

Module 7: Configuring Remote Access

Contents

Overview	1
Examining Remote Access in Windows 2000	2
Configuring Inbound Connections	10
Configuring Outbound Connections	17
Configuring Multilink Connections	22
Lab A: Configuring a VPN Connection	24
Configuring Authentication Protocols	30
Configuring Encryption Protocols	34
Configuring Routing and Remote Access for DHCP Integration	36
Review	40



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. 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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

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

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
90 Minutes

This module provides students with the knowledge and skills necessary to configure a remote access server and clients in a Microsoft® Windows® 2000 network.

Lab:
45 Minutes

At the end of this module, students will be able to:

- Describe the remote access process and protocols.
- Configure inbound connections on a remote access server.
- Configure outbound connections on a remote access client.
- Configure Multilink connections.
- Configure authentication protocols for remote access sessions.
- Configure encryption protocols for remote access sessions.
- Configure Routing and Remote Access for Dynamic Host Configuration Protocol (DHCP) integration.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the Microsoft PowerPoint® file 2153a_07.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the following white papers:
 - *Microsoft Privacy Protected Network Access: Virtual Private Networking and Intranet Security*
 - *Windows 2000–Based Virtual Private Networking: Supporting VPN Interoperability*
 - *Virtual Private Networking: An Overview*
 - *Microsoft Windows 2000 TCP/IP Implementation Details*
- Search for and read the “Remote Access Server” and “Virtual Private Networking” topics in the Windows 2000 Server Resource Kit.
- Search for and read the “Remote Access” and “Virtual Private Networks” topics in Windows 2000 Server Help.

Module Strategy

Use the following strategy to present this module:

- **Examining Remote Access in Windows 2000**
Describe the remote access process. Compare dial-up and virtual private network (VPN) connections. Explain the remote access and local area network (LAN) protocols that Windows 2000 supports. Compare Point-to-Point Tunneling Protocol (PPTP) with Layer Two Tunneling Protocol (L2TP) as VPN protocols.
- **Configuring Inbound Connections**
Explain and demonstrate the procedures for configuring dial-up and VPN inbound connections. Explain and demonstrate the procedures for configuring modem and cable ports. Discuss the types of settings that can be configured for a user account for dial-in connections.
- **Configuring Outbound Connections**
Discuss the hardware options for remote access clients. Explain and demonstrate the procedures for configuring dial-up, VPN, and direct cable inbound connections.
- **Configuring Multilink Connections**
Explain the advantages of Multilink and the Bandwidth Allocation Protocol (BAP). Explain the procedure for configuring Multilink connections on the remote access server and client.
- **Configuring Authentication Protocols**
Explain the purpose of authentication protocols. Describe each of the standard authentication protocols that Windows 2000 supports. Explain how extensible authentication protocols are used.
- **Configuring Encryption Protocols**
Explain how to configure encryption protocols.
- **Configuring Routing and Remote Access for DHCP Integration**
List the options for assigning Internet Protocol (IP) addresses to remote access clients. Explain how to use DHCP for IP addressing for remote access clients.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Lab Setup

The lab in this module requires that you perform the procedure specified in the Classroom Setup Guide before performing the lab.

Lab Results

Performing the labs in this module introduces the following configuration change:

- A VPN connection between each pair of student computers is created in Network and Dial-up Connections.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about Routing and Remote Access in Windows 2000.

- **Examining Remote Access in Windows 2000**
- **Configuring Inbound Connections**
- **Configuring Outbound Connections**
- **Configuring Multilink Connections**
- **Configuring Authentication Protocols**
- **Configuring Encryption Protocols**
- **Configuring Routing and Remote Access for DHCP Integration**

*****ILLEGAL FOR NON-TRAINER USE*****

Remote access allows users to connect to your network from a remote location. The primary tasks for enabling remote access are configuring Routing and Remote Access, creating appropriate remote access connections on remote access clients, and configuring users' access rights to the remote access server.

After you install and configure Routing and Remote Access, there are several ways to enhance remote access to your Microsoft® Windows® 2000 network. You can configure authentication and encryption protocols to increase the security of your remote access connections, and use Dynamic Host Configuration Protocol (DHCP) to provide Internet Protocol (IP) addresses to dial-up clients.

At the end of this module, you will be able to:

- Describe the remote access process and protocols.
- Configure inbound connections on a remote access server.
- Configure outbound connections on a remote access client.
- Configure Multilink connections.
- Configure authentication protocols for remote access sessions.
- Configure encryption protocols for remote access sessions.
- Configure Routing and Remote Access for DHCP integration.

◆ Examining Remote Access in Windows 2000

Topic Objective

To list the process and protocols of remote access.

Lead-in

Remote access allows users to connect to your network from a remote location.

- Establishing a Remote Access Connection
- Data Transport Protocols
- Virtual Private Network Protocols

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 allows remote clients to connect to remote access servers through a variety of hardware, including analog modems, Integrated Services Digital Network (ISDN) adapters, and digital subscriber line (DSL) modems. The remote access server runs Routing and Remote Access, which supports various data transport protocols and virtual private network (VPN) protocols to enable remote connections. Familiarity with the benefits and limitations of these protocols will help you to take advantage of their capabilities and decide which protocols are appropriate for your network.

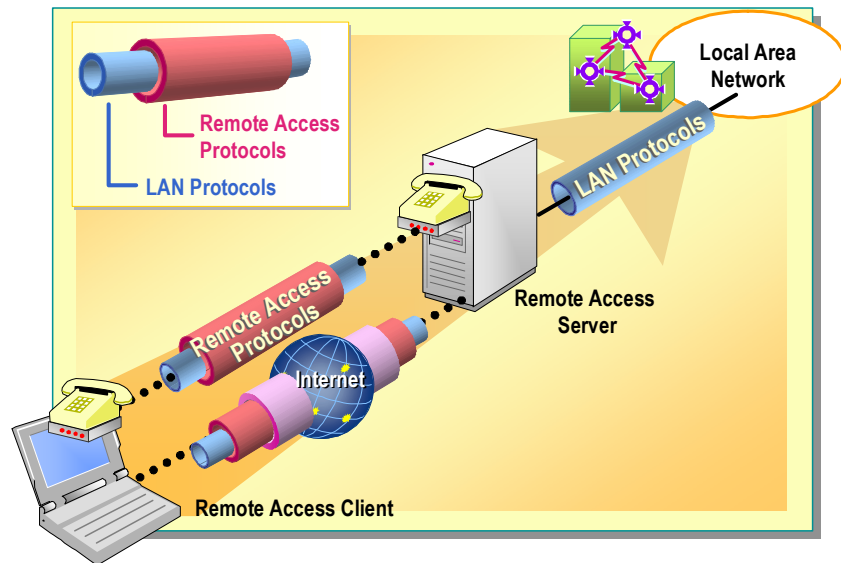
Establishing a Remote Access Connection

Topic Objective

To illustrate the process that occurs when establishing a remote access connection.

Lead-in

Remote or mobile workers can connect to the corporate network with remote access.



*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 Server remote access, part of the Routing and Remote Access service, enables remote or mobile workers to connect to corporate networks.

The Remote Access Process

Users run remote access software and initiate a connection to the remote access server. This connection uses a remote access protocol, such as the Point-to-Point Protocol (PPP).

The remote access server, which is a computer running Windows 2000 Server and the Routing and Remote Access service, authenticates users and remote access sessions until terminated by the user or network administrator. The remote access server acts as a gateway by sending data between the client and the local area network (LAN).

Using this connection, the client sends data to and receives data from the remote access server. The data is encoded by a protocol such as Transmission Control Protocol/Internet Protocol (TCP/IP) and is then encapsulated in a remote access protocol.

All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled for a remote user by means of the remote access connection.

Types of Remote Access Connectivity

Windows 2000 provides two different types of remote access connectivity.

Dial-up Connections

To connect to the network with dial-up remote access, a remote access client uses a communications network, such as the Public Switched Telephone Network (PSTN), to create a physical connection to a port on a remote access server on the private network. This is typically done by using a modem or ISDN adapter to dial in to the remote access server.

Dial-up remote access allows an organization to keep users connected to their network when they are working remotely. However, if your organization has a large number of users traveling to many locations, the expense of long-distance telephone charges will become significant. An alternative to increasing the size of a dial-up remote access network is to consider a VPN solution for remote connectivity.

Virtual Private Network Connections

A VPN provides secure remote access through the Internet, rather than through direct dial-up connections. A VPN client uses an IP internetwork to create an encrypted, virtual, point-to-point connection with a VPN gateway on the private network. Typically, the user connects to the Internet through an Internet service provider (ISP), and then creates a VPN connection to the VPN gateway. By using the Internet in this way, companies can reduce their long-distance telephone expenses and rely on existing infrastructure instead of managing their own infrastructures.

Companies that want to reduce the cost of remote access and increase their network flexibility can take advantage of VPN remote access. Traveling employees can dial the local ISP and then make a VPN connection back to the corporate network. This eliminates the long-distance charges or toll calls associated with a dial-up connection.

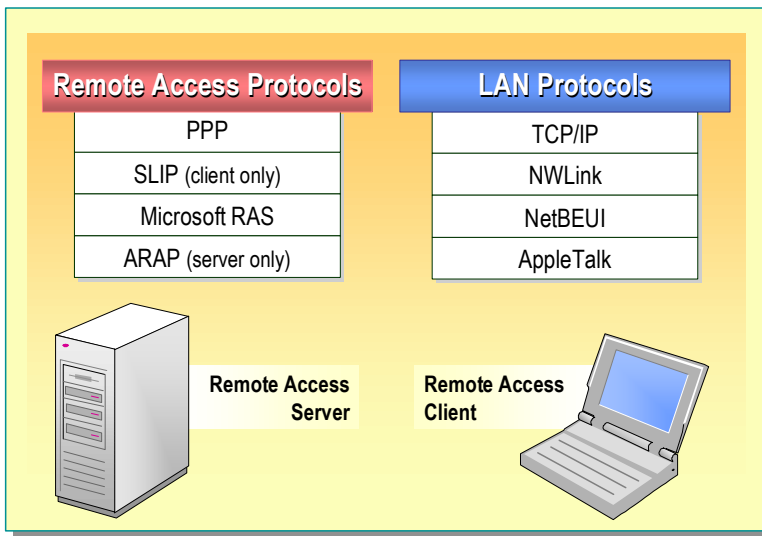
Data Transport Protocols

Topic Objective

To introduce the protocols that are used for remote access.

Lead-in

Windows 2000 uses both remote access protocols and LAN protocols to support remote access.



*****ILLEGAL FOR NON-TRAINER USE*****

Routing and Remote Access in Windows 2000 uses both remote access protocols and LAN protocols to enable clients to connect to remote access servers. Remote access protocols control transmission of data over wide area network (WAN) links, whereas LAN protocols control transmission of data within the local area network.

Windows 2000 uses a remote access protocol to establish a connection between the remote access devices (usually modems). Windows 2000 then uses LAN protocols to establish communication between the two computers. When a remote access client communicates with a server, Routing and Remote Access encapsulates the data in a LAN protocol packet for transport in the LAN. This packet is then encapsulated in a remote access protocol packet for transport to the server.

When you install and configure Routing and Remote Access, any protocols already installed on the computer are automatically enabled for remote access on inbound and outbound connections. For each LAN protocol, you must also specify whether you want to provide access to the entire network or only the remote access server. By default, access to the entire network is configured. If you provide access to the entire network by using TCP/IP, you must also configure how the server provides IP addresses.

Remote Access Protocols

Windows 2000 supports several remote access protocols to provide clients using a dial-up connection with access to a variety of remote access servers.

PPP

PPP enables remote access clients and servers to operate together in a multivendor network. For example, clients running Windows 2000 can connect to remote networks through any server that uses PPP. Similarly, computers running other remote access software can also use PPP to dial in to a computer running Routing and Remote Access. This is the most commonly used remote access protocol.

Serial Line Internet Protocol (SLIP)

SLIP allows Windows 2000 Professional-based computers to connect to a SLIP server. SLIP is most commonly used with Telnet, and is not suitable for most modern remote access applications. Routing and Remote Access does not include a SLIP server component, so a computer running Windows 2000 cannot be used as a SLIP server.

Microsoft RAS

For client computers running Microsoft Windows NT® version 3.1, Microsoft Windows for Workgroups, Microsoft MS-DOS®, or Microsoft LAN Manager to connect to a remote access server running Windows 2000, the client must use the network basic input/output system (NetBIOS) Enhanced User Interface (NetBEUI) protocol. The remote access server uses the Microsoft RAS protocol to act as a gateway for the remote access client, providing access to servers that use the NetBEUI, TCP/IP, or NWLink IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink) protocol. Client computers running Windows 2000 use the Microsoft RAS protocol to connect to remote access servers running Windows NT 3.1, Windows for Workgroups, MS-DOS, or LAN Manager.

AppleTalk Remote Access Protocol (ARAP)

Apple Macintosh clients can connect to a remote access server running Windows 2000 by using the ARAP protocol. Routing and Remote Access includes an ARAP server component but not a client component, so that client computers running Windows 2000 cannot connect to remote access servers that only support ARAP.

LAN Protocols

Routing and Remote Access supports the following LAN protocols:

- TCP/IP
- NWLink
- NetBEUI
- AppleTalk

Support for these protocols enables you to integrate Routing and Remote Access into existing Microsoft-based, UNIX, or Novell NetWare networks by using remote access protocols. For example, a remote access client can connect to a remote access server by using NetBEUI, and can use that server as a gateway to communicate with a UNIX server running TCP/IP or a NetWare server running Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

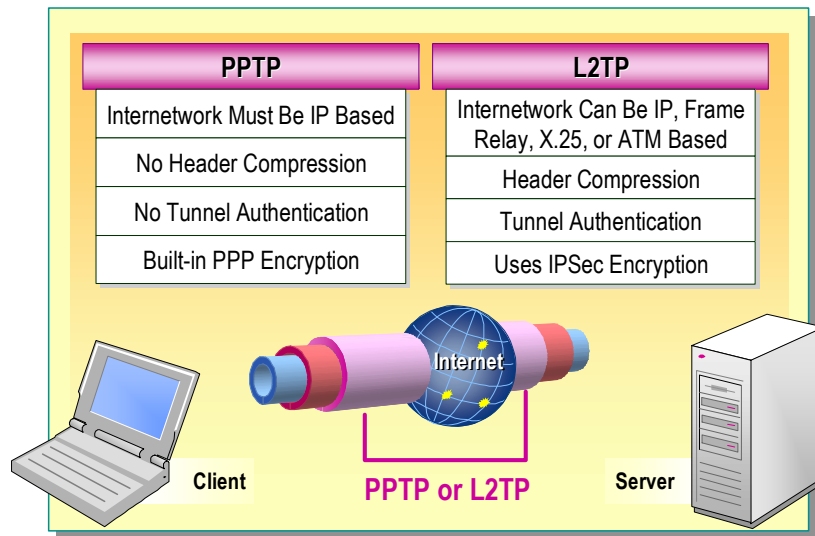
Virtual Private Network Protocols

Topic Objective

To list the differences between PPTP and L2TP.

Lead-in

VPN connections are encrypted and secure.



*****ILLEGAL FOR NON-TRAINER USE*****

A VPN connection over the Internet is encrypted and secure. The remote access server enforces authentication and encryption protocols. Sensitive data is hidden from Internet users, but made securely accessible to appropriate users through a VPN.

VPN Operation

Key Points

VPNs work by putting normal data packets inside encrypted PPP packets.

Most VPN connections start with a connection to an ISP, although only network connectivity to the VPN server is required.

VPN protocols encapsulate data packets inside PPP data packets. The remote access server performs all security checks and validations, and enables data encryption, making it safer to send data over nonsecure networks such as the Internet. Typically, users will connect to the VPN by first connecting to an ISP and then connecting to the VPN ports through that Internet connection.

Note A VPN does not require a dial-up connection. It only requires IP connectivity between the client and the server. If the client is directly attached to a LAN that uses IP, and it can reach a server through the LAN, you can establish a tunnel across the LAN.

VPNs use either the Point-to-Point Tunneling Protocol (PPTP) or the Layer Two Tunneling Protocol (L2TP) to establish connections. Windows 2000 automatically enables these protocols when you create VPN ports during the installation of Routing and Remote Access.

PPTP and L2TP

Both PPTP and L2TP use PPP to provide an initial envelope for the data and to append additional headers for transport through an internetwork. Some of the key differences between PPTP and L2TP include:

- *Connectivity.* L2TP performs over a wide range of WAN connection media such as IP or frame relay, requiring only that the tunnel media provide packet-oriented, point-to-point connectivity. PPTP requires an IP-based internetwork.
- *Header Compression.* L2TP supports header compression, but PPTP does not. When header compression is enabled, L2TP operates with headers of four bytes, but PPTP operates with six-byte headers.
- *Authentication.* L2TP supports tunnel authentication, but PPTP does not. IPsec provides computer-level authentication, in addition to data encryption, for VPN connections that use the L2TP protocol. IPsec negotiates between your computer and its remote access server before an L2TP connection is established, which secures both passwords and data.
- *Encryption.* PPTP uses PPP encryption. L2TP provides a secure tunnel by cooperating with other encryption technologies, such as Internet Protocol Security (IPsec).

◆ Configuring Inbound Connections

Topic Objective

To list topics relevant to configuring inbound connections in Windows 2000.

Lead-in

Inbound connections are configured with the Network Connection wizard or Routing and Remote Access.

- **Configuring Inbound Dial-up Connections**
- **Configuring Virtual Private Network Ports**
- **Configuring Modem and Cable Ports**
- **Configuring User Dial-in Settings**

*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

To create an inbound connection, you first enable a port for the appropriate type of connection (VPN, modem, or cable).

You use the Routing and Remote Access Server Setup wizard to configure common types of remote access servers, such as VPN servers.

When you configure an inbound connection on a remote access server, you enable a port through which a client can connect to your server. You can enable ports for VPN connections, modem connections, and direct cable connections.

If the computer is running Windows 2000 Professional, or is a server that is not a member of a domain, you configure inbound connections by using the Network Connection wizard.

When the computer is a server and a member of a domain, you must use Routing and Remote Access to configure inbound connections. Experience using Routing and Remote Access can help you set up VPNs and modem pools on a remote access server.

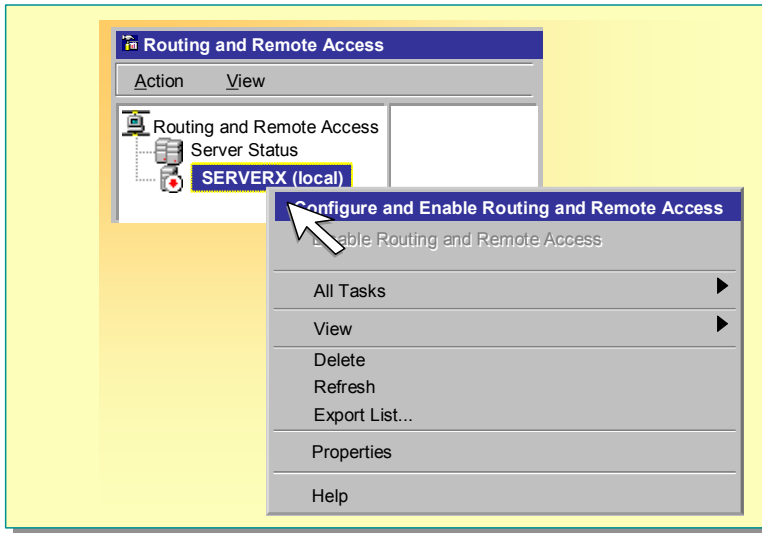
Configuring Inbound Dial-up Connections

Topic Objective

To illustrate the procedure for installing Routing and Remote Access.

Lead-in

The majority of computers that create inbound connections are members of a domain. Administrators must configure inbound connections on computers that belong to a domain by using Routing and Remote Access.



*****ILLEGAL FOR NON-TRAINER USE*****

To configure inbound connections on a computer that is a member of a domain, you must use Routing and Remote Access.

To configure remote access on the server:

Delivery Tips

Demonstrate installation of Routing and Remote Access, showing that the console is installed, but the service is not started initially.

Emphasize that students must *not* follow along with you during the demonstration. They will perform this task in the lab.

1. If necessary, verify the compatibility of your hardware by using the Hardware Compatibility List (HCL), and then install the hardware.
2. Install and configure all of the protocols that dial-up users will use, such as TCP/IP, NWLink, NetBEUI, and AppleTalk.
3. Open Routing and Remote Access from the **Administrative Tools** menu.
4. In the console tree, right-click the server name, and then click **Configure and Enable Routing and Remote Access**.
5. In the Routing and Remote Access Server Setup wizard, click **Next**.
6. On the **Common Configuration** page, select **Remote access server**, and then click **Next**.
7. On the **Remote Client Protocols** page, verify that you have all of the transport protocols that you want to use with remote access, and then click **Next**.
8. On the **Network Selection** page, select the network connection to which the remote access clients will be assigned, and then click **Next**.
9. On the **IP Address Assignment** page, select **Automatically** or **From a specified range of addresses** for assigning IP addresses to the dial-in clients.

10. On the **Managing Multiple Remote Access Servers** page, select whether you want to configure RADIUS (Remote Authentication Dial-In User Service) now, and then click **Next**.
11. Click **Finish** to complete the wizard.
12. Verify that dial-up clients are allocated an appropriate IP address, Domain Name System (DNS) server address, IPX network address, NetBIOS name, or AppleTalk network when they are connected.
13. Configure remote access policies, authentication, and encryption settings.

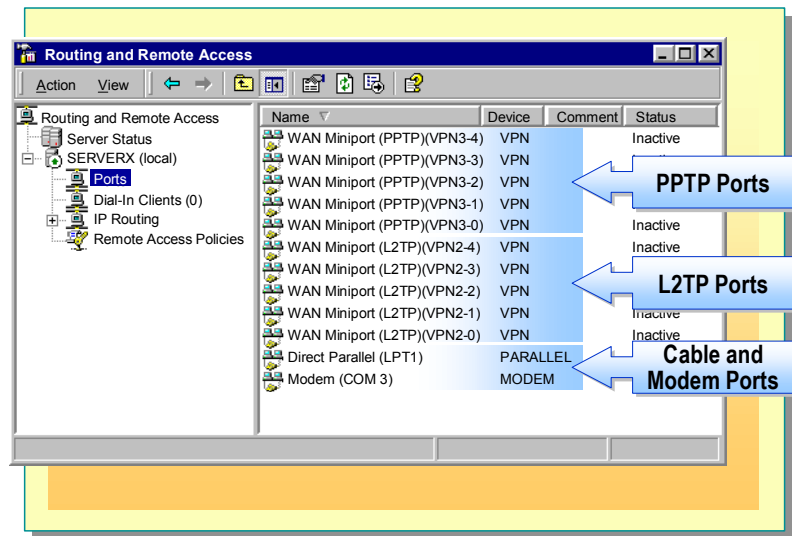
Configuring Virtual Private Network Ports

Topic Objective

To illustrate the location of different remote access ports in Routing and Remote Access.

Lead-in

You configure VPN ports by using Routing and Remote Access.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Windows 2000 automatically creates five PPTP and five L2TP ports.

The number of virtual ports is not limited by physical hardware as it is with modems.

When you start Routing and Remote Access for the first time, Windows 2000 automatically creates five PPTP and five L2TP ports. The number of virtual ports that are available to any remote access server is not limited to availability of hardware. You can increase or decrease the number of available VPN ports to a number that is appropriate for the bandwidth that is available to the remote access server.

Note If you select the **Virtual private network (VPN)** option in the Routing and Remote Access Setup wizard, Windows 2000 automatically creates 128 PPTP and 128 L2TP ports.

To configure VPN ports on the server:

1. In the console tree of Routing and Remote Access, open the **Properties** dialog box for **Ports**.
2. In the **Ports Properties** dialog box, select a device—for VPN ports, these will appear as **WAN Miniport (PPTP)** and **WAN Miniport (L2TP)**—and then click **Configure**.
3. In the **Configure Ports** dialog box, select the **Remote access (inbound)** check box to enable inbound VPN connections.
4. You can increase or decrease the number of virtual ports available on the server.
5. In the **Configure Device** and **Ports Properties** dialog boxes, click **OK**.

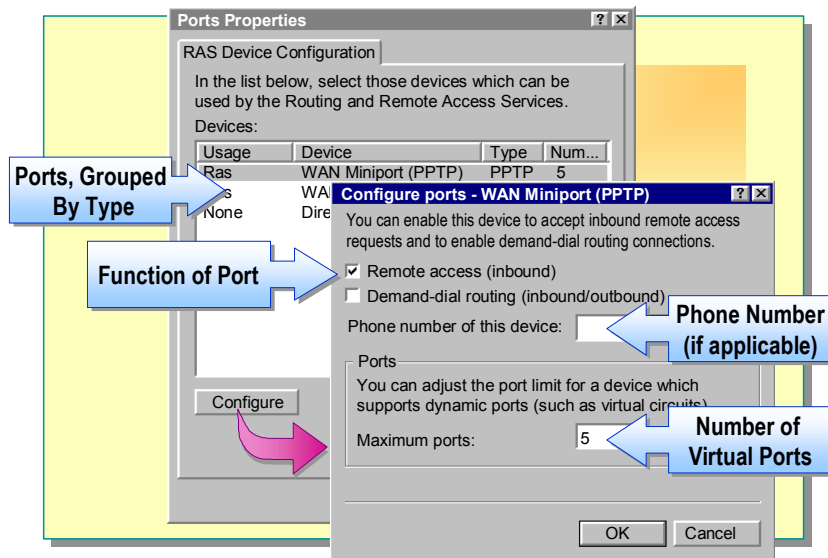
Configuring Modem and Cable Ports

Topic Objective

To illustrate the dialog boxes for configuring modem and cable ports.

Lead-in

Hardware ports are configured from the same location as virtual ports.



*****ILLEGAL FOR NON-TRAINER USE*****

When you start Routing and Remote Access for the first time, Windows 2000 automatically detects any modems that are installed and creates modem ports for them. Windows 2000 also creates ports for each parallel or serial cable connection that it detects. You can also configure these ports manually under **Ports** in the console tree of Routing and Remote Access.

To configure modem or cable ports on the server:

1. In the console tree of Routing and Remote Access, open the **Properties** dialog box for **Ports**.
2. In the **Ports Properties** dialog box, click a device, and then click **Configure**.

Modem, parallel, and serial ports are listed individually, but are grouped together and can be configured either individually or together. To configure several ports simultaneously, press CTRL while you click multiple ports, and then click **Configure**.

3. In the **Configure Ports** dialog box, select the **Remote access (inbound)** check box to enable inbound connections.
4. If you are configuring a modem port, type a telephone number.
5. In the **Configure Ports** and **Ports Properties** dialog boxes, click **OK**.

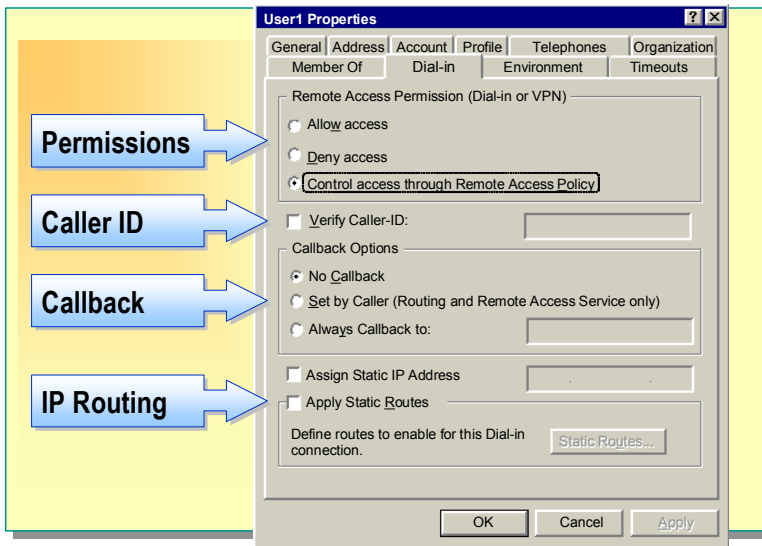
Configuring User Dial-in Settings

Topic Objective

To illustrate the locations of user dial-in settings.

Lead-in

You must also configure users' dial-in properties for remote access to work correctly.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Open the **Properties** dialog box for a user to illustrate the location of the dial-in settings.

On a stand-alone server, you configure the dial-in settings on the **Dial-in** tab in the **Properties** dialog box for a user account in Local Users and Groups. For an Active Directory™ directory service–based server, you configure the dial-in settings on the **Dial-in** tab in the **Properties** dialog box for a user account in Active Directory Users and Computers.

Key Point

All of the settings on this tab must be in agreement with the settings in the policy's profile and the conditions of the connection attempt. These settings should be used with caution if used in conjunction with remote access policies.

Setting Remote Access Permissions

The **Remote Access Permission** settings offer the options to **Allow access**, **Deny access**, or **Control access through Remote Access Policy**. If access is explicitly allowed, remote access policy conditions, user account properties, or profile properties can still deny the connection attempt. The **Control access through Remote Access Policy** option is only available on user accounts for stand-alone Windows 2000–based remote access servers or members of a Windows 2000 domain in native mode.

Enabling Caller ID Verification

If the **Verify Caller-ID** option is enabled, the server verifies the caller's telephone number. If the caller's telephone number does not match the configured telephone number, the connection attempt is denied.

All parts of the connection must support caller ID. Caller ID support on the remote access server consists of caller ID answering equipment and the driver that passes caller ID information to Routing and Remote Access. If you configure a caller ID setting for a user and you do not have the driver for passing the caller ID information from the caller to Routing and Remote Access, the connection attempt will be denied.

Setting Callback Options

If the callback property is enabled, the server calls back a specific telephone number (set by the caller or by the network administrator) during the connection process.

Assigning a Static IP Address

If the **Assign Static IP Address** option is enabled, Windows 2000 assigns a specific IP address to the user when a connection is made.

Applying Static Routes

If the **Apply Static Routes** option is enabled, the network administrator defines a series of static IP routes that are added to the routing table of the remote access server when a connection is made. This setting is designed for use with demand-dial routing.

Important If a remote access server is a member of a Windows NT version 4.0 domain or a Windows 2000 domain in mixed mode, only the **Allow access** and **Deny access** options (under **Remote Access Permission**) and the **Callback Options** dial-in settings are available. You can also use User Manager for Domains in Windows NT to grant or deny dial-in access and set callback options.

◆ Configuring Outbound Connections

Topic Objective

To identify the types of outbound connections that are configured in Windows 2000.

Lead-in

There are four general types of outbound connections that you configure in Windows 2000. Any outbound connection can be configured quickly and easily with the Network Connection wizard.

- Exploring Hardware Options
- Creating a Dial-up Connection
- Connecting to a Virtual Private Network
- Connecting Directly Through a Cable

*****ILLEGAL FOR NON-TRAINER USE*****

Outbound connections are connections made from a client to a server. Although it is possible for a computer running Windows 2000 Server to be a client, clients are typically computers running Windows 2000 Professional.

There are three basic types of outbound connections:

- Dial-up connections, which include:
 - Connections to a private network or server. This can include connections to a stand-alone computer in someone's home or a modem pool in a corporate intranet.
 - Connections to an ISP.
- Connections to a VPN.
- Direct connections to another computer through a cable.

You configure all outbound connections in Windows 2000 by using the Network Connection wizard. Much of the work of configuring protocols and services is automated when you use this process. Understanding the options in the wizard will help you configure connections efficiently.

Tip Connection Manager provides a graphical user interface so that your customers can connect to your service by using connection features and telephone numbers that you define. The Connection Manager Administration Kit (CMAC) wizard simplifies the customization process because you can use it to specify custom elements for your service, such as dial-up locations, telephone numbers, and VPN settings. It then builds a customized installation package for you.

For more information about using Connection Manager and creating customized profiles with the CMAC wizard, see Windows 2000 Server Help.

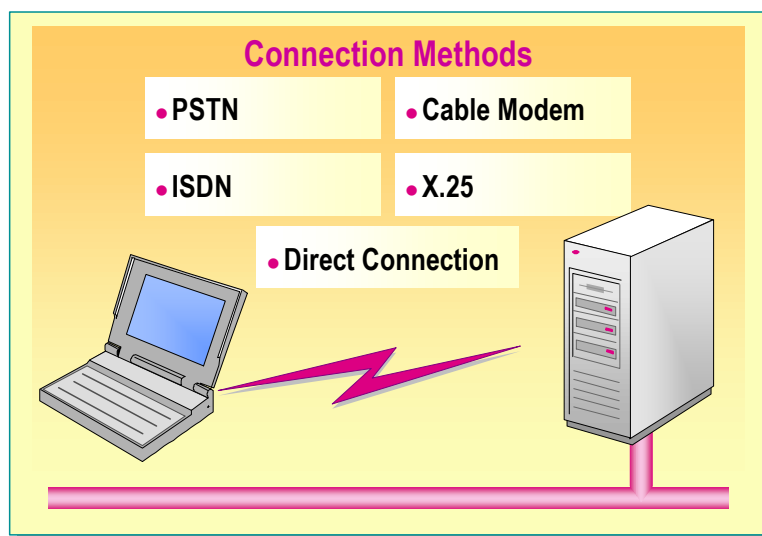
Exploring Hardware Options

Topic Objective

To illustrate the connectivity options that Windows 2000 includes for remote access.

Lead-in

Routing and Remote Access supports PSTN, ISDN, cable modems, X.25, and direct connections.



*****ILLEGAL FOR NON-TRAINER USE*****

You can connect remote access clients to a remote access server by using any of several types of hardware. Windows 2000 supports connections over the Public Switched Telephone Network (PSTN), ISDN lines, cable modems, an X.25 network, or direct cable connections. When selecting a hardware type to use for remote access, you should consider the advantages and disadvantages of each type of hardware.

Hardware type	Advantages	Disadvantages
PSTN	Universal availability; inexpensive modems; higher speeds available with DSL	Toll charges; low speeds unless using DSL; DSL is not available in all locations and requires expensive modems
ISDN	Faster than most PSTN connections; dedicated lines; wide availability in urban areas	Low speeds compared with DSL or cable modems; expensive adapters
Cable modem	Very fast connections	Lower availability; expensive modems
X.25	Secure, dedicated network	Expensive adapters
Direct connection (parallel cables, serial cables, or infrared sensors)	Simple, secure, dedicated connection; inexpensive cables	Distance between computers limited to length of cable or infrared sensor range

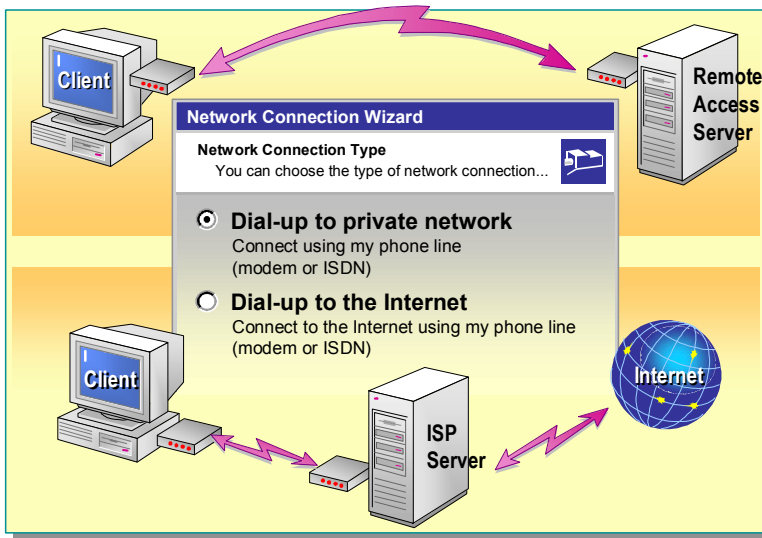
Creating a Dial-up Connection

Topic Objective

To illustrate two types of dial-up connections.

Lead-in

You can use the Network Connection wizard to create and configure an outbound dial-up connection.



*****ILLEGAL FOR NON-TRAINER USE*****

You can use the Network Connection wizard to create and configure an outbound dial-up connection either to a private network or to an ISP.

To create a new outbound connection:

Delivery Tip

Demonstrate how to create these connections with the wizard.

1. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**.
2. In Network and Dial-up Connections, double-click **Make New Connection**.
3. In the Network Connection wizard, click **Next**, and then click either **Dial-up to private network** or **Dial-up to the Internet**.
4. Do one of the following:
 - If you clicked **Dial-up to private network**, type the telephone number of the computer to which you are connecting. This may be an ISP for an Internet connection or the modems for your private network.
 - If you clicked **Dial-up to the Internet**, the Internet Connection wizard will start. Complete this wizard to create the connection.
5. If you want this connection to be made available to all users of this computer, click **For all users**, and then click **Next**. If you want to reserve the connection for yourself, click **Only for myself**, and then click **Next**.
6. If you clicked **Only for myself** in the previous step, proceed to the last step. If you clicked **For all users**, and you want to enable other computers to gain access to external resources through this dial-up connection, select the **Enable Internet Connection Sharing for this connection** check box.
7. By default, selecting shared access also enables on-demand dialing. If you want to prevent other computers from automatically dialing this connection, clear the **Enable on-demand dialing** check box, then click **Next**.
8. Type a name for the connection, and then click **Finish**.

Key Point

Explain the difference between sharing the connection and providing shared access. The first relates to the connection icon, and the second refers to the resources that the connection accesses.

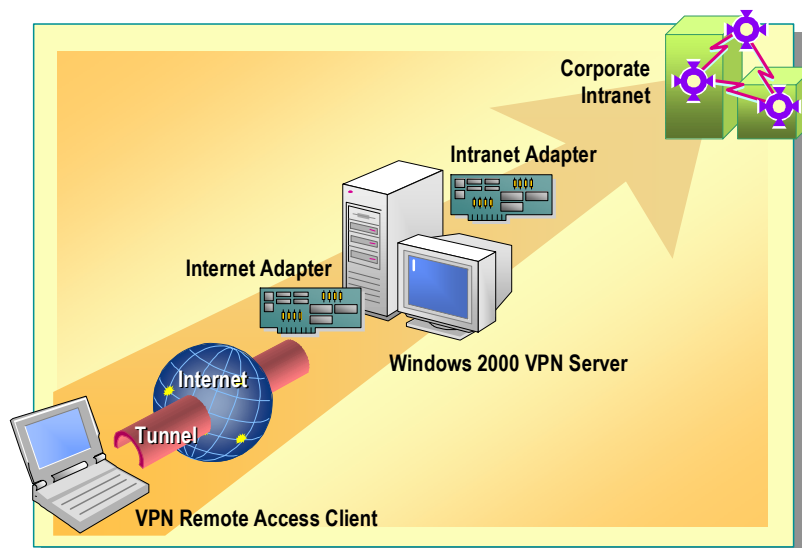
Connecting to a Virtual Private Network

Topic Objective

To illustrate the concept of a VPN.

Lead-in

You can use the Network Connection wizard to create a connection to a VPN, by specifying the initial connection and the host name or address of the VPN server.



*****ILLEGAL FOR NON-TRAINER USE*****

You can also use the Network Connection wizard to create a connection to a VPN. To create a new VPN connection:

1. In Network and Dial-up Connections, double-click **Make New Connection**.
2. In the Network Connection wizard, select **Connect to a private network through the Internet**, click **Next**, and then do one of the following:
 - If you must establish a connection with your ISP or some other network before connecting to the VPN, click **Automatically dial this initial connection**, click a connection on the list, and then click **Next**.
 - If you do not want to establish an initial connection automatically, click **Do not dial the initial connection**, and then click **Next**.
3. Type the host name or IP address of the computer to which you are connecting, and then click **Next**.
4. If you want this connection to be made available to all users of this computer, click **For all users**, and then click **Next**. If you want to reserve the connection for yourself, click **Only for myself**, and then click **Next**.
5. If you selected **Only for myself** in the previous step, proceed to the last step. If you selected **For all users**, and you want to enable other computers to gain access to external resources through this dial-up connection, select the **Enable Internet Connection Sharing for this connection** check box.
6. By default, selecting shared access also enables on-demand dialing. If you want to prevent other computers from automatically dialing this connection, clear the **Enable on-demand dialing** check box, and then click **Next**.
7. Type a name for the connection, and then click **Finish**.

Key Point

Mention that to be presented with the option to dial an initial connection, an initial connection icon must already exist.

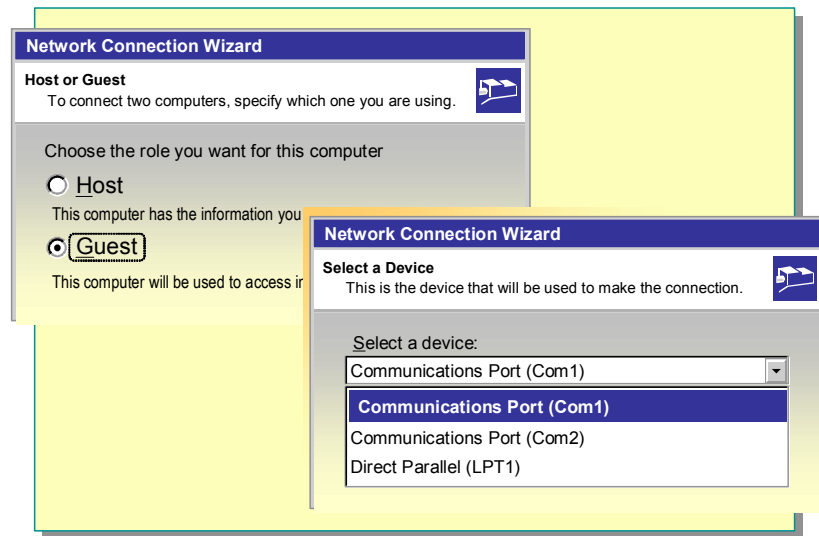
Connecting Directly Through a Cable

Topic Objective

To illustrate key pages in the Network Connection wizard for establishing a direct connection.

Lead-in

You can also use the Network Connection wizard to create a direct (cable) connection to another computer, unless you are a member of a domain and want to host a direct connection.



*****ILLEGAL FOR NON-TRAINER USE*****

You can use the Network Connection wizard to create a direct (cable or infrared) connection to another computer. However, if you are a member of a domain and want to host a direct connection, use Routing and Remote Access instead of configuring the port as you would for a modem port.

To create a direct connection to another computer:

1. In Network and Dial-up Connections, double-click **Make New Connection**.
2. In the Network Connection wizard, click **Connect directly to another computer**, click **Next**, and then do one of the following:
 - If your computer will be the host for the connection, click **Host**, and then click **Next**.
 - If your computer will be the guest for the connection, click **Guest**, and then click **Next**.
3. Choose the port that is connected to the other computer, and then click **Next**.
4. If you want this connection to be made available to all users of this computer, click **For all users**, and then click **Next**. If you want to reserve the connection for yourself, click **Only for myself**, and then click **Next**.
5. If you clicked **Only for myself** in the previous step, proceed to the next step. If you clicked **For all users**, and you want to enable other computers to gain access to resources through this dial-up connection, select the **Enable shared access for this connection** check box, and then click **Next**.
6. Type a name for the connection, and then click **Finish**.

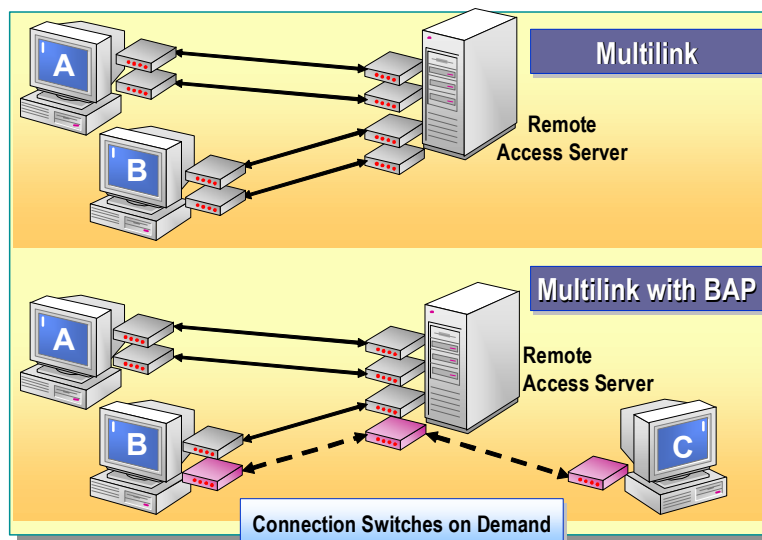
Configuring Multilink Connections

Topic Objective

To illustrate the dynamic linking function of BAP.

Lead-in

BAP allows Multilink servers to dynamically reallocate hardware resources where more bandwidth is needed.



*****ILLEGAL FOR NON-TRAINER USE*****

Multilink allows users to combine analog modem paths, ISDN paths, and even mixed analog and digital communications links on client and server computers. Multilinking combines multiple physical links into a logical bundle to increase bandwidth.

Multilink enables your computer to use two or more communications ports as if they were a single port of greater bandwidth. This means that if you use two modems to connect to the Internet, you can connect at double the speed of a single modem. For example, a computer with four modems operating at 33.6 kilobits per second (Kbps), and a telephone line for each modem, can connect to a remote access server with multiple modems and maintain a sustained transfer rate of 134.4 Kbps. Four 128-Kbps ISDN lines would return a throughput rate of 512 Kbps. To dial multiple devices, your connection and your remote access server must both have Multilink enabled.

The Multilink feature in Routing and Remote Access uses the PPP Multilink protocol. Windows 2000 also supports the Bandwidth Allocation Protocol (BAP) for dynamic multilinking.

PPP Multilink

The PPP Multilink protocol combines the bandwidth of two or more communication lines to create a single virtual data connection, providing scalable bandwidth based on the volume of data. Routing and Remote Access can use Multilink over multiple modems, ISDN, or X.25 cards. Both the client and remote access server must have Multilink enabled.

BAP

BAP enhances Multilink by dynamically adding or dropping links on demand. BAP is especially valuable to operations that have carrier charges based on bandwidth utilization. BAP is a PPP control protocol that works with PPP to provide bandwidth on demand.

Note For more information about Multilink, see RFC 1990, and for more information about BAP, see RFC 2125 under **Additional Reading** on the Web page on the Student Materials compact disc.

Configuring Multilink and BAP on the Remote Access Server

You can enable the PPP Multilink and BAP protocols on a serverwide basis on the **PPP** tab in the **Properties** dialog box for each remote access server. Select the **Multilink connections** and **Dynamic bandwidth control (BAP/BACP)** check boxes to enable PPP Multilink and BAP, respectively. This is the only configuration necessary for the server to accept Multilink connections.

Configuring Multilink on the Remote Access Client

To configure an outbound connection with multiple devices:

1. Right-click the connection on which you want to enable the dialing of multiple devices, and then click **Properties**.
2. On the **General** tab, select the check boxes for all the devices that you want the connection to use.
3. On the **Options** tab, in **Multiple devices**, do one of the following:
 - a. If you want Windows 2000 to dial only the first available device, click **Dial only first available device**, and then click **Configure**.
 - b. If you want Windows 2000 to use all of your devices, click **Dial all devices**, and then click **Configure**.
 - c. If you want Windows 2000 to dynamically dial and hang up devices as needed, click **Dial devices only as needed**, and then click **Configure**.
 - i. In the **Automatic Dialing and Hanging Up** dialog box, click the **Activity at least** percentage and **Duration at least** time that you want to set. Another line is dialed when connection activity reaches this level for the amount of time that you specify.
 - ii. In the **Automatic hangup** dialog box, click the **Activity no more than** percentage and **Duration at least** time that you want to set. A device is hung up when connection activity decreases to this level for at least the amount of time that you specify, and then click **OK**.
4. Click **OK**.

Lab A: Configuring a VPN Connection

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create a VPN connection.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Install Routing and Remote Access.
- Configure Routing and Remote Access to allow incoming VPN connections.
- Configure and test an outgoing VPN connection by using the Network Connection wizard.

Prerequisite

Before working on this lab, you must be familiar with remote access concepts and VPN concepts.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller
- A static IP address and subnet mask
- A lab partner with a similarly configured computer

You will also need the following information. If you are unsure about any of these values, please ask your instructor.

Number	Record value here
Your student number	x=
Your partner's student number	y=
Your classroom number (usually 1)	z=

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

Your company, Northwind Traders, has employees that travel to remote locations. You do not have the resources to set up a worldwide network to allow dial-up connections to these locations, so you are going to configure a VPN server on the Internet and allow your staff to connect to your network through the VPN connection.

Estimated time to complete this lab: 45 minutes

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Exercise 1

Configuring Inbound VPN Connections

Scenario

The sales staff at Northwind Traders has started traveling to remote locations. Although the traveling sales force will have access to the Internet at all of the remote locations, they still need access to your network for demonstration purposes. You need to enable secure remote access to your network over the Internet for these traveling users.

Goal

In this exercise, you will set up Routing and Remote Access, create VPN ports, and grant access permissions to the Administrator account for testing purposes.

Tasks	Detailed Steps
1. Install Routing and Remote Access. Use the Configuration wizard to configure the remote access server with the following values: For the IP address, use 10.x.0.10 (where <i>x</i> is your student number). Address range: 5 addresses.	a. Log on as <code>administrator@domain.nwtraders.msft</code> (where <i>domain</i> is the name of your domain) with a password of password. b. Open Routing and Remote Access from the Administrative Tools menu. c. In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Configure and Enable Routing and Remote Access. d. In the Routing and Remote Access Server Setup wizard, click Next. e. On the Common Configurations page, click Remote access server, and then click Next. f. On the Remote Client Protocols page, click Next. g. On the Network Selection page, under Name, verify that Classroom is selected, and then click Next. h. On the IP Address Assignment page, click From a specified range of addresses, and then click Next. i. On the Address Range Assignment page, click New. j. In the Start IP address box, type 10.x.0.10 (where <i>x</i> is your student number), and then in the Number of addresses box, type 5. k. Click OK, and then click Next. l. On the Managing Multiple Remote Access Servers page, verify that No, I don't want to set up this server to use RADIUS now is selected, click Next, and then click Finish. m. Click OK to close the Routing and Remote Access message box, and then close Routing and Remote Access.

(continued)

Tasks	Detailed Steps
2. Grant dial-in permissions to the Administrator account.	- Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand <i>domain</i> (where <i>domain</i> is the name of your domain), click Users, and then in the details pane, double-click Administrator. - On the Dial-in tab, verify that Allow access is selected, and then click OK. - Close Active Directory Users and Computers.

Exercise 2

Configuring and Testing Outbound VPN Connections

Scenario

To verify that remote access works for the traveling users, you need to connect to the remote access server that you have installed and configured.

Goal

In this exercise, you will create and test a VPN connection to your partner's remote access server.

Tasks	Detailed Steps
 Both partners must complete the previous procedure before either partner can continue.	
1. Use the Network Connection wizard to configure a VPN connection to your partner's computer. Area Code: Location area code. Network Connection Type: Connect to a private network through the Internet. Destination Address: 192.168.z.y (where z is your assigned classroom number and y is your partner's student number). Connection Availability page: Only for myself .	a. Right-click My Network Places , and then click Properties . b. In Network and Dial-up Connections, double-click Make New Connection . c. On the Location Information page, type an area code, click OK , and then click OK to close the Phone And Modem Options dialog box. d. In the Network Connection wizard, click Next . e. On the Network Connection Type page, click Connect to a private network through the Internet , and then click Next . f. On the Destination Address page, type 192.168.z.y (where z is your assigned classroom number and y is your partner's student number), and then click Next . g. On the Connection Availability page, click Only for myself , click Next , and then click Finish .
2. Initiate a connection to your partner's computer, logging on as Administrator.	a. In the Connect Virtual Private Connection dialog box, verify that the user name is Administrator , and in the Password box, type password and then click Connect .  <i>After connecting to your partner's computer, a message appears indicating that Virtual Private Connection is connected. Notice that there is an icon in the system tray representing the new connection.</i> b. Click OK to close the "Connection Complete" message. c. Close Network and Dial-up Connections.

(continued)

Tasks	Detailed Steps
3. Use the Ipconfig utility to verify that you have established a VPN connection and received an IP address for that connection.	a. At a command prompt, type ipconfig and then press ENTER.  Notice that there are four network adapters: the Classroom network adapter, the PartnerNet network adapter, the remote access server connection, and the Virtual Private Network connection. The IP address for the VPN connection was assigned from the static address pool on your partner's computer. b. Close the command prompt window.
4. Close the connection.	a. In the system tray, double-click the Connection icon. b. In the Virtual Private Connection Status dialog box, click Disconnect. c. Close all open windows.

◆ Configuring Authentication Protocols

Topic Objective

To list topics relevant to authentication protocols.

Lead-in

There are several different protocols that can be used to authenticate users on your network.

- **Standard Authentication Protocols**
- **Extensible Authentication Protocols**

*****ILLEGAL FOR NON-TRAINER USE*****

Remote access servers use authentication to determine the identity of users attempting to connect to the network remotely. After a user is authenticated, the user receives the appropriate access permissions and is allowed to connect to the network.

The correct and secure authentication of user accounts is critical for the security of a network. Without authentication, a potentially large number of unauthorized users can access your network.

Routing and Remote Access uses several protocols to perform authentication, and also allows for the use of Extensible Authentication Protocols, through which you can load third-party protocols.

Standard Authentication Protocols

Topic Objective

To list the level of security and appropriate use of standard authentication protocols.

Lead-in

Windows 2000 supports many different standard authentication protocols, some of which are more secure than others.

Protocol	Security	Use when
PAP	<i>Low</i>	The client and server cannot negotiate using more secure validation
SPAP	<i>Medium</i>	Connecting a Shiva LANRover and Windows 2000-based client or a Shiva client and a Windows 2000-based remote access server
CHAP	<i>Medium</i>	You have clients that are not running Microsoft operating systems
MS-CHAP	<i>High</i>	You have clients running Windows NT version 4.0 and later or, Microsoft Windows 95 and later
MS-CHAP v2	<i>High</i>	You have dial-up clients running Windows 2000, or VPN clients running Windows NT 4.0 or Windows 98

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 supports many different authentication protocols that have varying levels of security. You enable standard authentication protocols in Routing and Remote Access by selecting the appropriate check boxes on the **Security** tab in the **Properties** dialog box for the remote access server. Only those protocols that you select on this tab can be used to authenticate users to the remote access server.

PAP

The Password Authentication Protocol (PAP) uses clear-text passwords. If the passwords match, the server grants access to the remote access client. This protocol provides little protection against unauthorized access.

SPAP

The Shiva Password Authentication Protocol (SPAP) is a two-way reversible encryption mechanism employed by Shiva, a hardware manufacturer. SPAP encrypts the password data that is sent between the client and server and is, therefore, more secure than PAP.

CHAP

The Challenge Handshake Authentication Protocol (CHAP) (also known as Message Digest 5 [MD5]–CHAP) is a challenge-response authentication protocol. CHAP uses the industry-standard MD5 one-way encryption scheme to encrypt the response, providing a medium level of protection against unauthorized access. The authentication process works as follows:

1. The remote access server sends a challenge—consisting of a session identifier and an arbitrary challenge string—to the remote access client.
2. The remote access client sends a response that contains the user name and a one-way encryption of the challenge string, the session identifier, and the password.
3. The remote access server checks the response, and, if valid, allows the connection.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a one-way, encrypted password authentication protocol. If the server uses MS-CHAP as the authentication protocol, it can use Microsoft Point-to-Point Encryption (MPPE) to encrypt data to the client or server. On a remote access server running Windows 2000, MS-CHAP is enabled by default.

MS-CHAP v2

A new version of MS-CHAP, MS-CHAP v2, is available. This new protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving.

For VPN connections, Windows 2000 Server offers MS-CHAP v2 before offering MS-CHAP. Windows 2000 dial-up and VPN connections can use MS-CHAP v2. Computers running Windows NT 4.0 and Microsoft Windows 98 can use MS-CHAP v2 authentication for VPN connections only.

Selecting Authentication Protocols

The following table describes the situations in which you use these protocols.

Protocols	Security	Use when
PAP	Low	The client and server cannot negotiate by using a more secure form of validation.
SPAP	Medium	Connecting to a Shiva LanRover, or when a Shiva client connects to a Windows 2000–based remote access server.
CHAP	Medium	You have clients that are not running Microsoft operating systems.
MS-CHAP	High	You have clients running Windows 2000, Windows NT 4.0, or Microsoft Windows 95 or later.
MS-CHAP v2	High	You have dial-up clients running Windows 2000, or VPN clients running Windows NT 4.0 or Windows 98. MS-CHAP v2 is the most secure form of authentication.

Extensible Authentication Protocols

Topic Objective

To list the key points related to the EAP protocol.

Lead-in

EAP is designed to provide proprietary and future authentication methods.

- **Allows the Client and Server to Negotiate the Authentication Method That They Will Use**
- **Supports Authentication by Using**
 - MD5-CHAP
 - Transport Layer Security
 - Additional third-party authentication methods
- **Ensures Support of Future Authentication Methods Through an API**

*****ILLEGAL FOR NON-TRAINER USE*****

The Extensible Authentication Protocol (EAP) allows for customized authentication to remote access servers. The client and the remote access server negotiate the exact authentication method to be used. EAP supports authentication by using:

- *MD5-CHAP*. This protocol encrypts user names and passwords with an MD5 algorithm.
- *Transport Layer Security*. Transport Layer Security (TLS) is used for smart card (and other) intermediary security devices. Smart cards require a card and reader. The smart card electronically stores the user certificate and private key.
- *Additional, third-party authentication methods*. EAP allows vendors to add their own authentication methods, such as token cards. Token cards are physical cards that provide passwords and may use several authentication methods, including the use of codes that change with each use.

Through the use of the EAP application programming interfaces (APIs), independent software vendors can supply new client and server authentication methods for technologies such as token cards, smart cards, biometric hardware (such as retina or fingerprint scanners), and authentication technologies that are not yet developed.

To enable EAP authentication, open **Routing and Remote Access**, right-click your server, and then click **Properties**. The configuration settings are on the **Security** tab. You enable and configure specific EAP types on the **Authentication** tab of the **Edit Dial-in Profile** dialog box for the remote access policy.

Note For more information about EAP, see RFC 2284 and RFC 2716 under **Additional Reading** on the Web page on the Student Materials compact disc.

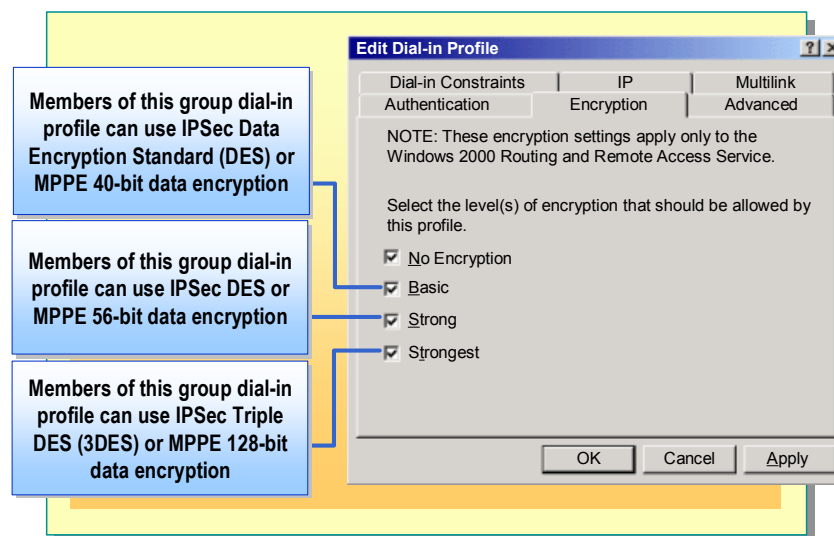
Configuring Encryption Protocols

Topic Objective

To illustrate the concept of an IPSec operation.

Lead-in

IPSec ensures secure communication over an IP network by using encryption.



*****ILLEGAL FOR NON-TRAINER USE*****

Data encryption provides security by encrypting, or encoding, data that is sent between a remote access client and a remote access server. For installations that require the highest degree of security, the administrator can set the server to force encrypted communications. Clients connecting to that server must encrypt their data or the server will refuse their connection.

You enable encryption protocols on the **Encryption** tab in the **Edit Profile** dialog box for the remote access policy.

Important Data encryption is only available if you use MS-CHAP (v1 or v2) or TLS (an EAP protocol) as the authentication protocol.

There are two methods of encrypting the data that is transmitted over a Windows 2000 remote access connection: MPPE and IPSec.

Encrypting Data by Using MPPE

MPPE encrypts data that moves between a PPTP connection and the VPN server. It has three levels of encryption: strongest (128-bit), strong (56-bit), and basic (40-bit) schemes.

Note For 128-bit encryption, you must download the Windows 2000 high encryption pack from the Windows Update Web site.

Encrypting Data by Using IPSec

IPSec is a framework of open standards for ensuring secure private communications over IP networks by using encryption. IPSec provides aggressive protection against private network and Internet attacks. IPSec is also easy to use. Clients negotiate a security association that acts as a private key to encrypt the data flow.

You use IPSec policies to configure IPSec security services. IPSec security services provide protection for most types of network traffic. Your network security administrator can configure IPSec policies to meet the security requirements of a user, group, application, domain, site, or global enterprise network.

You create and manage IPSec policies by using IP Security Policy Management, which is a snap-in that you can add to Microsoft Management Console (MMC).

Note For more information about configuring IPSec policies, see module 6, “Configuring Network Security by Using IPSec,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

◆ Configuring Routing and Remote Access for DHCP Integration

Topic Objective

To introduce the topics related to configuring Routing and Remote Access for DHCP integration.

Lead-in

You can configure the DHCP server to assign IP addresses to remote access clients from an existing address pool.

- **Assigning IP Addresses to Remote Access Clients by Using DHCP**
- **Configuring Routing and Remote Access to Use DHCP**

*****ILLEGAL FOR NON-TRAINER USE*****

When you configure a remote access server to allow clients to connect to a corporate network by using dial-up networking, you select how clients will receive an IP address from one of the following options:

- *Static IP Address.* You configure the IP address on the client computer. When clients use preassigned IP addresses, you need to ensure that the IP address is valid for each network to which the client connects and that no other client uses the same address. Because of this, it is not recommended that you use static IP addresses for dial-up networking.
- *From a Range of IP Addresses.* A remote access server can assign an IP address from a range of addresses that you configure. If you choose this option, you need to ensure that you have a sufficient number of IP addresses allocated exclusively for the remote access server to assign to client computers.
- *From the DHCP Server.* A remote access server can obtain IP addresses from a DHCP server and assign the IP addresses to dial-up clients. This is the most versatile configuration, because you do not have to reserve IP addresses for use by dial-up clients, and you only need to maintain one address pool.

Note For more information about how dial-up clients obtain a subnet mask and addresses of DNS servers and WINS server, see the “DHCP Option Parameters” topic in the Windows 2000 Server Resource Kit.

Tip When using DHCP to obtain IP addresses for dial-up clients, you can reduce the number of required IP addresses by setting a short lease duration, such as one hour. Configuring a short lease duration allows you to support many dial-up clients while keeping the number of allocated IP addresses low. A remote access server only requires as many IP addresses as there are simultaneously connected clients.

Assigning IP Addresses to Remote Access Clients by Using DHCP

Topic Objective

To explain the implications of using DHCP to assign IP addresses to remote access clients.

Lead-in

The remote access server gets 10 IP address at a time from the DHCP server.

■ **If DHCP Server is Available**

Remote Access Server Obtains 10 IP Addresses at a Time

■ **If DHCP Server is Unavailable**

Remote Access Server Uses Automatic Private IP Addressing

*****ILLEGAL FOR NON-TRAINER USE*****

If the remote access server is configured to use DHCP to obtain IP addresses, the remote access server initially obtains 10 IP addresses from a DHCP server. The remote access server uses the first IP address obtained from DHCP for itself and allocates subsequent addresses to TCP/IP-based remote access clients as they connect. IP addresses that are released when remote access clients disconnect are reused. When all 10 IP addresses are used, the remote access server obtains 10 more. When the Routing and Remote Access service is stopped, all IP addresses obtained through DHCP are released.

If a DHCP server is not available when Routing and Remote Access is started, Automatic Private IP Addressing addresses in the range from 169.254.0.1 through 169.254.255.254 are used. Because this may prevent client computers from accessing computers on your network other than the remote access server, you should ensure that a DHCP server is always available.

The remote access server uses a specific LAN adapter to obtain DHCP-allocated IP addresses for remote access clients. The IP addresses that the remote access server receives are valid for the network segment to which the adapter is attached. You can select which adapter you want to use. By default, Routing and Remote Access randomly picks a LAN adapter to use. For a remote access server with multiple adapters, you should select the adapter that is connected to a network segment where DHCP-allocated addresses can be obtained.

Tip You can assign DHCP options to dial-up clients that differ from the options that you assign to clients that are directly connected to the network. To do this, use the Default Routing and Remote Access Class user class.

For more information about DHCP, see module 2, “Automating IP Address Assignment by Using DHCP,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

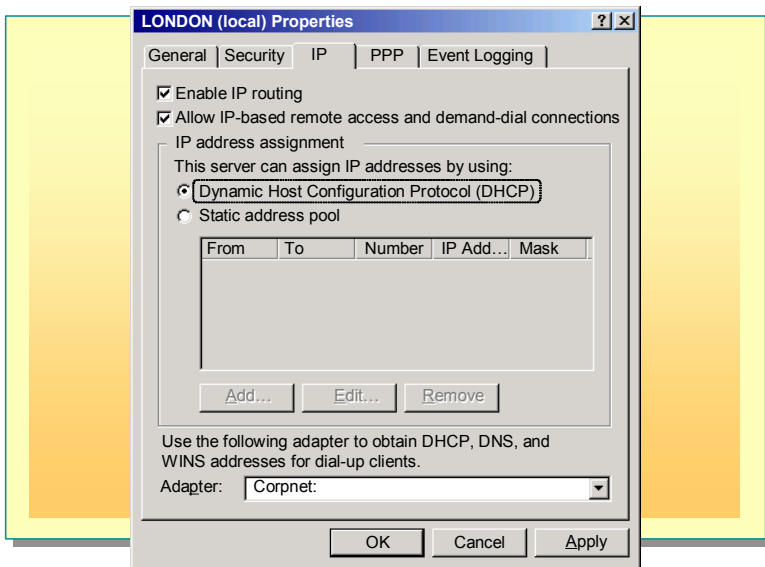
Configuring Routing and Remote Access to Use DHCP

Topic Objective

To illustrate configuration of Routing and Remote Access to obtain IP addresses from a DHCP server.

Lead-in

You can configure Routing and Remote Access to obtain IP addresses from the DHCP server.



*****ILLEGAL FOR NON-TRAINER USE*****

You can configure Routing and Remote Access to obtain IP addresses from a DHCP server.

To configure a remote access server to obtain IP addresses from a DHCP server:

1. Open Routing and Remote Access from the **Administrative Tools** menu.
2. Right-click the server name for which you want to view properties, and then click **Properties**.
3. In the **Properties** dialog box for the remote access server, on the **IP** tab, click **Dynamic Host Configuration Protocol (DHCP)**.
4. In the **Adapter** box, click the network adapter from which you want the remote access server to obtain IP addresses by using DHCP.
5. Click **OK**.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Examining Remote Access in Windows 2000
- Configuring Inbound Connections
- Configuring Outbound Connections
- Configuring Multilink Connections
- Configuring Authentication Protocols
- Configuring Encryption Protocols
- Configuring Routing and Remote Access for DHCP Integration

*****ILLEGAL FOR NON-TRAINER USE*****

1. What are the advantages of using L2TP rather than using PPTP?

L2TP supports more types of internetworks, supports header compression, and works with IPSec for encryption.

2. In the Network Connection wizard, you must configure two settings regarding sharing the connection and its associated resources. Describe the difference between these two settings.

The settings are whether you want to allow others who use the computer to use the connection (access to the connection) and whether you want to allow other computers to access resources through this port (sharing the connection after it is established).

3. Your organization has many employees that are connecting to your network by modems over the telephone system, but are requesting more bandwidth so that they can be more productive. High-speed connections such as ISDN and DSL are not currently available in your area. What can you do to increase bandwidth for people working remotely?

Configure multiple modems and telephone lines, and then allow Multilink connections to the server. The employees working remotely can then obtain more bandwidth by using multiple modems and combining them with the Multilink protocol.

4. People in your organization use a number of different operating systems to connect to your network by remote access. You want a remote access authentication protocol that is very secure but will allow all of your client operating systems to connect. What is the best authentication protocol to select?

CHAP—this protocol will work with a range of operating systems and uses industry-standard MD5 encryption to keep the passwords secure.

5. You are configuring a remote access server for your organization, and you want to make sure that users who are using the remote access server get only specified IP addresses, and that these addresses are always available to the remote access server. How can you do this?

Configure the remote access server to assign IP addresses from a range of IP addresses. That way, remote access users will not use an IP address from DHCP and will use a known range of addresses.

6. Help desk has received a call from a user who is dialing into your network by using remote access. The user connects successfully, but is unable to access any resources on the network. You ask the user to use Ipconfig to verify the IP address for the connection, and the user reports that she has an IP address of 169.254.5.23. What is a likely cause of this problem? Why?

A DHCP server is unavailable, so the remote access server is allocating IP addresses by using Automatic Private IP addressing. Because these addresses do not work with the IP address on your network, the user is unable to access resources on the network.

