



Operating System

Windows 2000 Virtual Private Networking Scenario

White Paper

Abstract

The use of both public and private networks to create a network connection is called a virtual private network (VPN). In this scenario, Electronic, Inc., a fictional company, has deployed Windows 2000 Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) VPN technologies to create secure remote access, branch office, and business partner connectivity solutions. This paper describes the design and configuration of the Electronic, Inc. VPN and dial-up remote access infrastructure.

© 2000 Microsoft Corporation. All rights reserved.

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, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

3/00

CONTENTS

INTRODUCTION	1
COMMON CONFIGURATION FOR THE VPN SERVER.....	2
Network Configuration	2
Remote Access Policy Configuration	5
Domain Configuration	5
Security Configuration	6
VPN REMOTE ACCESS FOR EMPLOYEES	7
Domain Configuration	7
Remote Access Policy Configuration	7
PPTP-based Remote Access Client Configuration	8
L2TP-based Remote Access Client Configuration	8
ON-DEMAND BRANCH OFFICE	9
Domain Configuration	9
Remote Access Policy Configuration	10
PPTP-based On-Demand Branch Office	10
Demand-Dial Interface for the Connection to the ISP	11
Demand-Dial Interface for Router-to-Router VPN Connection	11
Static Route for Corporate Headquarters and Branch Offices	12
Static Route for Electronic, Inc. VPN Server	12
PPTP Packet Filters on the Demand-Dial Interface Connecting to ISP	12
L2TP-based On-Demand Branch Office	12
Certificate Configuration	13
Demand-Dial Interface for the Connection to the ISP	13
Demand-Dial Interface for Router-to-Router VPN Connection	13
Static Route for Corporate Headquarters and Branch Offices	14
Static Route for Electronic, Inc. VPN Server	14
L2TP Over IPsec Packet Filters on Demand-Dial Interface Connecting to ISP	14
PERSISTENT BRANCH OFFICE.....	15
Domain Configuration	15
Remote Access Policy Configuration	16
IP Address Pool Configuration	17
PPTP-based Persistent Branch Office	18
VPN Server Configuration	18
Chicago Router Configuration	19
L2TP-based Persistent Branch Office	20
VPN Server Configuration	20
Phoenix Router Configuration	21
EXTRANET FOR BUSINESS PARTNERS.....	24
Domain Configuration	25
Remote Access Policy Configuration	25

PPTP-based Extranet for Business Partners	26
Demand-Dial Interface for Router-to-Router VPN Connection	26
Static Route for Electronic, Inc. Extranet	27
PPTP Packet Filters on the Internet Interface	27
L2TP-based Extranet for Business Partners	27
Certificate Configuration	27
Demand-Dial Interface for Router-to-Router VPN Connection	27
Static Route for Electronic, Inc. Extranet	28
L2TP Over IPsec Packet Filters on the Internet Interface	28
DIAL-UP AND VPNs WITH RADIUS AUTHENTICATION.....	29
Domain Configuration	29
Remote Access Policy Configuration	29
RADIUS Configuration	30
Dial-up Remote Access Client Configuration	30
APPENDIX A - PROCEDURES.....	31
Enabling the Routing and Remote Access Service	31
Creating a Static IP Address Pool	31
Enabling EAP	31
Adding PPTP or L2TP Ports	32
Setting a Phone Number on a Device	32
Adding PPTP Packet Filters	32
Adding L2TP Packet Filters	33
Configuring Automatic Certificate Allocation	34
Copying the IAS Configuration to Another Server	34
Registering RADIUS Clients	35
Configuring RADIUS Authentication	35
Configuring RADIUS Accounting	36
SUMMARY	37
For More Information	37

INTRODUCTION

This white paper describes how common virtual private network scenarios are configured for a fictional company by using the Windows 2000 operating system. Although your network configuration may be different than those described here, you can still apply the basic concepts of virtual private networking in your network environment.

The use of both public and private networks to create a network connection is called a virtual private network (VPN).

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. 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 link in which the private data is encapsulated and encrypted is a virtual private network (VPN) connection.

Electronic, Inc. is a fictional electronics design and manufacturing company with a main corporate campus in New York and branch offices and distribution business partners throughout the United States. Electronic, Inc. has implemented a VPN solution by using the Windows 2000 operating system to connect remote access users, branch offices, and business partners.

The VPN server at the corporate office provides both remote access and router-to-router PPTP and L2TP VPN connections. In addition, the VPN server provides the routing of packets to intranet and Internet locations.

Based on the common configuration of the VPN server, the following virtual private network scenarios are described:

- VPN remote access for employees.
- On-demand branch office access.
- Persistent branch office access.
- Extranet for business partners.
- Dial-up and VPNs with RADIUS authentication.

Note: The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

COMMON CONFIGURATION FOR THE VPN SERVER

To deploy a VPN solution for Electronic, Inc., the network administrator performs an analysis and makes design decisions regarding:

- The network configuration.
- The remote access policy configuration.
- The domain configuration.
- The security configuration.

Network Configuration

The key elements of the network configuration are:

- The Electronic, Inc. corporate intranet uses the private networks of 172.16.0.0 with a subnet mask of 255.240.0.0 and 192.168.0.0 with a subnet mask of 255.255.0.0. The corporate campus network segments use subnets of 172.16.0.0 and the branch offices use subnets of 192.168.0.0.
- The VPN server computer is directly attached to the Internet using a T3 (also known as a DS-3) dedicated WAN link.
- The IP address of the WAN adapter on the Internet is 207.46.130.1 as allocated by the Internet service provider (ISP) for Electronic, Inc. The IP address of the WAN adapter is referred to on the Internet by the domain name vpn.electronic.microsoft.com.
- The VPN server computer is directly attached to an intranet network segment that contains a router that connects to the rest of the Electronic, Inc. corporate campus intranet. The intranet network segment has the IP network ID of 172.31.0.0 with the subnet mask of 255.255.0.0.
- The VPN server computer is configured with a static pool of IP addresses to allocate to remote access clients and calling routers that is a subset of the intranet network segment (an on-subnet address pool).

Figure 1 shows the network configuration of the Electronic, Inc. VPN server.

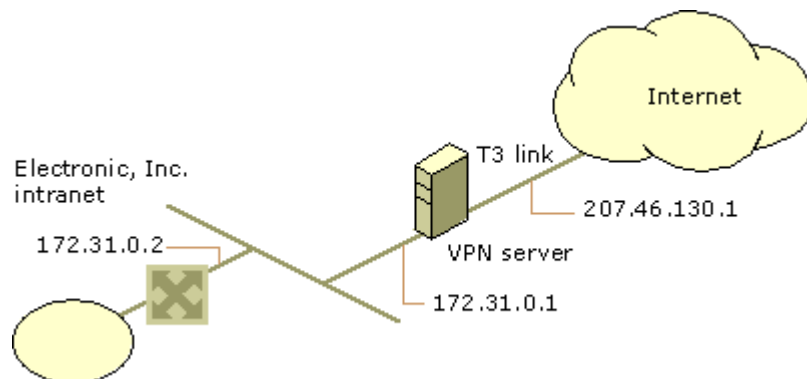


Figure 1: The network configuration of the Electronic, Inc. VPN server

Based on the network configuration of the Electronic, Inc. corporate campus intranet, the VPN server computer is configured as follows:

1. Install hardware on the VPN server.

The network adapter that is used to connect to the intranet segment and the WAN adapter that is used to connect to the Internet are installed according to the adapter manufacturer's instructions. Once drivers are installed and functioning, both adapters appear as local area connections in the Network and Dial-up Connections folder.

2. Configure TCP/IP on the LAN and WAN adapters.

For the LAN adapter, an IP address of 172.31.0.1 with a subnet mask 255.255.0.0 is configured. For the WAN adapter, an IP address of 207.46.130.1 with a subnet mask 255.255.255.255 is configured. A default gateway is not configured for either adapter. DNS and WINS server addresses are also configured.

3. Install the Routing and Remote Access service.

The Routing and Remote Access Server Setup wizard is run. In the wizard, the **Manually configured server** option is selected. For more information, see the ["Enabling the Routing and Remote Access service"](#) procedure in Appendix A.

After the wizard is complete, a static IP address pool with a starting IP address of 172.31.255.1 and an ending IP address of 172.31.255.254 is configured. This creates a static address pool for up to 253 VPN clients.

For more information, see the ["Creating a Static IP Address Pool"](#) procedure in Appendix A.

The default method of authenticating remote access and demand-dial connections is to use Windows authentication, which is appropriate in this configuration containing only one VPN server. For information on the use of RADIUS authentication for Electronic, Inc., see the ["Dial-up and VPNs with RADIUS"](#) section in this paper. For more information on the use of Windows and RADIUS authentication, see the topic titled "Authentication vs. Authorization" in the Windows 2000 Server Help.

4. Enable the EAP authentication method.

To enable the use of smart card-based remote access VPN clients and certificate-based calling routers, the network administrator enables the Extensible Authentication Protocol (EAP) on the VPN server.

For more information, see the ["Enabling EAP"](#) procedure in Appendix A.

5. Configure static routes on the VPN server to reach intranet and Internet locations.

To reach intranet locations, a static route is configured with the following settings:

- Interface: The LAN adapter attached to the intranet
- Destination: 172.16.0.0
- Network mask: 255.240.0.0
- Gateway: 172.31.0.2
- Metric: 1

This static route simplifies routing by summarizing all destinations on the Electronic, Inc. intranet. This static route is used so that the VPN server does not need to be configured with a routing protocol such as RIP or OSPF. For more information on routing basics, see the “Unicast Routing Principles” white paper at

<http://www.microsoft.com/NTServer/commserve/techdetails/prodarch/unicast.asp>

and the Windows 2000 Server Help.

To reach Internet locations, a static route is configured with the following settings:

- Interface: The WAN adapter attached to the Internet
- Destination: 0.0.0.0
- Network mask: 0.0.0.0
- Gateway: 0.0.0.0
- Metric: 1

This static route summarizes all destinations on the Internet. This route allows the VPN server to respond to a remote access client or demand-dial router VPN connection from anywhere on the Internet.

Note: Because the WAN adapter creates a point-to-point connection to the ISP, any address can be entered for the gateway. The gateway address of 0.0.0.0 is an example. 0.0.0.0 is the unspecified IP address.

6. Increase the number of PPTP and L2TP ports.
By default, only five L2TP ports and five PPTP ports are enabled for VPN connections. The number of L2TP and PPTP ports is increased to 253. For more information, see the “[Adding PPTP or L2TP Ports](#)” procedure in Appendix A.
7. Configure PPTP and L2TP over IPsec packet filters.
Both PPTP and L2TP over IPsec packet filters are configured on the WAN adapter that connects to the Internet. To secure the VPN server from sending or receiving any traffic on its Internet interface, except for PPTP or L2TP over IPsec traffic from branch office routers or remote access clients, PPTP and L2TP over IPsec input and output filters must be configured on the Internet interface. Because IP routing is enabled on the Internet interface, if you do not configure L2TP over IPsec and PPTP filters on the Internet interface of the VPN server, then any traffic received on the Internet interface is routed, potentially forwarding unwanted Internet traffic to the intranet. For more information, see the “[Adding PPTP Packet Filters](#)” and “[Adding L2TP Packet Filters](#)” procedures in Appendix A. For information on IP packet filtering, see Windows 2000 Server Help and the *Microsoft Windows 2000 Server Resource Kit Internetworking Guide*.
8. Setting the phone number for the PPTP and L2TP devices.
To assist in the configuration of remote access policies that confine VPN

connections from Internet users, the port properties for the **WAN Miniport (PPTP)** and **WAN Miniport (L2TP)** devices are modified with the IP address of the VPN server's Internet interface in the **Phone number for this device** field. For more information, see the "[Setting a Phone Number on a Device](#)" procedure in Appendix A.

9. Configure a static route on the intranet router to reach all branch offices. To reach branch office locations from the intranet router, a static route is configured with the following settings:
 - Interface: The LAN adapter attached to the intranet
 - Destination: 192.168.0.0
 - Network mask: 255.255.0.0
 - Gateway: 172.31.0.1
 - Metric: 1

This static route simplifies routing by summarizing all destinations at Electronic, Inc. branch offices.

Remote Access Policy Configuration

Electronic, Inc. has migrated to a Windows 2000-based native-mode domain and the network administrator for Electronic, Inc. has decided on an access-by-policy administrative model. The remote access permission on all user accounts is set to **Control access through Remote Access Policy**. The granting of remote access permission to connection attempts is controlled by the remote access permission setting on the first matching remote access policy. Remote access policies are used to apply different VPN connection settings based on group membership, and the default remote access policy named **Allow access if dial-in permission is enabled** is deleted.

For more information, see the topic "Remote Access Policy Administrative Models" in Windows 2000 Server Help.

Domain Configuration

To take advantage of the ability to apply different connection settings to different types of VPN connections, the following Windows 2000 groups are created:

- VPN_Users
Used for remote access VPN connections
- VPN_Routers
Used for router-to-router VPN connections from Electronic, Inc. branch offices
- VPN_Partners
Used for router-to-router VPN connections from Electronic, Inc. business partners

Note: All users and groups in this scenario are created in the electronic.microsoft.com Active Directory™ domain.

Security Configuration

To enable L2TP over IPSec connections and the use of smart cards by remote access clients, the Electronic, Inc. domain is configured to auto-enroll machine certificates to all domain members.

For more information, see the [“Configuring Automatic Certificate Allocation”](#) procedure in Appendix A.

VPN REMOTE ACCESS FOR EMPLOYEES

Remote access for Electronic, Inc. employees is deployed by using remote access VPN connections across the Internet based on the settings configured in the [“Common Configuration for the VPN Server”](#) section of this paper and the following additional settings.

Figure 2 shows the Electronic, Inc. VPN server that provides remote access VPN connections.

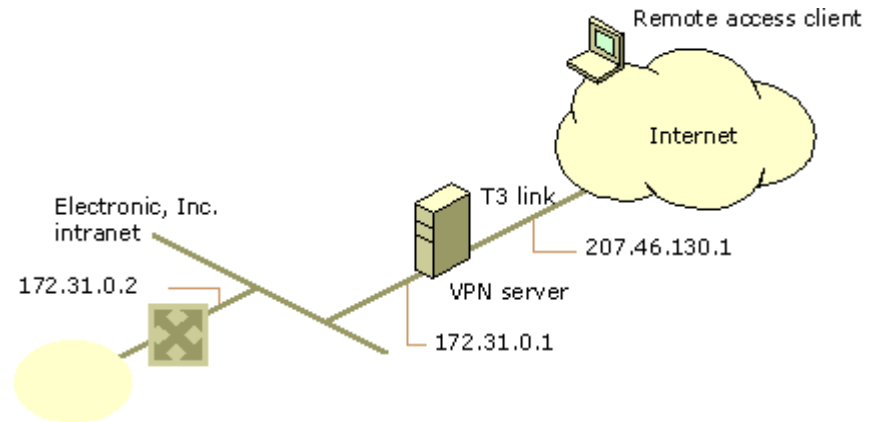


Figure 2: The Electronic, Inc. VPN server that provides remote access VPN connections

Domain Configuration

For each employee that is allowed VPN access:

- The remote access permission on the dial-in properties of the user account is set to **Control access through Remote Access Policy**.
- The user account is added to the VPN_Users Windows 2000 group.

Remote Access Policy Configuration

To define the authentication and encryption settings for remote access VPN clients, the following remote access policy is created:

- Policy name: Remote Access VPN Clients
- Conditions:
 - **NAS-Port-Type** is set to Virtual (VPN).
 - **Windows-Groups** is set to VPN_Users.
 - **Called-Station-ID** is set to 207.46.130.1.
- Permission is set to **Grant remote access permission**.
- Profile settings:
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** and **Microsoft Encrypted Authentication (MS-CHAP)** are also selected.
 - **Encryption** tab: **Strong** and **Strongest** are the only options that are selected.

Note: The **Called-Station-ID** condition is set to the IP address of the Internet interface for the VPN server. Only tunnels initiated from the Internet are allowed. Tunnels initiated from the Electronic, Inc. intranet are not permitted. Electronic, Inc. users that require Internet access from the Electronic, Inc. intranet must go through the Electronic, Inc. proxy server (not shown), where Internet access is controlled and monitored.

PPTP-based Remote Access Client Configuration

The **Make New Connection** wizard is used on client computers to create a VPN connection with the following setting:

- Host name or IP address: vpn.electronic.microsoft.com

The VPN connection settings are modified as follows:

- On the **Networking** tab, **Type of dial-up server I am calling** is set to **Point-to-Point Tunneling Protocol (PPTP)**. This is done to provide better performance when connecting. When **Type of dial-up server I am calling** is set to **Automatic**, an IPSec security association (SA) for an L2TP connection is attempted first. By configuring the connection for PPTP, the IPSec SA for an L2TP connection is not attempted.

L2TP-based Remote Access Client Configuration

The remote access computer logs on to the Electronic, Inc. domain using a local area network (LAN) connection to the Electronic, Inc. intranet and receives a certificate through auto-enrollment. Then, the **Make New Connection** wizard is used to create VPN connection with the following setting:

- Host name or IP address: vpn.electronic.microsoft.com

The VPN connection settings are modified as follows:

- On the **Networking** tab, **Type of dial-up server I am calling** is set to **Layer-2 Tunneling Protocol (L2TP)**. When **Type of dial-up server I am calling** is set to **Automatic**, an IPSec security association (SA) for an L2TP connection is attempted first. If the IPSec SA is not successful, then a PPTP connection is attempted. In this case, the network administrator for Electronic, Inc. does not want remote access clients that are capable of establishing an L2TP connection to fall back to the PPTP connection.

ON-DEMAND BRANCH OFFICE

The Portland and Dallas branch offices of Electronic, Inc. are connected to the corporate office by using on-demand router-to-router VPN connections. Both the Portland and Dallas offices contain a small number of employees who only need occasional connectivity with the corporate office. The Windows 2000 routers in the Portland and Dallas offices are equipped with an ISDN adapter that dials a local Internet service provider to gain access to the Internet, and then a router-to-router VPN connection is made across the Internet. When the VPN connection is not used for five minutes, the routers at the branch offices terminate the VPN connection.

The Dallas branch office uses the IP network ID of 192.168.28.0 with a subnet mask of 255.255.255.0. The Portland branch office uses the IP network ID of 192.168.4.0 with a subnet mask of 255.255.255.0.

To simplify the configuration, the VPN connection is a one-way initiated connection that is always initiated by the branch office router. For more information, see the topic titled "One-way Initiated Demand-Dial Connections" in the Windows 2000 Server Help.

Figure 3 shows the Electronic, Inc. VPN server that provides on-demand branch office connections.

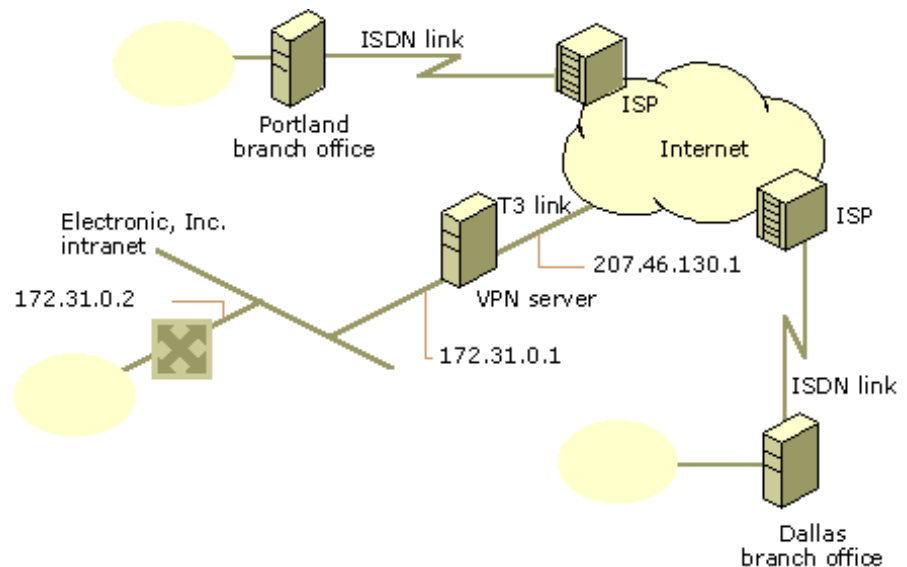


Figure 3: The Electronic, Inc. VPN server that provides on-demand branch office connections

To deploy on-demand router-to-router VPN connections to connect the Portland and Dallas branch offices to the corporate office based on the settings configured in the "[Common Configuration for the VPN server](#)" section of this paper, the following additional settings are configured.

Domain Configuration

For the VPN connection to the Dallas office, the user account VPN_Dallas is created with the following settings:

-
- Password of nY7W{q8~z3.
 - For the dial-in properties on the VPN_Dallas account, the remote access permission is set to **Control access through Remote Access Policy** and the static route 192.168.28.0 with a subnet mask of 255.255.255.0 is added.
 - For the account properties on the VPN_Dallas account, the **Password never expires** account option is selected.
 - The VPN_Dallas account is added to the VPN_Routers group.

For the VPN connection to the Portland office, the user account VPN_Portland is created with the following settings:

- Password of P*4s=wq!Gx1.
- For the dial-in properties on the VPN_Portland account, the remote access permission is set to **Control access through Remote Access Policy** and the static route 192.168.4.0 with a subnet mask of 255.255.255.0 is added.
- For the account properties on the VPN_Portland account, the **Password never expires** account option is selected.
- The VPN_Portland account is added to the VPN_Routers group.

Remote Access Policy Configuration

To define the authentication and encryption settings for the VPN routers, the following remote access policy is created:

- Policy name: VPN Routers.
- Conditions:
 - **NAS-Port-Type** is set to Virtual (VPN)
 - **Windows-Groups** is set to VPN_Routers
 - **Called-Station-ID** is set to 207.46.130.1
- Permission is set to **Grant remote access permission**.
- Profile settings:
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** is also selected.
 - **Encryption** tab: **Strong** and **Strongest** are the only options that are selected.

Note: The **Called-Station-ID** is set to the IP address of the Internet interface for the VPN server. Only tunnels initiated from the Internet are allowed. Tunnels initiated from the Electronic, Inc. intranet are not permitted. Electronic, Inc. users that require Internet access from the Electronic, Inc. intranet must go through the Electronic, Inc. proxy server (not shown), where Internet access is controlled and monitored.

The following sections describe a PPTP-based on-demand branch office connection for the Dallas office and an L2TP-based on-demand branch office connection for the Portland office.

PPTP-based On-Demand Branch Office

The Dallas branch office is a PPTP-based branch office that uses a Windows 2000

router to create an on-demand, router-to-router VPN connection with the VPN server in New York as needed. When the connection is made and is idle for five minutes, the connection is terminated.

To deploy a PPTP, one-way initiated, on-demand, router-to-router VPN connection to the corporate office based on the settings configured in the [“Common Configuration for the VPN Server”](#) and [“On-Demand Branch Office”](#) sections of this paper, the following settings are configured on the Dallas router.

Demand-Dial Interface for the Connection to the ISP

To connect the Dallas office router to the Internet by using a local ISP, a demand-dial interface is created using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
ISP
- **Connection type**
Connect using a modem, ISDN adapter, or other physical device is selected.
- **Select a device**
The appropriate ISDN device is selected.
- **Phone number or address**
Phone number of the ISP for the Dallas office.
- **Protocols and security**
The Route IP packets in this interface check box is selected.
- **Dial-out credentials**
User name: Dallas office ISP account name
Password: Dallas office ISP account password
Confirm password: Dallas office ISP account password

To run the Demand-Dial Interface wizard, right-click **Routing Interfaces**, and then click **New Demand-Dial Interface**.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the Dallas office router to the VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
CorpHQ
- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Point to Point Tunneling Protocol (PPTP) is selected.
- **Destination address**

207.46.130.1

- **Protocols and security**

The **Route IP packets on this interface** check box is selected.

- **Dial-out credentials**

User name: VPN_Dallas

Domain: electronic.microsoft.com

Password: nY7W{q8~=#z3

Confirm password: nY7W{q8~=#z3

Static Route for Corporate Headquarters and Branch Offices

To make all locations on the corporate intranet reachable, the following static route is configured:

- Interface: CorpHQ
- Destination: 172.16.0.0
- Network mask: 255.240.0.0
- Metric: 1

To make all locations on Electronic, Inc. branch offices reachable, the following static route is configured:

- Interface: CorpHQ
- Destination: 192.168.0.0
- Network mask: 255.255.0.0
- Metric: 1

Static Route for Electronic, Inc. VPN Server

To create the connection to the Dallas ISP when the router-to-router VPN connection needs to be made, the following static route is configured:

- Interface: ISP
- Destination: 207.46.130.1
- Network mask: 255.255.255.255
- Metric: 1

PPTP Packet Filters on the Demand-Dial Interface Connecting to ISP

To ensure that only PPTP-based traffic is allowed on the connection to the Internet, PPTP packet filters are configured on the ISP demand-dial interface. For more information, see the "[Adding PPTP Packet Filters](#)" procedure in Appendix A.

L2TP-based On-Demand Branch Office

The Portland branch office is an L2TP-based branch office that uses a Windows 2000 router to create an on-demand, router-to-router VPN connection with the VPN server in New York as needed. When the connection is made and is idle for five minutes, the connection is terminated.

To deploy an L2TP, one-way initiated, on-demand, router-to-router VPN connection to the corporate office based on the settings configured in the "[Common](#)

[Configuration for the VPN Server](#)” and “[On-Demand Branch Office](#)” sections of this paper, the following settings are configured on the Portland router:

Certificate Configuration

The Portland router was configured by the Electronic, Inc. network administrator while it was physically connected to the Electronic, Inc. intranet and then shipped to the Portland site. While the Portland router was connected to the Electronic, Inc. intranet, a computer certificate was installed through auto-enrollment.

Demand-Dial Interface for the Connection to the ISP

To connect the Portland office router to the Internet by using a local ISP, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
ISP
- **Connection type**
Connect using a modem, ISDN adapter, or other physical device is selected.
- **Select a device**
The appropriate ISDN device is selected.
- **Phone number or address**
Phone number of the ISP for the Portland office.
- **Protocols and security**
The **Route IP packets on this interface** check box is selected.
- **Dial-out credentials**
User name: Portland office ISP account name.
Password: Portland office ISP account password.
Confirm password: Portland office ISP account password.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the Portland office router to the VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
CorpHQ
- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Layer-2 Tunneling Protocol (L2TP) is selected.
- **Destination address**
207.46.130.1
- **Protocols and security**

The **Route IP packets on this interface** check box is selected.

- **Dial-out credentials**

User name: VPN_Portland

Domain: electronic.microsoft.com

Password: P*4s=wq!Gx1

Confirm password: P*4s=wq!Gx1

Static Route for Corporate Headquarters and Branch Offices

To make all locations on the corporate intranet reachable, the following static route is configured:

- Interface: CorpHQ
- Destination: 172.16.0.0
- Network mask: 255.240.0.0
- Metric: 1

To make all locations on Electronic, Inc. branch offices reachable, the following static route is configured:

- Interface: CorpHQ
- Destination: 192.168.0.0
- Network mask: 255.255.0.0
- Metric: 1

Static Route for Electronic, Inc. VPN Server

To create the connection to the Portland ISP when the router-to-router VPN connection needs to be made, the following static route is configured:

- Interface: ISP
- Destination: 207.46.130.1
- Network mask: 255.255.255.255
- Metric: 1

L2TP Over IPSec Packet Filters on Demand-Dial Interface Connecting to ISP

To ensure that only L2TP over IPSec-based traffic is allowed on the connection to the Internet, L2TP over IPSec packet filters are configured on the ISP demand-dial interface. For more information, see the "[Adding L2TP Packet Filters](#)" procedure in Appendix A.

PERSISTENT BRANCH OFFICE

The Chicago and Phoenix branch offices of Electronic, Inc. are connected to the corporate office by using persistent router-to-router VPN connections that stay connected 24 hours a day. The Windows 2000 routers in the Chicago and Phoenix offices are equipped with T1 WAN adapters that have a permanent connection to a local Internet service provider to gain access to the Internet.

The Chicago branch office uses the IP network ID of 192.168.9.0 with a subnet mask of 255.255.255.0. The Chicago branch office router uses the public IP address of 131.107.0.1 for its Internet interface. The Phoenix branch office uses the IP network ID of 192.168.14.0 with a subnet mask of 255.255.255.0. The Phoenix branch office router uses the public IP address of 131.107.128.1 for its Internet interface.

The VPN connection is a two-way initiated connection. The connection is initiated from either the branch office router or the VPN server. Two-way initiated connections require the creation of demand-dial interfaces, remote access policies, IP address pools, and packet filters on the routers on both sides of the connection.

Figure 4 shows the Electronic, Inc. VPN server that provides persistent branch office connections.

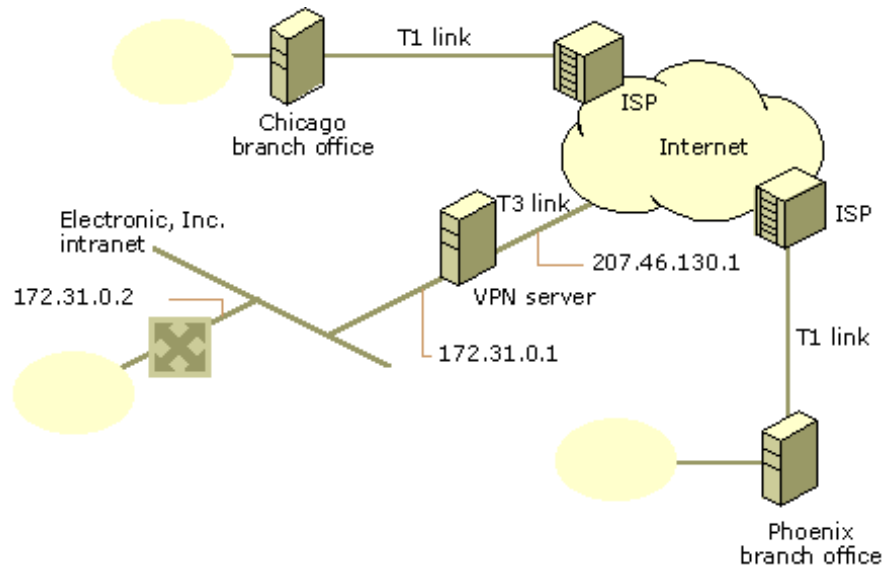


Figure 4: The Electronic, Inc. VPN server that provides persistent branch office connections

To deploy persistent router-to-router VPN connections to connect the Chicago and Phoenix branch offices to the corporate office based on the settings configured in the [“Common Configuration for the VPN Server”](#) section of this paper, the following additional settings are configured.

Domain Configuration

For the Chicago office VPN connection that is initiated by the Chicago router, the user account VPN_Chicago is created with the following settings:

-
- Password of U9!j5dP(%q1.
 - For the dial-in properties on the VPN_Chicago account, the remote access permission is set to **Control access through Remote Access Policy**.
 - For the account properties on the VPN_Chicago account, the **Password never expires** account option is selected.
 - The VPN_Chicago account is added to the VPN_Routers group.

For the Phoenix office VPN connection that is initiated by the Phoenix router, the user account VPN_Phoenix is created with the following settings:

- Password of z2F%s)bW\$4f.
- For the dial-in properties on the VPN_Phoenix account, the remote access permission is set to **Control access through Remote Access Policy**.
- For the account properties on the VPN_Phoenix account, the **Password never expires** account option is selected.
- The VPN_Phoenix account is added to the VPN_Routers group.

For the Chicago office VPN connection and the Phoenix office VPN connection that are initiated by the VPN server, the user account VPN_CorpHQ is created with the following settings:

- Password of o3\Dn6@`-J4.
- For the dial-in properties on the VPN_CorpHQ account, the remote access permission is set to **Control access through Remote Access Policy**.
- The VPN_CorpHQ account is added to the VPN_Routers group.

Remote Access Policy Configuration

Remote access policies must be configured at the VPN server, the Chicago router, and the Phoenix router.

Remote Access Policy Configuration at the VPN Server

The remote access policy configuration for the VPN server is the same as described in the [“On-Demand Branch Office”](#) section of this paper.

Remote Access Policy Configuration at the Chicago Router

To define the authentication and encryption settings for the VPN connections, the default policy named **Allow access if dial-in permission is enabled** is deleted and the following remote access policy is created:

- Policy name: VPN Routers
- Conditions:
 - **NAS-Port-Type** is set to Virtual (VPN)
 - **Windows-Groups** is set to VPN_Routers
 - **Called-Station-ID** is set to 131.107.0.1
- Permission is set to **Grant remote access permission**
- Profile settings:
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-**

-
- **CHAP v2** is also selected.
 - **Encryption** tab: **Strong** and **Strongest** are the only options that are selected.

Note: The **Called-Station-ID** is set to the IP address of the Internet interface for the branch office router. Only tunnels initiated from the Internet are allowed. Tunnels initiated from the Electronic, Inc. branch office network are not permitted.

Remote Access Policy Configuration at the Phoenix Router

To define the authentication and encryption settings for the VPN connections, the default policy named **Allow access if dial-in permission is enabled** is deleted and the following remote access policy is created:

- Policy name: VPN Routers
- Conditions:
 - **NAS-Port-Type** is set to **Virtual (VPN)**
 - **Windows-Groups** is set to VPN_Routers
 - **Called-Station-ID** is set to 131.107.128.1
- Permission is set to **Grant remote access permission**
- Profile settings:
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** is also selected.
 - **Encryption** tab: **Strong** and **Strongest** are the only options that are selected.

Note: The **Called-Station-ID** is set to the IP address of the Internet interface for the branch office router. Only tunnels initiated from the Internet are allowed. Tunnels initiated from the Electronic, Inc. branch office network are not permitted.

IP Address Pool Configuration

IP address pools must be configured at the VPN server, the Chicago router, and the Phoenix router.

IP Address Pool Configuration at the VPN Server

The IP address pool configuration for the VPN server is the same as described in the "[Common Configuration for the VPN Server](#)" section of this paper.

IP Address Pool Configuration at the Chicago Router

A static IP address pool with an IP address of 192.168.9.248 and an ending IP address of 192.168.9.253 is configured. This creates a static address pool for up to five VPN clients.

For more information, see the "[Creating a Static IP Address Pool](#)" procedure in Appendix A.

IP Address Pool Configuration at the Phoenix Router

A static IP address pool with a starting IP address of 192.168.14.248 and an ending IP address of 192.168.14.253 is configured. This creates a static address pool for

up to five VPN clients.

For more information, see the [“Creating a Static IP Address Pool”](#) procedure in Appendix A.

The following sections describe a PPTP-based persistent branch office connection for the Chicago office and an L2TP-based persistent branch office connection for the Phoenix office.

PPTP-based Persistent Branch Office

The Chicago branch office is a PPTP-based branch office that uses a Windows 2000 router to create a persistent, router-to-router VPN connection with the VPN server in New York. The connection is never terminated, even when idle.

To deploy a PPTP, two-way initiated, persistent, router-to-router VPN connection to the corporate office based on the settings configured in the [“Common Configuration for the VPN Server”](#) and [“Persistent Branch Office”](#) sections of this paper, the following settings are configured on the VPN server and Chicago router.

VPN Server Configuration

The VPN server is configured with a demand-dial interface, static routes, and PPTP packet filters.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the VPN server to the Chicago router by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
VPN_Chicago
- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Point to Point Tunneling Protocol (PPTP) is selected.
- **Destination address**
131.107.0.1
- **Protocols and security**
The **Route IP packets on this interface** check box is selected.
- **Dial-out credentials**
User name: VPN_CorpHQ
Domain: electronic.microsoft.com
Password: o3\Dn6@`-J4
Confirm password: o3\Dn6@`-J4

Once the demand-dial interface is created, the following change is made:

- For the properties of the demand-dial interface, on the **Options** tab, under

Connection type, Persistent connection is selected.

Static Route for Chicago Office Network

To make all locations on the Chicago network reachable, the following static route is configured:

- Interface: VPN_Chicago
- Destination: 192.168.9.0
- Network mask: 255.255.255.0
- Metric: 1

Chicago Router Configuration

The Chicago router is configured with a demand-dial interface and static routes.

Demand-dial interface for router-to-router VPN connection

To connect the Chicago office router to the VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the Demand-Dial Interface wizard with the following settings:

- **Interface name**
VPN_CorpHQ
- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Point to Point Tunneling Protocol (PPTP) is selected.
- **Destination address**
207.46.130.1
- **Protocols and security**
The **Route IP packets on this interface** check box is selected.
- **Dial-out credentials**
User name: VPN_Chicago
Domain: electronic.microsoft.com
Password: U9!j5dP(%q1
Confirm password: U9!j5dP(%q1

Once the demand-dial interface is created, the following change is made:

- For the properties of the demand-dial interface, on the **Options** tab, under **Connection type, Persistent connection** is selected. To view properties for a demand-dial interface, click **Routing Interfaces**, right-click the desired demand-dial interface, and then click **Properties**.

Static route for the Electronic, Inc. VPN server

To make the Electronic, Inc. VPN server on the Internet reachable, the following static route is configured:

- Interface: The WAN adapter attached to the Internet
- Destination: 207.46.130.1

-
- Network mask: 255.255.255.255
 - Gateway: 0.0.0.0
 - Metric: 1

Note: Because the WAN adapter creates a point-to-point connection to the ISP, any address can be entered for the gateway. The gateway address of 0.0.0.0 is an example. 0.0.0.0 is the unspecified IP address.

Static Routes for Corporate Intranet and Branch Offices

To make all locations on the corporate intranet reachable, the following static route is configured:

- Interface: VPN_CorpHQ
- Destination: 172.16.0.0
- Network mask: 255.240.0.0
- Metric: 1

To make all locations on Electronic, Inc. branch offices reachable, the following static route is configured:

- Interface: VPN_CorpHQ
- Destination: 192.168.0.0
- Network mask: 255.255.0.0
- Metric: 1

PPTP Packet Filters on the Internet Interface

To ensure that only PPTP-based traffic is allowed on the connection to the Internet, you can configure PPTP packet filters on the Internet interface. For more information, see the [“Adding PPTP Packet Filters”](#) procedure in Appendix A.

L2TP-based Persistent Branch Office

The Phoenix branch office is an L2TP-based branch office that uses a Windows 2000 router to create a persistent, router-to-router VPN connection with the VPN server in New York. The connection is never terminated, even when idle.

To deploy an L2TP, two-way initiated, persistent, router-to-router VPN connection to the corporate office based on the settings configured in the [“Common Configuration for the VPN Server”](#) and [“Persistent Branch Office”](#) sections of this paper, the following settings are configured on the VPN server and Phoenix router.

VPN Server Configuration

The VPN server is configured with a demand-dial interface and a static route.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the VPN server to the Phoenix router by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- Interface name
VPN_Phoenix

-
- Connection type
Connect using virtual private networking (VPN) is selected.
 - VPN type
Layer-2 Tunneling Protocol (L2TP) is selected.
 - Destination address
131.107.128.1
 - Protocols and security
The **Route IP packets on this interface** check box is selected.
 - Dial-out credentials
User name: VPN_CorpHQ
Domain: electronic.microsoft.com
Password: o3\Dn6@`-J4
Confirm password: o3\Dn6@`-J4

After the demand-dial interface is created, the following change is made:

- For the properties of the demand-dial interface, on the **Options** tab, under **Connection type**, **Persistent connection** is selected.

Static Route for Phoenix Office Network

To make all locations on the Phoenix network reachable, the following static route is configured:

- Interface: VPN_Phoenix
- Destination: 192.168.14.0
- Network mask: 255.255.255.0
- Metric: 1

Phoenix Router Configuration

The Phoenix router was configured by the Electronic, Inc. network administrator while connected to the Electronic, Inc. intranet and then shipped to the Phoenix site. While the Phoenix router was connected to the Electronic, Inc. intranet, a computer certificate was installed through auto-enrollment. Additionally, the Phoenix router computer was configured with a demand-dial interface and a static route.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the Phoenix office router to the VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
VPN_CorpHQ
- Connection type
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Layer-2 Tunneling Protocol (L2TP) is selected.

-
- **Destination address**
207.46.130.1
 - **Protocols and security**
The **Route IP packets on this interface** check box is selected.
 - **Dial-out credentials**
User name: VPN_Phoenix
Domain: electronic.microsoft.com
Password: z2F%s)bW\$4f
Confirm password: z2F%s)bW\$4f

Once the demand-dial interface is created, the following change is made:

- For the properties of the demand-dial interface, on the **Options** tab, under **Connection type**, **Persistent connection** is selected.

Static Route for the Electronic, Inc. VPN Server

To make the Electronic, Inc. VPN server on the Internet reachable, the following static route is configured:

- Interface: The WAN adapter attached to the Internet
- Destination: 207.46.130.1
- Network mask: 255.255.255.255
- Gateway: 0.0.0.0
- Metric: 1

Note: Because the WAN adapter creates a point-to-point connection to the ISP, any address can be entered for the gateway. The gateway address of 0.0.0.0 is an example. 0.0.0.0 is the unspecified IP address.

Static Route for Corporate Intranet and Branch Offices

To make all locations on the corporate intranet reachable, the following static route is configured:

- Interface: VPN_CorpHQ
- Destination: 172.16.0.0
- Network mask: 255.240.0.0
- Metric: 1

To make all locations on Electronic, Inc. branch offices reachable, the following static route is configured:

- Interface: VPN_CorpHQ
- Destination: 192.168.0.0
- Network mask: 255.255.0.0
- Metric: 1

L2TP over IPSec Packet Filters on the Internet Interface

To ensure that only L2TP over IPSec-based traffic is allowed on the connection to the Internet, L2TP over IPSec packet filters are configured on the Internet interface.

For more information, see the [“Adding L2TP Packet Filters”](#) procedure in Appendix A.

EXTRANET FOR BUSINESS PARTNERS

The network administrator for Electronic, Inc. has created an extranet, a portion of the Electronic, Inc. private network that is available to business partners through secured VPN connections. The Electronic, Inc. extranet is the network attached to the Electronic, Inc. VPN server and contains a file server and a Web server. Parts distributors Tasmanian Traders and Parnell Aerospace are Electronic, Inc. business partners and connect to the Electronic, Inc. extranet by using on-demand, router-to-router VPN connections. An additional remote access policy is used to ensure that the business partners can only access the extranet file server and Web server.

The file server on the Electronic, Inc. extranet is configured with an IP address of 172.31.0.10 and the Web server is configured with an IP address of 172.31.0.11. Tasmanian Traders uses the public network ID of 131.107.254.0 with a subnet mask of 255.255.255.0. Parnell Aerospace uses the public network ID of 131.107.250.0 with a subnet mask of 255.255.255.0. To ensure that the extranet Web server and file server can reach the business partners, static routes are configured on the file server and Web server for each of the business partner networks that use the gateway address of 172.31.0.1

To simplify configuration, the VPN connection is a one-way initiated connection. The connection is always initiated by the business partner's router. For more information, see the topic titled "One-Way Initiated Demand-Dial Connections" in Windows 2000 Server Help.

Figure 5 shows the Electronic, Inc. VPN server that provides extranet connections for business partners.

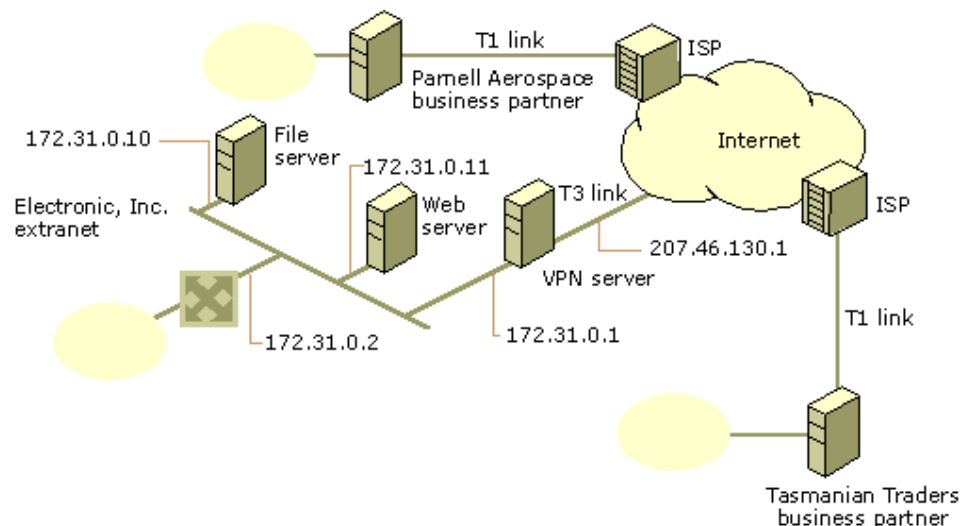


Figure 5: The Electronic, Inc. VPN server that provides extranet connections for business partners

To deploy business partner, on-demand, one-way initiated, router-to-router VPN connections to connect Tasmanian Traders and Parnell Aerospace to the Electronic, Inc. extranet based on the settings configured in the ["Common](#)

[Configuration for the VPN Server](#)” section of this paper, the following additional settings are configured.

Domain Configuration

For the VPN connection to Tasmanian Traders, the user account PTR_Tasmanian is created with the following settings:

- Password of Y8#-vR7?jfl.
- For the dial-in properties on the PTR_Tasmanian account, the remote access permission is set to **Control access through Remote Access Policy** and the static route 131.107.254.0 with a subnet mask 255.255.255.0 is added.
- For the account properties on the PTR_Tasmanian account, the **Password never expires** account option is enabled.
- The PTR_Tasmanian account is added to the VPN_Partners group.

For the VPN connection to Parnell Aerospace, the user account PTR_Parnell is created with the following settings:

- Password of W@8c^4r;2\.
- For the dial-in properties on the PTR_Parnell account, the remote access permission is set to **Control access through Remote Access Policy** and the static route 131.107.250.0 with a subnet mask 255.255.255.0 is added.
- For the account properties on the PTR_Parnell account, the **Password never expires** account option is selected.
- The PTR_Parnell account is added to the VPN_Partners group.

Remote Access Policy Configuration

To define the authentication and encryption settings for business partner VPN connections, the following remote access policy is created:

- Policy name: VPN Partners
- Conditions:
 - **NAS-Port-Type** is set to **Virtual (VPN)**
 - **Windows-Groups** is set to VPN_Partners
 - **Called-Station-ID** is set to 207.46.130.1
- Permission is set to **Grant remote access permission**
- Profile settings:
 - On the **IP** tab, the following TCP/IP packet filters are configured:
From client:
 - Filter action: Deny all traffic except those listed below
 - Filter 1: Destination network IP address of 172.31.0.10 and subnet mask of 255.255.255.255
 - Filter 2: Destination network IP address of 172.31.0.11 and subnet mask of 255.255.255.255

To client:

- Filter action: Deny all traffic except those listed below

-
- Filter 1: Source network IP address of 172.31.0.10 and subnet mask of 255.255.255.255
 - Filter 2: Source network IP address of 172.31.0.11 and subnet mask of 255.255.255.255
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** is also selected.
 - **Encryption** tab: **Strong** and **Strongest** are the only options that are selected.

Note: The **Called-Station-ID** is set to the IP address of the Internet interface for the VPN server. Only tunnels initiated from the Internet are allowed. Tunnels initiated from the Electronic, Inc. intranet are not permitted. Electronic, Inc. users that require Internet access from the Electronic, Inc. intranet must go through the Electronic, Inc. proxy server (not shown), where Internet access is controlled and monitored.

The following sections describe a PPTP-based extranet for the business partner Tasmanian Traders and an L2TP-based extranet for the business partner Parnell Aerospace.

PPTP-based Extranet for Business Partners

Tasmanian Traders is a business partner that uses a Windows 2000 router to create an on-demand, PPTP-based, router-to-router VPN connection with the Electronic, Inc. VPN server in New York as needed. When the connection is created and is idle for five minutes, the connection is terminated. The Tasmanian Traders router is connected to the Internet by using a permanent WAN connection.

To deploy a PPTP, one-way initiated, on-demand, router-to-router VPN connection to the corporate office based on the settings configured in the [“Common Configuration for the VPN Server”](#) and [“Extranet for Business Partners”](#) sections of this paper, the following settings are configured on the Tasmanian Traders router.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the Tasmanian Traders router to the Electronic, Inc. VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**
Electronic
- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Point to Point Tunneling Protocol (PPTP) is selected.
- **Destination address**

207.46.130.1

- **Protocols and security**

The **Route IP packets on this interface** check box is selected.

- **Dial-out credentials**

User name: PTR_Tasmanian

Domain: electronic.microsoft.com

Password: Y8#-vR7?]fl

Confirm password: Y8#-vR7?]fl

Static Route for Electronic, Inc. Extranet

To make all locations on the Electronic, Inc. extranet reachable, the following static route is configured:

- Interface: Electronic
- Destination: 172.31.0.0
- Network mask: 255.255.0.0
- Metric: 1

PPTP Packet Filters on the Internet Interface

To ensure that only PPTP-based traffic is allowed on the connection to the Internet, you can configure PPTP packet filters on the Internet interface. For more information, see the "[Adding PPTP Packet Filters](#)" procedure in Appendix A.

L2TP-based Extranet for Business Partners

Parnell Aerospace is a business partner that uses a Windows 2000 router to create an on-demand, L2TP-based, router-to-router VPN connection with the Electronic, Inc. VPN server in New York as needed. When the connection is created and is idle for five minutes, the connection is terminated. The Parnell Aerospace router is connected to the Internet by using a permanent WAN connection.

To deploy an L2TP, one-way initiated, on-demand, router-to-router VPN connection to the corporate office based on the settings configured in the "[Common Configuration for the VPN Server](#)" and "[Extranet for Business Partners](#)" sections of this paper, the following settings are configured on the Parnell Aerospace router:

Certificate Configuration

The Parnell Aerospace router was configured by the Electronic, Inc. network administrator while physically connected to the Electronic, Inc. intranet and then shipped to the network administrator at Parnell Aerospace. While the Parnell Aerospace router was connected to the Electronic, Inc. intranet, a computer certificate was installed through auto-enrollment.

Demand-Dial Interface for Router-to-Router VPN Connection

To connect the Parnell Aerospace router to the Electronic, Inc. VPN server by using a router-to-router VPN connection over the Internet, a demand-dial interface is created by using the **Demand-Dial Interface** wizard with the following settings:

- **Interface name**

Electronic

- **Connection type**
Connect using virtual private networking (VPN) is selected.
- **VPN type**
Layer-2 Tunneling Protocol (L2TP) is selected.
- **Destination address**
207.46.130.1 (This is the IP address of the Electronic, Inc. VPN server's interface on the Internet).
- **Protocols and security**
The **Route IP packets on this interface** check box is selected.
- **Dial-out credentials**
User name: PTR_Parnell
Domain: electronic.microsoft.com
Password: W@8c^4r-;2\
Confirm password: W@8c^4r-;2\

Static Route for Electronic, Inc. Extranet

To make all locations on the Electronic, Inc. extranet reachable, the following static route is configured:

- Interface: Electronic
- Destination: 172.31.0.0
- Network mask: 255.255.0.0
- Metric: 1

L2TP Over IPSec Packet Filters on the Internet Interface

To ensure that only L2TP over IPSec-based traffic is allowed on the connection to the Internet, L2TP over IPSec packet filters are configured on the Internet interface. For more information, see the "[Adding L2TP Packet Filters](#)" procedure in Appendix A.

DIAL-UP AND VPNs WITH RADIUS AUTHENTICATION

In addition to VPN-based remote access, the network administrator for Electronic, Inc. wants to provide modem-based dial-up remote access for employees of the New York office. All employees of the New York office belong to a Windows 2000-based group called NY_Employees. A separate remote access server running Windows 2000 provides dial-up remote access at the phone number 555-0111. Rather than administer the remote access policies of both the VPN server and the remote access server separately, the network administrator is using a computer running Windows 2000 with the Internet Authentication Service (IAS) as a RADIUS server. The IAS server has an IP address of 172.31.0.9 on the Electronic, Inc. extranet and provides centralized remote access authentication, authorization, and accounting for both the remote access server and the VPN server.

Figure 6 shows the Electronic, Inc. RADIUS server that provides authentication and accounting for the VPN server and the remote access server.

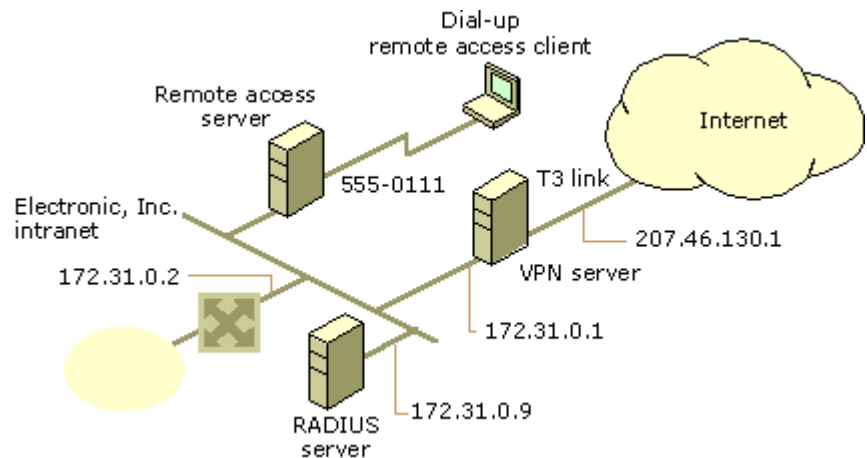


Figure 6: The Electronic, Inc. RADIUS server that provides authentication and accounting for the VPN server and the remote access server

Domain Configuration

For each New York office employee that is allowed dial-up access, the remote access permission for the dial-in properties of the user account is set to **Control access through Remote Access Policy**.

Remote Access Policy Configuration

Remote access policies must be modified in two ways:

1. The existing remote access policies that are configured on the VPN server running Windows 2000 must be copied to the IAS server.
2. A new remote access policy is added for dial-up remote access clients on the IAS server.

Copying the Remote Access Policies

Once the VPN server running Windows 2000 is configured to use RADIUS authentication, the remote access policies stored on the VPN server are no longer

used. Instead, the remote access policies stored on the IAS server running Windows 2000 are used. Therefore, the current set of remote access policies is copied to the IAS server.

For more information, see the [“Copying the IAS Configuration to Another Server”](#) procedure in Appendix A.

Creating a New Remote Access Policy for Dial-up Remote Access Clients

To define the authentication and encryption settings for dial-up connections by employees of the New York office, the following remote access policy is created on the RADIUS server computer:

- Policy name: Dial-Up for New York Employees
- Conditions:
 - **NAS-Port-Type** is set to all types *except* **Virtual (VPN)**.
 - **Windows-Groups** is set to NY_Employees.
- Permission is set to **Grant remote access permission**.
- Profile settings:
 - **Authentication** tab: **Extensible Authentication Protocol** is selected and **Smartcard or other certificate (TLS)** is configured to use the installed machine certificate. **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** and **Microsoft Encrypted Authentication (MS-CHAP)** are also selected.
 - **Encryption** tab: All options are selected.

RADIUS Configuration

To configure RADIUS authentication and accounting, the network administrator for Electronic, Inc. configures the following:

- The RADIUS server is a computer running Windows 2000 Server with the Internet Authentication Service networking component installed. The Internet Authentication Service is configured for two RADIUS clients: the remote access server and the VPN server. For more information, see the [“Registering RADIUS Clients”](#) procedure in Appendix A.
- The remote access server running Windows 2000 is configured to use RADIUS authentication and accounting at the IP address of 172.31.0.9 and a shared secret. For more information, see the [“Configuring RADIUS Authentication”](#) and [“Configuring RADIUS Accounting”](#) procedures in Appendix A.
- The VPN server running Windows 2000 is configured to use RADIUS authentication and accounting at the IP address of 172.31.0.9 and a shared secret. For more information, see the [“Configuring RADIUS Authentication”](#) and [“Configuring RADIUS Accounting”](#) procedures in Appendix A.

Dial-up Remote Access Client Configuration

The **Make New Connection** wizard is used to create a dial-up connection with the following setting:

- Phone number: 555-0111

APPENDIX A - PROCEDURES

Enabling the Routing and Remote Access Service

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.

By default, the local computer is listed as a server.
To add another server, in the console tree, right-click **Server Status**, and then click **Add Server**.
In the **Add Server** dialog box, click the applicable option, and then click **OK**.
2. In the console tree, right-click the server you want to enable, and then click **Configure and Enable Routing and Remote Access**.
3. In the **Routing and Remote Access Server Setup** wizard, click **Next**.
4. In **Common Configurations**, click **Manually configured server**, click **Next**, and then click **Finish**.
5. When prompted, start the **Routing and Remote Access** service.

Note: If this server is a member of a Windows 2000 Active Directory domain and you are not a domain administrator, instruct your domain administrator to add the computer account of this server to the RAS and IAS Servers security group in the domain of which this server is a member. The domain administrator can add the computer account to the RAS and IAS Servers security group by using **Active Directory Users and Computers** or with the command **netsh ras add registeredserver**.

Creating a Static IP Address Pool

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, right-click the server for which you want to create a static IP address pool, and then click **Properties**.
3. On the **IP** tab, click **Static address pool**, and then click **Add**.
4. In **Start IP address**, type a starting IP address, and then either type an ending IP address for the range in **End IP address** or type the number of IP addresses in the range in **Number of addresses**.
5. Click **OK**, and then repeat steps 3 and 4 for as many ranges as you want to add.

Note: If the static IP address pool consists of IP addresses ranges that are for a separate subnet, then you need to either enable an IP routing protocol on the remote access server computer or add static IP routes consisting of the {IP Address, Mask} of each range to the intranet routers. If the routes are not added, then remote access clients cannot receive traffic from intranet resources.

Enabling EAP

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click the server name for which you want to configure EAP, and then click **Properties**.
3. On the **Security** tab, click **Authentication Methods**.
4. In the **Authentication Methods** dialog box, select the **Extensible authentication protocol (EAP)** check box, and then click **OK**.

Note: When you enable EAP, all installed EAP types are enabled. By default, EAP-MD5 CHAP and EAP-TLS are installed and enabled. To see the installed EAP types, click **EAP Methods**.

Adding PPTP or L2TP Ports

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, click the server for which you want to configure PPTP or L2TP ports.
3. In the details pane, right-click **Ports**, and then click **Properties**.
4. In the **Ports Properties** dialog box, click either **WAN Miniport (PPTP)** or **WAN Miniport (L2TP)**, and then click **Configure**.
5. In **Maximum ports**, type the number of ports, and then click **OK**.
6. Click **OK** to save changes to ports properties.

Setting a Phone Number on a Device

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, click the server for which you want to set a phone number.
3. In the details pane, right-click **Ports**, and then click **Properties**.
4. In the **Ports Properties** dialog box, click the device that corresponds to the dial-up or VPN equipment, and then click **Configure**.
5. In **Phone number for this device**, type the phone number for the port. For VPN ports, type the IP address of the VPN server Internet interface.
6. Click **OK**.

Adding PPTP Packet Filters

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, double-click the server for which you want to configure PPTP packet filtering.
3. Double-click **IP Routing**.
4. Click **General**.
5. In the details pane, right-click the interface that is connected to the Internet and then click **Properties**.
6. On the **General** tab, click **Input Filters**.
7. In the **Input Filters** dialog box, click **Add**.
8. In the **Add IP Filter** dialog box, select the **Destination network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **Other**. In **Protocol number**, type **47**, and then click **OK**.
9. In the **Input Filters** dialog box, click **Add**.
10. In the **Add IP Filter** dialog box, select the **Destination network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **TCP**. In **Destination port**, type **1723**, and then click **OK**.
11. In the **Input Filters** dialog box, click **Add**.

-
12. In the **Add IP Filter** dialog box, select the **Destination network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **TCP [established]**. In **Source port**, type **1723** and then click **OK**.
 13. In the **Input Filters** dialog box, click **Drop all packets except those that meet the criteria below**, and then click **OK**.
 14. On the **General** tab, click **Output Filters**.
 15. In the **Output Filters** dialog box, click **Add**.
 16. In the **Add IP Filter** dialog box, select the **Source network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **Other**. In **Protocol number**, type **47**, and then click **OK**.
 17. In the **Output Filters** dialog box, click **Add**.
 18. In the **Add IP Filter** dialog box, select the **Source network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **TCP**. In **Source port**, type **1723**, and then click **OK**.
 19. In the **Output Filters** dialog box, click **Add**.
 20. In the **Add IP Filter** dialog box, select the **Source network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **TCP [established]**. In **Destination port**, type **1723**, and then click **OK**.
 21. In the **Output Filters** dialog box, click **Drop all packets except those that meet the criteria below**, and then click **OK**.
 22. Click **OK** to save changes to the interface.

Adding L2TP Packet Filters

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, double-click the server for which you want to configure L2TP packet filtering.
3. Double-click **IP Routing**.
4. Click **General**.
5. In the details pane, right-click the interface connected to the Internet, and then click **Properties**.
6. On the **General** tab, click **Input Filters**.
7. In the **Input Filters** dialog box, click **Add**.
8. In the **Add IP Filter** dialog box, select the **Destination network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **UDP**. In **Source port**, type **500**. In **Destination port**, type **500**, and then click **OK**.
9. In the **Input Filters** dialog box, click **Add**.
10. In the **Add IP Filter** dialog box, select the **Destination network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **UDP**. In

-
- Source port**, type **1701**. In **Destination port**, type **1701**, and then click **OK**.
 11. In the **Input Filters** dialog box, click **Drop all packets except those that meet the criteria below**, and then click **OK**.
 12. On the **General** tab, click **Output Filters**.
 13. In the **Output Filters** dialog box, click **Add**.
 14. In the **Add IP Filter** dialog box, select the **Source network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **UDP**. In **Source port**, type **500**. In **Destination port**, type **500**, and then click **OK**.
 15. In the **Output Filters** dialog box, click **Add**.
 16. In the **Add IP Filter** dialog box, select the **Source network** check box. In **IP address**, type the IP address of the VPN server or demand-dial router's Internet interface, and in **Subnet mask**, type **255.255.255.255**. In **Protocol**, click **UDP**. In **Source port**, type **1701**. In **Destination port**, type **1701**, and then click **OK**.
 17. In the **Output Filters** dialog box, click **Drop all packets except those that meet the criteria below**, and then click **OK**.
 18. Click **OK** to save changes to the interface.

Configuring Automatic Certificate Allocation

1. Log on as a domain administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In **Active Directory Users and Computers**, right-click the domain that contains your certificate authority (CA) and then click **Properties**.
4. Click the **Group Policy** tab, click **Default Domain Policy**, and then click **Edit**.
5. In **Group Policy**, double-click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, and then click **Public Key Policies**.
6. Right-click **Automatic Certificate Request Settings**, click **New**, and then click **Automatic Certificate Request**.
7. In the **Automatic Certificate Request Setup** wizard, click **Next**.
8. In **Certificate templates**, click **Computer**, and then click **Next**.
9. Select your certificate authority, click **Next**, and then click **Finish**.
10. Close the **Group Policy** console.
11. To obtain a certificate immediately on the VPN server through auto-enrollment, either restart the VPN server computer or type **secdit /refreshpolicy machine_policy** at a Windows 2000 command prompt.

Copying the IAS Configuration to Another Server

1. At a command prompt, type **netsh aaa show config <path>\file.txt**. This stores the configuration settings, including registry settings, in a text file. The path can be relative, absolute, or a UNC path.
2. Copy the file you created to the destination computer and, at a command prompt on the destination computer, type **netsh exec <path>\file.txt**. A message appears indicating whether the update was successful.

Notes: You do not need to stop IAS on the destination computer to run the **netsh exec** command. When the command is run, IAS is automatically refreshed with the

updated configuration settings. This procedure replicates all remote access policy, registry, and logging configuration.

Registering RADIUS Clients

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Authentication Service**.
2. Right-click **Clients**, and then click **New Client**.
3. In **Friendly name**, type a descriptive name.
4. In **Protocol**, click **RADIUS**, and then click **Next**.
5. In **Client address (IP or DNS)**, type the DNS name or IP address for the client. If you are using a DNS name, click **Verify**. In the **Resolve DNS Name** dialog box, click **Resolve**, and then select the IP address you want to associate with that name from **Search results**.
6. If the client is a NAS and you are planning to use NAS-specific remote access policies for configuration purposes (for example, a remote access policy that contains vendor-specific attributes), click **Client Vendor**, and select the manufacturer's name. If you do not know the manufacturer name or it is not in the list, click **RADIUS Standard**.
7. In **Shared secret**, type the shared secret for the client, and then type it again in **Confirm shared secret**.
8. If your NAS supports using digital signatures for verification (with PAP, CHAP, or MS-CHAP), click **Client must always send the signature attribute in the request**. If the NAS does not support digital signatures for PAP, CHAP, or MS-CHAP, do not click this option.

Notes: If IAS receives an access request from a RADIUS proxy server, IAS cannot detect the manufacturer of the NAS that originated the request. This can cause problems if you plan to use authorization conditions based on the client vendor and have at least one client defined as a RADIUS proxy server.

- Passwords (shared secrets) are case-sensitive. Be sure that the client's shared secret and the shared secret you type in this field are identical to each other and conform to the password rules.
- If the client address cannot be resolved when you click **Verify**, make sure that the DNS name you typed is correct.
- The friendly name that you provide for your RADIUS clients can be used in remote access policies to restrict access.

Configuring RADIUS Authentication

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, right-click the server name for which you want to configure RADIUS authentication, and then click **Properties**.
3. On the **Security** tab, in **Authentication provider**, click **RADIUS Authentication**, and then click **Configure**.
4. In the **RADIUS Authentication** dialog box, click **Add**.

-
5. In the **Add RADIUS Server** dialog box, configure the settings for your RADIUS authentication server, and then click **OK**.

Configuring RADIUS Accounting

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. In the console tree, right-click the server name for which you want to configure RADIUS accounting, and then click **Properties**.
3. On the **Security** tab, in **Accounting provider**, click **RADIUS Accounting**, and then click **Configure**.
4. In the **RADIUS Accounting** dialog box, click **Add**.
5. In the **Add RADIUS Server** dialog box, configure the settings for your RADIUS accounting server, and then click **OK**.

SUMMARY

Electronic, Inc. used Windows 2000 VPN technologies to extend the connectivity of the Internet to connect remote users, branch offices, and business partners. Electronic, Inc.'s Windows 2000 VPN and dial-up remote access servers, used in conjunction with the Internet Authentication Service, provide centralized authentication, authorization, accounting, and administration of remote access policies for a scalable VPN and dial-up remote access solution.

For More Information

For the latest information on Windows 2000, check out our Web site at <http://www.microsoft.com/windows2000> and the Windows 2000/NT Forum at <http://computingcentral.msn.com/topics/windowsnt>.