L2TP-based Router-to-Router VPN Connection " sections of this paper and whose principal characteristics are the following:

- The VPN router has multiple network adapters—at least one connected to the site and at least one connected to the Internet.
- The VPN router has static public IP addresses assigned to its Internet interfaces.
- The VPN router is only acting as a security gateway providing a routed connection to the site. The VPN router is not hosting any other Internet services such as NAT or Web services.

The two other most common configurations are the following:

1. The VPN router computer is performing other functions such as network address translation or Web hosting.
2. The VPN router computer has a single network adapter and its public IP address is published by a firewall.

The following sections detail the changes to make in the deployment of a VPN router to accommodate these additional common configurations.

### Multiple Internet Function VPN Router

In this configuration, the VPN router's principal characteristics are the following:

- The VPN router has multiple network adapters—at least one connected to the site and at least one connected to the Internet.
- The VPN router has static public IP addresses assigned to its Internet interfaces.
- The VPN router is acting as a security gateway providing remote access to the site and is hosting any other Internet services such as NAT or Web hosting.

In this configuration, you can follow the procedures as described in the "Deploying PPTP-based Remote Access" and "Deploying L2TP-based Remote Access" sections of this paper except that when you run the Routing and Remote Access Server Setup Wizard, you select from the list of **Common Configurations**, do not choose **Virtual Private Network (VPN) server**. Instead, select **Network router**. You are prompted to select an interface over which DHCP, DNS, and WINS configuration is obtained, to determine how you want to assign IP addresses to remote access clients, and to configure RADIUS.

When you select **Network router**, only five PPTP and L2TP ports are configured. For additional ports, configure the properties of the **WAN Miniport (PPTP)** and **WAN Miniport (L2TP)** devices from the properties of the **Ports** object in the Routing and Remote Access snap-in.

By selecting **Network router** in the wizard, PPTP and L2TP packet filters are not configured on the Internet interface of the VPN router computer. Whether you have to manually configure these filters depends on whether the VPN router computer is also hosting NAT.

- If NAT is needed on the VPN router computer, do not configure PPTP and L2TP packet filters or packet filters for other types of traffic. If you configure PPTP and L2TP packet filters on the Internet interface, NAT cannot function. Even though you do not configure any packet filters on the Internet interface of the

VPN router computer, the function of the NAT discards any traffic from the Internet that does not correspond to traffic requested by site clients.

- If NAT is not needed on the VPN router computer, you can configure PPTP and L2TP packet filters and other types of filters for additional services hosted by the VPN router computer. For example, if the VPN router computer is also hosting a Web site, then filters should be added to allow traffic to and from the public IP address of the VPN router computer and TCP port 80.

### Single-Adapter VPN Router

In this configuration, the VPN router computer has only a single network adapter and nodes on the site of the calling router are accessing services hosted on the VPN router computer. If the VPN router computer has only a single network adapter and is configured with a public IP address, all traffic to and from the services running on the VPN router computer are sent as clear text outside the VPN tunnel. For more information about why this happens, see "Routing and multi-use VPN routers" in this paper.

The only way a single adapter VPN router can work properly is if it is behind a firewall that is providing a publishing and translation service for the VPN router. The firewall publishes or makes known on the Internet a static public IP address for the VPN router. When VPN packets are sent to this published IP address, the firewall translates the address of the packet to a private or other public address by which the VPN router is known on the site.

Figure 6 shows an example of the published and actual addresses of a VPN router in this configuration.

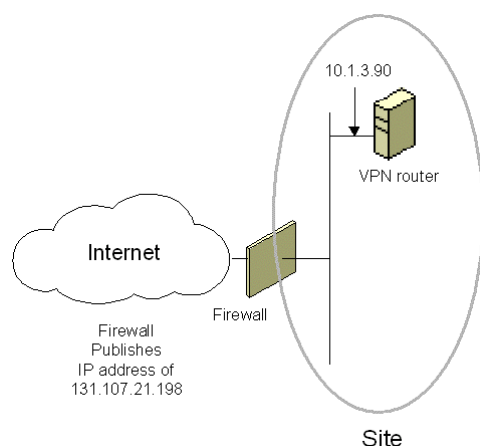


Figure 6 The single-adapter VPN router configuration

The VPN router is configured according to "Deploying a PPTP-based Router-to-Router VPN Connection" in this paper with its site interface acting as an Internet interface. The firewall is configured to:

- Publish the name and public IP address of the VPN router on the Internet.
- Translate PPTP traffic sent to the public IP address of the VPN router to the site interface of the VPN router computer.
- Discard all traffic except PPTP traffic going to and from the VPN router computer.

---

## Appendix C: Troubleshooting

### Troubleshooting tools

Windows 2000 provides the following tools to troubleshoot VPN connections:

- TCP/IP Troubleshooting Tools
- Authentication and Accounting Logging
- Unreachability reason
- Event Logging
- IAS Event Logging
- PPP Logging
- Tracing
- Network Monitor

### TCP/IP Troubleshooting Tools

The Ping, Tracert, and Pathping tools use ICMP Echo and Echo Reply messages to verify connectivity, display the path to a destination, and test path integrity. The **route print** command can be used to display the IP routing table. Alternately, you can use the **netsh routing ip show rtmroutes** command or the Routing and Remote Access snap-in.

In addition to the normal TCP/IP tools, use the Netdiag tool to test and display your network configuration.

### Authentication and Accounting Logging

A VPN router running Windows 2000 supports the logging of authentication and accounting information for VPN connections in local logging files when Windows authentication or Windows accounting is enabled. This logging is separate from the events recorded in the system event log. You can use the information that is logged to track router-to-router connection usage and authentication attempts. Authentication and accounting logging is especially useful for troubleshooting remote access policy issues. For each authentication attempt, the name of the remote access policy that either accepted or rejected the connection attempt is recorded.

Enable authentication and accounting logging from the **Settings** tab on the properties of the **Local File** object in the **Remote Access Logging** folder in the Routing and Remote Access snap-in (if the Routing and Remote Access service is configured for Windows authentication and accounting) or the Internet Authentication Service snap-in (if the Routing and Remote Access service is configured for RADIUS authentication and accounting and the RADIUS server is an IAS server)

The authentication and accounting information is stored in a configurable log file or files stored in the *SystemRoot\System32\LogFiles* folder. The log files are saved in Internet Authentication Service (IAS) or database-compatible format, meaning that any database program can read the log file directly for analysis.

If the VPN router is configured for RADIUS authentication and accounting and the RADIUS server is a computer running Windows 2000 and IAS, the authentication and accounting logs are stored in the *SystemRoot\System32\LogFiles* folder on the IAS server computer.

## Unreachability Reason

When a demand-dial interface fails to make a connection, the interface is left in an unreachable state and the Routing and Remote Access service records the reason why the connection attempt failed. To view the unreachable reason in the Routing and Remote Access snap-in, click **Routing Interfaces**. In the details pane, right-click the demand-dial interface, and then click **Unreachability Reason**.

## Event Logging

On the **Event Logging** tab in the properties of a VPN router in the Routing and Remote Access snap-in, there are four levels of logging. Select **Log the maximum amount of information**, and then try the connection again. After the connection fails, check the system event log for events logged during the connection process. After you are done viewing remote access events, select the **Log errors and warnings option** on the **Event logging** tab to conserve system resources.

## IAS Event Logging

If your VPN routers are configured for RADIUS authentication and your RADIUS servers are computers running Windows 2000 Server and IAS, check the system event log for IAS events for rejected or accepted connection attempts. IAS system event log entries contain a lot of information on the connection attempt including the name of the remote access policy that accepted or rejected the connection attempt. IAS event logging for rejected or accepted connection attempts is enabled by default and configured from the **Service** tab from the properties of an IAS server in the Internet Authentication Service snap-in.

## PPP logging

PPP logging records the series of programming functions and PPP control messages during a PPP connection and is a valuable source of information when you are troubleshooting the failure of a PPP connection. To enable PPP logging, select the **Enable Point-to-Point Protocol (PPP) logging** option on the **PPP** tab on the properties of a remote access server.

The PPP log in Windows NT 4.0 has been replaced by the tracing function. To duplicate the PPP log, you need to enable file tracing for the PPP key. By default, the PPP log is stored as the Ppp.log file in the *SystemRoot\Tracing* folder.

## Tracing

The Windows 2000 Routing and Remote Access service has an extensive tracing capability that you can use to troubleshoot complex network problems. You can enable the components in Windows 2000 Server to log tracing information to files using the Netsh command or through the registry.

### Enabling Tracing with Netsh

You can use the Netsh command to enable and disable tracing for specific components or for all components. To enable and disable tracing for a specific component, use the following syntax:

```
netsh ras set tracing Component enabled|disabled
```

where *Component* is a component in the list of Routing and Remote Access service components found in the Windows 2000 registry under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Tracing. For example, to enable

tracing for the RASAUTH component, the command is:

```
netsh ras set tracing rasauth enabled
```

To enable tracing for all components, use the following command:

```
netsh ras set tracing * enabled
```

### **Enabling Tracing through the Registry**

The tracing function can also be configured by changing settings in the Windows 2000 registry under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing
```

You can enable tracing for each Routing and Remote Access service component by setting the registry values described later. You can enable and disable tracing for components while the Routing and Remote Access service is running. Each component is capable of tracing and appears as a subkey under the preceding registry key.

To enable tracing for each component, you can configure the following registry value entries for each protocol key:

**EnableFileTracing** REG\_DWORD *Flag*

You can enable logging tracing information to a file by setting **EnableFileTracing** to 1. The default value is 0.

**FileDirectory** REG\_EXPAND\_SZ *Path*

You can change the default location of the tracing files by setting **FileDirectory** to the path you want. The file name for the log file is the name of the component for which tracing is enabled. By default, log files are placed in the *SystemRoot\Tracing* folder.

**FileTracingMask** REG\_DWORD *LevelOfTracingInformationLogged*

**FileTracingMask** determines how much tracing information is logged to the file. The default value is 0xFFFF0000.

**MaxFileSize** REG\_DWORD *SizeOfLogFile*

You can change the size of the log file by setting different values for **MaxFileSize**. The default value is 0x10000 (64K).

---

**Notes:** Tracing consumes system resources and should be used sparingly to help identify network problems. After the trace is captured or the problem is identified, you should immediately disable tracing. Do not leave tracing enabled on multiprocessor computers.

Tracing information can be complex and very detailed. Most of the time this information is useful only to Microsoft support professionals or to network administrators who are very experienced with the Routing and Remote Access service. Tracing information can be saved as files and sent to Microsoft support for analysis.

---

### **Network Monitor**

Use Network Monitor, a packet capture and analysis tool supplied with Windows 2000 Server, to capture and view the traffic sent between VPN routers during the VPN connection process and during data transfer. You cannot interpret the encrypted portions of VPN traffic with Network Monitor. Network Monitor is installed as an optional management and monitoring tool when you select Add/Remove Windows Components from Control Panel-Add/Remove Programs.

The proper interpretation of the VPN traffic with Network Monitor requires an in-depth understanding of PPP, PPTP, IPSec, and other protocols. Network Monitor captures can be saved as files and sent to Microsoft support for analysis.

### Troubleshooting router-to-router VPN connections

Router-to-router VPN problems typically fall into the following categories:

- Connection attempt is rejected when it should be accepted.
- Connection attempt is accepted when it should be rejected.
- Unable to reach locations beyond the VPN router.
- Unable to reach the virtual interfaces of VPN routers.
- On-demand connection is not made automatically.
- Unable to establish tunnel.

Use the following troubleshooting tips to isolate the configuration or infrastructure problem causing the stated VPN problem.

#### **Connection attempt is rejected when it should be accepted**

- Verify that the credentials of the calling router, consisting of user name, password, and domain name, are correct and can be validated by the answering router.
- Verify that the user account of the calling router is not locked out, expired, disabled, or that the time the connection is being made does not correspond to the configured logon hours.
- Verify that the user account of the calling router is not configured to change its password at the next logon or if the password has expired. A calling router cannot change an expired password during the connection process and the connection attempt is rejected.
- Verify that the user account has not been locked out due to remote access account lockout. For more information, see the topic titled "Account lockout" in Windows 2000 online Help.
- Verify that the Routing and Remote Access service is running on the answering router.
- Verify that the answering router is enabled for LAN and demand-dial routing from the **General** tab on the properties of a VPN router in the Routing and Remote Access snap-in.
- Verify that the **WAN Miniport (PPTP)** and **WAN Miniport (L2TP)** devices are enabled for demand-dial routing connections (inbound and outbound) from the properties of the **Ports** object in the Routing and Remote Access snap-in.
- Verify that the calling router, the answering router, and the remote access policy corresponding to router-to-router VPN connections are configured to use at least one common authentication method.
- Verify that the calling router and the remote access policy corresponding to router-to-router VPN connections are configured to use at least one common encryption strength. If the calling router is not capable of 128-bit encryption and the **Strongest** encryption level is required in the remote access policy, the connection attempt is rejected.
- Verify that the parameters of the connection are authorized through remote access policies. In order for the connection to be established, the parameters of the connection attempt must:
  - Match all of the conditions of at least one remote access policy.
  - Be granted remote access permission through the user account (set to **Allow access**), or if the user account has the **Control access through Remote Access Policy** option selected, the remote access permission of the matching remote access policy must have the **Grant remote access**

**permission** option selected.

- Match all the settings of the profile.
- Match all the settings of the dial-in properties of the user account.

To obtain the name of the remote access policy that rejected the connection attempt, scan the accounting log for the entry corresponding to the connection attempt for the policy name.

- If you are logged on using an account with domain administrator permissions when you run the Routing and Remote Access Server Setup Wizard, it automatically adds the computer account of the **RAS and IAS Servers** domain-local security group. This group membership allows the answering router computer to access user account information. If the answering router is unable to access user account information, verify that:
  - The computer account of the answering router computer is a member of the **RAS and IAS Servers** security group for all the domains that contain user accounts for which the answering router is authenticating remote access. You can use the **netsh ras show registeredserver** command at the command prompt to view the current registration. You can use the **netsh ras add registeredserver** command to register the server in a domain in which the answering router is a member or other domains. Alternately, you or your domain administrator can add the computer account of the answering router computer to the **RAS and IAS Servers** security group of all the domains that contain user accounts for which the answering router is authenticating router-to-router VPN connections.
  - If you add or remove the answering router computer to the **RAS and IAS Servers** security group, the change does not take effect immediately (due to the way that Windows 2000 caches Active Directory information). For the change to take effect immediately, you need to restart the answering router computer.
- For demand-dial connections using EAP-TLS and Router (Offline Request) certificates, verify that the calling router and answering router are correctly configured.

On the calling router, verify that EAP is configured as the authentication protocol in the **Security** properties of the demand-dial interface. Verify the settings of the properties of the **Smart Card or other Certificate (encryption enabled)** EAP type. Verify that the correct Router (Offline Request) certificate is selected when configuring the credentials of the demand-dial interface.

On the answering router, verify that EAP is enabled as an authentication protocol on the answering router and EAP-TLS is enabled on the matching remote access policy. Verify that the correct computer certificate of the authenticating server (the answering router or IAS server) is selected from the configuration settings of the **Smart Card or other Certificate** EAP type in the matching remote access policy.

Verify that the user certificate of the calling router was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the answering router trusts. Additionally, verify that the computer certificate of the answering router was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the calling router trusts.

By default, an answering router checks the certificate revocation list (CRL) when authenticating the calling router. If the CRL is locally available, it can be checked. In some configurations, the CRL cannot be checked until after the connection is made. The CRL is stored at the root CA and, optionally, in Active Directory. For a branch office router that is acting as an answering router in a site that does not contain the root CA, there are two solutions to this problem:

1. Publish the CRL in Active Directory. For more information, see the topics titled "Schedule the

publication of the certificate revocation list" or "To manually publish the certificate revocation list" in Windows 2000 online Help. Once the CRL is published in Active Directory, the local domain controller in the site will have the latest CRL after Active Directory synchronization.

2. On the branch office router, set the following registry value to 1:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\RasMan\PPP\EAP\13\IgnoreRevocationOffline

- For an answering router that is a member server in a mixed-mode or native-mode Windows 2000 domain that is configured for Windows authentication, verify that:
  - The **RAS and IAS Servers** security group exists. If not, then create the group and set the group type to **Security** and the group scope to **Domain local**.
  - The **RAS and IAS Servers** security group has **Read** permission to the **RAS and IAS Servers Access Check** object.
- Verify that the LAN protocols (TCP/IP and IPX) used for routing over the router-to-router VPN connection are enabled for routing on both the calling router and answering router.
- Verify that all of the PPTP or L2TP ports on the calling router and answering router are not already being used. If necessary, change the number of PPTP to L2TP ports from the properties of the **Ports** object in the Routing and Remote Access snap-in to allow more concurrent connections.
- Verify that the tunneling protocol of the calling router is supported by the answering router.  
By default, a Windows 2000 demand-dial interface with the VPN type set to **Automatic** will try to establish a L2TP/IPSec-based VPN connection first, then they try a PPTP-based VPN connection. If either the **Point to Point Tunneling Protocol (PPTP)** or **Layer-2 Tunneling Protocol (L2TP)** server type option is selected, verify that the selected tunneling protocol is supported by the answering router.

Depending on your selections when running the Routing and Remote Access Server Setup Wizard, a Windows 2000 Server-based computer running the Routing and Remote Access service is a PPTP and L2TP server with five or 128 L2TP ports and five or 128 PPTP ports. To create a PPTP-only server, set the number of L2TP ports to zero. To create an L2TP-only server, set the number of PPTP ports to 1 and disable remote access inbound connections and demand-dial connections for the **WAN Miniport (PPTP)** device from the properties of the **Ports** object in the Routing and Remote Access snap-in.

- For L2TP/IPSec connections, verify that computer certificates, also known as machine certificates, are installed on the calling router and the answering router.  
Verify that the calling router has a valid computer certificate installed that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the answering router trusts. Additionally, the answering router must have a valid computer certificate installed that was issued by a CA that follows a valid certificate chain from the issuing CA up to a root CA that the calling router trusts.
- Verify the configuration of the authentication provider. The answering router can be configured to use either Windows or RADIUS to authenticate the credentials of the calling router.
  - For RADIUS authentication, verify that the answering router computer can communicate with the RADIUS server.
  - For an answering router that is a member of a Windows 2000 native-mode domain, verify that the answering router has joined the domain.
  - For a computer Windows NT version 4.0 Service Pack 4 and later with RRAS server that is a member of a Windows 2000 mixed mode domain or a Windows 2000 answering router that is a member of a Windows NT 4.0 domain that is accessing user account properties for a user account in a trusted

Windows 2000 domain, verify that the **Everyone** group is added to the **Pre-Windows 2000 Compatible Access** group with the **net localgroup "Pre-Windows 2000 Compatible Access" /add** command. If not, issue the **net localgroup "Pre-Windows 2000 Compatible Access" everyone /add** command on a domain controller computer and then restart the domain controller.

- For a Windows NT version 4.0 Service Pack 3 and earlier RRAS server that is a member of a Windows 2000 mixed-mode domain, verify that the **Everyone** group has been granted list contents, read all properties, and read permissions to the root node of your domain and all sub-objects of the root domain.
- For PPTP connections using MS-CHAP and attempting to negotiate 40-bit MPPE encryption, verify that the password of the calling router is not larger than 14 characters.

### **Connection attempt is accepted when it should be rejected**

- Verify that the remote access permission on the user account is set to either **Deny access** or **Control access through Remote Access Policy**. If set to the latter, verify that the first matching remote access policy's remote access permission is set to **Deny remote access permission**. To obtain the name of the remote access policy that accepted the connection attempt, scan the accounting log for the entry corresponding to the connection attempt for the policy name.
- If you have created a remote access policy to explicitly reject all connections, verify the policy conditions, remote access permission, and profile settings.
- For certificate-based authentication when the certificate has been revoked, changes to the CRL of the CA might not yet be published. The authenticating server is using the old CRL that does not have the recently revoked certificate. To minimize the amount of time between the revoking of a certificate and when the authenticating server has knowledge of the revoked certificate, lower the CRL publication time. On a Windows 2000 CA, the publication time can be set as low as one hour. For more information, see the topic titled "Revoking certificates and publishing CRLs" in Windows 2000 online Help.

### **Unable to reach locations beyond the VPN router**

- Verify that IP routing is enabled (on the **IP** tab on the properties of the VPN router). Verify that network access is enabled (on the **IPX** tab on the properties of the VPN router).
- Verify that the appropriate demand-dial interface has been added to the protocol being routed.
- Verify that there are routes in the site routers on the calling router and answering router's site so that all locations on both networks are reachable. You can add routes to the routers of each site through static routes or by enabling a routing protocol on the site interface of the calling and answering routers. Unlike a remote access connection, a demand-dial connection does not automatically create a default route. You need to create routes on both sides of the demand-dial connection so that traffic can be routed to and from the other side of the demand-dial connection.

You can manually add static routes to the routing table, or you can add static routes through routing protocols. For persistent demand-dial connections, you can enable Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) across the demand-dial connection. For on-demand demand-dial connections, you can automatically update routes through an auto-static RIP update.

- For two-way initiated router-to-router VPN connections, verify that the router-to-router VPN connection is not interpreted by the VPN router as a remote access connection. For two-way initiated connections, either router can be the calling router or the answering router. The user names and demand-dial interface names must be properly matched. For example, two-way initiated

connections would work under the following configuration:

Router 1 has a demand-dial interface called NEW-YORK which is configured to use SEATTLE as the user name when sending authentication credentials.

Router 2 has a demand-dial interface called SEATTLE which is configured to use NEW-YORK as the user name when sending authentication credentials.

This example assumes that the SEATTLE user name can be validated by Router 2 and the NEW-YORK user name can be validated by Router 1.

If the incoming caller is a router, the port on which the call was received shows a status of **Active** and the corresponding demand-dial interface is in a **Connected** state. If the user account name in the credentials of the calling router appears under **Remote Access Clients** in the Routing and Remote Access snap-in, then the calling router has been interpreted by the answering router as a remote access client.

- For a one-way initiated demand-dial connection, verify that the appropriate static routes are enabled on the user account of the calling router and that the answering router is configured with a routing protocol so that when a connection is made, the static routes of the user account of the calling router are advertised to neighboring routers.
- Verify that there are no IP or IPX packet filters on the demand-dial interfaces of the calling router and answering router that prevent the sending or receiving of TCP/IP or IPX traffic.  
You can configure each demand-dial interface with IP and IPX input and output filters to control the exact nature of TCP/IP and IPX traffic that is allowed into and out of the demand-dial interface.

### Unable to reach the virtual interfaces of VPN routers

- Verify the IP address pools of the calling router and answering router.  
If the VPN router is configured to use a static IP address pool, verify that the routes to the range of addresses defined by the static IP address pools are reachable by the hosts and routers of the site. If not, then IP route consisting of the VPN router static IP address pools, as defined by the IP address and mask of the range, must be added to the routers of the site or enable the routing protocol of your routed infrastructure on the VPN router. If the routes to the address pool subnets are not present, calling router logical interfaces cannot receive traffic from locations on the site. Routes for the subnets are implemented either through static routing entries or through a routing protocol, such as Open Shortest Path First (OSPF) or Routing Information Protocol (RIP).

If the VPN router is configured to use DHCP for IP address allocation and no DHCP server is available, the VPN router assigns addresses from the Automatic Private IP Addressing (APIPA) address range from 169.254.0.1 through 169.254.255.254. Assigning APIPA addresses to VPN routers works only if the network to which the VPN router is attached is also using APIPA addresses.

If the VPN router is using APIPA addresses when a DHCP server is available, verify that the proper adapter is selected from which to obtain DHCP-allocated IP addresses. By default, the VPN router chooses the adapter to use to obtain IP addresses through DHCP based on your selections in the Routing and Remote Access Server Setup Wizard. You can manually choose a LAN adapter from the **Adapters** list on the **IP** tab on the properties of the VPN router in the Routing and Remote Access snap-in.

If the static IP address pools are a range of IP addresses that are a subset of the range of IP addresses for the network to which the VPN router is attached, verify that the range of IP addresses in the static IP address pool are not assigned to other TCP/IP nodes, either through static configuration or through DHCP.

### On-demand connection is not made automatically

- Verify that IP routing is enabled on the **IP** tab on the properties of the calling router.
- Verify that the correct static routes exist and are configured with the appropriate demand-dial interface.
- For the static routes that use a demand-dial interface, verify that the **Use this route to initiate demand-dial connections** check box on the properties of the demand-dial interface is selected.
- Verify that the demand-dial interface is not in a disabled state.  
To enable a demand-dial interface that is in a disabled state, right-click the demand-dial interface under **Routing Interfaces** in the Routing and Remote Access snap-in, and then click **Enable**.
- Verify that the dial-out hours for the demand-dial interface on the calling router are not preventing the connection attempt.  
To configure dial-out hours, right-click the demand-dial interface under **Routing Interfaces** in the Routing and Remote Access snap-in, and then click **Dial-out Hours**.
- Verify that the demand-dial filters for the demand-dial interface on the calling router are not preventing the connection attempt.  
To configure demand-dial filters, right-click the demand-dial interface under **Routing Interfaces** in the Routing and Remote Access snap-in, and then click **Set IP Demand-dial Filters**.

### Unable to establish tunnel

- Verify that packet filtering on a router interface between the calling router and the answering router is not preventing the forwarding of tunneling protocol traffic. See Appendix A for information on the types of traffic that must be allowed for PPTP and L2TP/IPSec traffic.

On a Windows 2000–based VPN router, IP packet filtering can be separately configured from the advanced TCP/IP properties and from the Routing and Remote Access snap-in. Check both places for filters that might be excluding VPN connection traffic.

- Verify that the Winsock Proxy client is not currently running on the VPN router.  
When the Winsock Proxy client is active, Winsock API calls such as those used to create tunnels and send tunneled data are intercepted and forwarded to a configured proxy server.

A proxy server–based computer allows an organization to access specific types of Internet resources (typically Web and FTP) without directly connecting that organization to the Internet. The organization can instead use private IP network IDs (such as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16).

Proxy servers are typically used so that private users in an organization can have access to public Internet resources as if they were directly attached to the Internet. VPN connections are typically used so that authorized public Internet users can gain access to private organization resources as if they were directly attached to the private network. A single computer can act as a proxy server (for private users) and a VPN server (for authorized Internet users) to facilitate both exchanges of information.

---

## Summary

This paper described in detail the components and their associated design decisions for a Windows 2000-based router-to-router VPN deployment including VPN routers, Internet infrastructure, authentication protocols, VPN protocols, site infrastructure, AAA infrastructure, and certificate infrastructure. This paper also included detailed walkthroughs of PTPP and L2TP-based router-to-router VPN deployments using computers running Windows 2000 Server, details of firewall configuration, and a discussion of VPN troubleshooting tools and common VPN problems with suggested solutions.

---

## Related Links

For more information about VPN, see the [Windows 2000 Virtual Private Networks page](http://www.microsoft.com/vpn) at <http://www.microsoft.com/vpn>.

For the latest information on Windows 2000, check out our World Wide Web site at <http://www.microsoft.com/windows2000/default.asp>.