MCSE EXAM MATERIAL

▶ Server
▶ Network

EXAM OBJECTIVES

Server ▶

Exam 70-215

- Install, configure, and troubleshoot a virtual private network (VPN).
- Configure, monitor, and troubleshoot remote access.
  - Configure inbound connections.
  - Create a remote access policy.
  - Configure a remote access profile.

Network ▶

Exam 70-216

- Configure and troubleshoot remote access.
  - Configure inbound connections.
  - Create a remote access policy.
  - Configure a remote access profile.
  - Configure a virtual private network (VPN).
  - Configure multilink connections.
  - Configure Routing and Remote Access for DHCP Integration.
- Manage and monitor remote access.
- Configure remote access security.
  - Configure authentication protocols.
  - Configure encryption protocols.
  - Configure a remote access policy.

CHAPTER

Managing Remote Access

17

This chapter is all about remote access in a Windows 2000 environment. Remote access is a critical networking function for today's highly mobile workforce. With remote access, users can connect to their company's network from home, from a hotel room, or from any computer connected to the Internet. The same service that provides routing functionality in Windows 2000 also provides remote access capability—the Routing and Remote Access service.

I'll begin by providing an overview of remote access, including a discussion of the remote access connection types, and the connection and transport protocols supported by the Routing and Remote Access Service. Then I'll show you how to enable remote access and how to configure the remote access server. I'll also explain how to add and configure inbound connection ports. Next, I'll show you how to control access to a remote access server by creating and using remote access policies.

Finally, I'll cover the tools you can use to monitor remote access and provide some tips for troubleshooting common remote access problems.

Chapter Pre-Test

1. What is a virtual private network (VPN) connection?
2. How do PPTP and L2TP differ from each other?
3. Which transport protocols are supported by the Routing and Remote Access service?
4. What is a multilink connection?
5. What kinds of ports are supported by the Routing and Remote Access service?
6. What is a remote access policy?

MCSE EXAM MATERIAL

Overview of Remote Access

Remote access is a feature that enables client computers to use dial-up and VPN connections to connect to a remote access server. (A *remote access server* is a Windows 2000 Server computer that runs the Routing and Remote Access service and is configured to provide remote access.) Once a connection with the remote access server is established, the client computer has access to the network the remote access server is connected to. Remote access enables users of remote computers to use the network as though they were directly connected to it. There is no difference in network functionality for the remote access client, except that the speed of the link is often much slower than a direct connection to the LAN.

Remote access is an important networking function in light of today's highly mobile workforce. With remote access, users can connect to their company's network from home, from a hotel room, from a client's remote office, or from any computer connected to the Internet.

The Routing and Remote Access service is a Windows 2000 Server service that enables a Windows 2000 Server computer to function both as a router and as a remote access server. I introduced you to this service in Chapter 16, where you learned all about the routing features of this service. In this chapter I'll tackle the other half of this service — remote access.

The Routing and Remote Access service is only available on Windows 2000 Server computers — in other words, it's not available on Windows 2000 Professional computers.

EXAM TIP

Remote access is a complex topic. Even administrators who manage remote access servers on a daily basis are well advised to study the details and nuances presented in this chapter before taking the Server or Network exam.

Client computers that run MS-DOS, Windows for Workgroups, Windows 95, Windows 98, Windows NT 4.0, and Windows 2000 can be configured as remote access clients of a Windows 2000 remote access server. In addition, any computer that supports the Point-to-Point Protocol (PPP) can connect to a Windows 2000 remote access server.

As implemented in Windows 2000, remote access supports multiple connection types, connection protocols, and transport protocols, as the following sections explain.

Remote Access Connection Types

Remote access client computers can connect to a Windows 2000 remote access server by using a variety of connection types, including:

- A standard telephone line (also called a Public Switched Telephone Network or PSTN) and modem
- A digital link
- ISDN
- X.25
- Virtual private network (VPN), including PPTP and L2TP

Probably the most common connection type is a standard analog telephone line and modem. This service is inexpensive and widely available.

A digital link is a new connection type in which the remote access server uses a digital connection to the public telephone system, and remote access clients connect to the remote access server by using V.90 modems. This connection type enables remote access clients to communicate at speeds of up to 33.6 Kbps, and enables the remote access server to communicate with its clients at speeds of up to 56 Kbps.

Integrated Services Digital Network (ISDN) is a digital, dial-up telephone service that supports faster data transmission rates than a standard analog telephone line. The standard ISDN connection is called an ISDN Basic Rate Interface (BRI) line. An ISDN BRI line consists of three separate data channels. Two of these channels (called B channels) support telephone or data communications at a rate of up to 64 Kbps. The third channel is called a D channel, and is used to establish and maintain the connection. If both B channels are used together, data transmission rates of up to 128 Kbps can be supported.

X.25 is a packet-switching protocol that is used on dial-up or leased lines. X.25 is available in most countries. An X.25 connection requires a fair amount of hardware, including an X.25 adapter card, with either a built-in or external Packet Assembler/Disassembler (PAD) in both the remote access server and the remote access client. In addition, access to an X.25 packet-switched network is required at both the remote access server and remote access client locations.

A virtual private network (VPN) is not a physical connection type. Rather, it's a virtual connection that is tunneled inside of an existing TCP/IP network connection. VPNs can be established by using either

PPTP or L2TP. Both of these protocols support encryption of the data sent over the VPN connection. Because a VPN uses an existing TCP/IP network connection, no additional hardware is required. VPN connections are commonly used between two computers that communicate over the Internet.

Connection Protocols Supported by Remote Access

Remote access in Windows 2000 can be carried out over several connection protocols. These protocols provide the data-link connectivity for remote access connections in much the same way as Ethernet or Token Ring provide the data-link connectivity on a local area network. Each of these protocols has different features and capabilities. The connection protocols Windows 2000 supports for remote access include: Point-to-Point Protocol (PPP), Point-to-Point Multilink Protocol, Point-to-Point Tunneling Protocol, Layer Two Tunneling Protocol (L2TP), Serial Line Internet Protocol (SLIP), and the Microsoft RAS protocol (also called AsyBEUI).

The *Point-to-Point Protocol (PPP)* is currently the industry standard remote connection protocol. PPP connections support multiple transport protocols, including TCP/IP, NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, AppleTalk, and NetBEUI.

The *Point-to-Point Multilink Protocol* is an extension of PPP. Point-to-Point Multilink Protocol combines the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, digital link, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support.

The *Point-to-Point Tunneling Protocol (PPTP)* permits a virtual private network (VPN) connection between two computers over an existing TCP/IP network connection. The existing TCP/IP network connection can be over the Internet, a local area network, or a remote access TCP/IP connection. All standard transport protocols are supported within the PPTP connection.

The *Layer Two Tunneling Protocol (L2TP)*, like PPTP, permits a VPN connection between two computers over an existing TCP/IP network connection. The major difference between PPTP and L2TP is that PPTP uses Microsoft Point-to-Point Encryption (MPPE) while L2TP uses IPSec for encryption. In addition, L2TP is rapidly becoming the industry standard tunneling protocol. Currently, only Windows 2000 remote access clients and remote access servers support L2TP.

TIP

If you plan to use L2TP VPN connections, you must install computer (machine) certificates on both the Windows 2000 remote access server and the remote access client. For more information on Certificate Services, see Chapter 18.

The *Serial Line Internet Protocol (SLIP)* is an older connection protocol commonly associated with UNIX computers. SLIP connections are only supported on the client side of the remote access connection—a Windows 2000 remote access server doesn't support incoming SLIP connections. The only transport protocol that SLIP supports is TCP/IP.

The *Microsoft RAS protocol* (also called *AsyBEUI*) is supported by the Windows 2000 Routing and Remote Access service to enable inbound connections from legacy client computers, including MS-DOS, Windows for Workgroups, and Windows NT 3.1. The only transport protocol that can be used with AsyBEUI is NetBEUI.

Transport Protocols Supported by Remote Access

All Windows 2000 standard transport protocols are supported by the Routing and Remote Access service. Remote access clients can connect to a Windows 2000 remote access server by using:

- TCP/IP
- IPX—including NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
- NetBEUI
- AppleTalk

The DLC protocol is not supported by remote access in Windows 2000.

Remote access clients can use one or more of these transport protocols on a remote access connection. For example, a client computer that needs to access a Windows 2000 Server and a NetWare server via a remote access server can use both TCP/IP and NWLink IPX/SPX/NetBIOS Compatible Transport Protocol during a single remote access connection.

A Windows 2000 remote access server can act as a router for remote access client computers that use TCP/IP, IPX, or AppleTalk, enabling these remote access clients to access other computers on the network. A Windows 2000 remote access server can also function as a NetBIOS gateway for remote access clients that use the NetBEUI protocol.

Enabling and Configuring Remote Access

The Routing and Remote Access Service is installed by default on all Windows 2000 Server (and Advanced Server) computers. However, remote access is not automatically enabled.

If you haven't enabled routing on your Windows 2000 Server computer, you can use the Routing and Remote Access Server Setup wizard to enable remote access.

If you have already enabled routing on your Windows 2000 Server computer, enabling remote access is as simple as selecting a check box in the server's Properties dialog box in Routing and Remote Access.

I'll show you how to use both of these methods to enable remote access.

STEP BY STEP

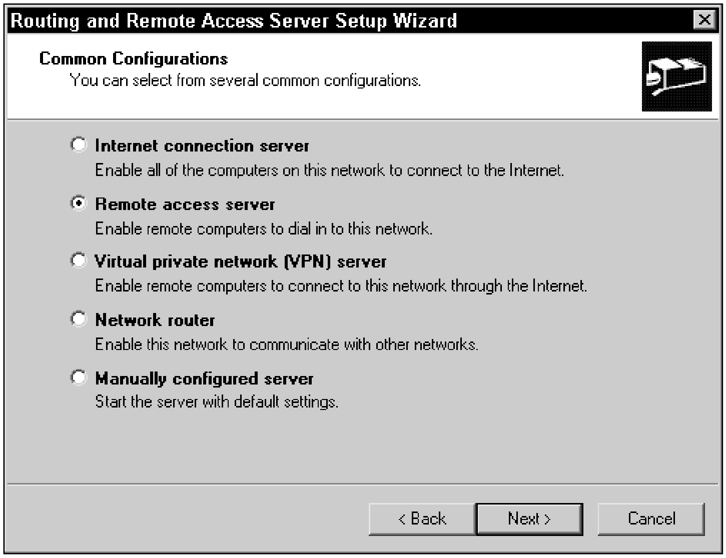
ENABLING REMOTE ACCESS WHEN ROUTING HAS NOT BEEN ENABLED

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, right-click the server on which you want to enable remote access and select "Configure and Enable Routing and Remote Access" from the menu that appears.
3. The Routing and Remote Access Server Setup wizard starts. Click Next.
4. The Common Configurations screen appears. Select the "Remote access server" option. Or, if this server will be used *only* for incoming VPN connections, select the "Virtual private network (VPN) server" option. Figure 17-1 shows this screen configured for a remote access server. Click Next.
5. In the Remote Client Protocols screen, verify that all network protocols required on the server are listed. Commonly listed protocols include TCP/IP, IPX, and AppleTalk.

   If you need to add additional protocols, select the "No, I need to add protocols" option. If you select this option, the wizard stops and directs you to install the necessary protocols in the `Network and Dial-up Connections` folder, and then to run this wizard again.

   If all the protocols you need are listed, accept the default option of "Yes, all of the available protocols are on this list." Click Next.
6. If your Windows 2000 Server computer has multiple network adapter cards installed, a list of the local area connections on this computer and their corresponding network adapters is displayed. Select the local area connection for which you want to enable remote access. Remote access clients will access resources on your LAN by using the selected local area connection. Click Next.

STEP BY STEP *Continued*



Routing and Remote Access Server Setup Wizard

Common Configurations
You can select from several common configurations.

○ **Internet connection server**
Enable all of the computers on this network to connect to the Internet.

● **Remote access server**
Enable remote computers to dial in to this network.

○ **Virtual private network (VPN) server**
Enable remote computers to connect to this network through the Internet.

○ **Network router**
Enable this network to communicate with other networks.

○ **Manually configured server**
Start the server with default settings.

FIGURE 17-1 Enabling remote access

7. In the IP Address Assignment screen, select the method you want to use for assigning IP addresses to remote access clients. Your choices are "Automatically" (this is the default setting), or "From a specified range of addresses." Select Automatically if you use a DHCP server on your network. Click Next.

TIP

If you choose to use a DHCP server to assign IP addresses to Remote Access clients, and the DHCP service is not installed on the Remote Access Server, you must install the DHCP Relay Agent on the Remote Access server to enable remote clients to receive IP Addresses from your DHCP server.

8. In the Managing Multiple Remote Access Servers screen, choose whether this remote access server will authenticate remote access clients directly, or will use a RADIUS server for client authentication. If you choose to use a RADIUS server, you will be prompted for a primary and alternate RADIUS server host name and for a shared secret password that this server will use to connect to the RADIUS server. Make your selection and click Next.
9. In the Completing the Routing and Remote Access Server Setup Wizard screen, click Finish.
10. If you chose to use a DHCP server for IP address assignments in Step 7, and this server is not a DHCP server, a warning dialog box appears, indicating that you must install and configure the DHCP Relay Agent on this server. (See Chapter 16 for information on installing and configuring this routing protocol.) Click OK.

STEP BY STEP *Continued*

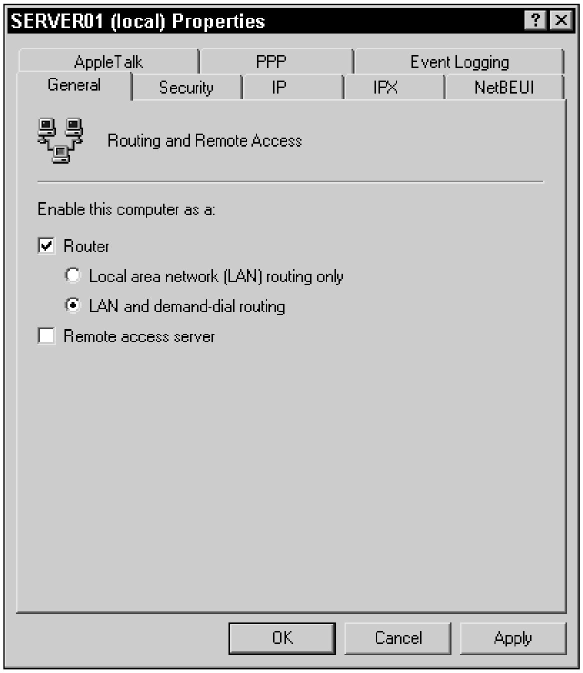
11. Windows 2000 starts the Routing and Remote Access service. Your Windows 2000 Server computer is now configured as a remote access server (or a VPN server). Close Routing and Remote Access.

If you have previously enabled routing on your Windows 2000 Server computer, the steps to enable remote access are much simpler.

STEP BY STEP

ENABLING REMOTE ACCESS WHEN ROUTING IS ENABLED

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, right-click the server on which you want to enable remote access and select Properties from the menu that appears.
3. The server's Properties dialog box appears, as shown in Figure 17-2. Select the check box next to "Remote access server." Click OK.



Routing and Remote Access

Enable this computer as a:

☑ Router

○ Local area network (LAN) routing only

● LAN and demand-dial routing

□ Remote access server

FIGURE 17-2 Enabling remote access when routing is already enabled

STEP BY STEP *Continued*

4. A Routing and Remote Access warning message appears, indicating that the router must be stopped and restarted. Click Yes.
5. Windows 2000 stops and restarts the Routing and Remote Access service. Close Routing and Remote Access.

Once remote access is enabled, you want to configure it, and you'll certainly want to add and configure inbound connection ports. I'll describe how to perform these tasks in the following sections.

Configuring the Properties of the Remote Access Server

Like many services in Windows 2000, Routing and Remote Access has its own administrative tool for configuring and managing the service. This tool is called Routing and Remote Access, and is accessed from the Administrative Tools menu. Alternately, you can access the Routing and Remote Access tool by using Computer Management. You can configure a Windows 2000 remote access server by accessing the server's Properties dialog box.

STEP BY STEP

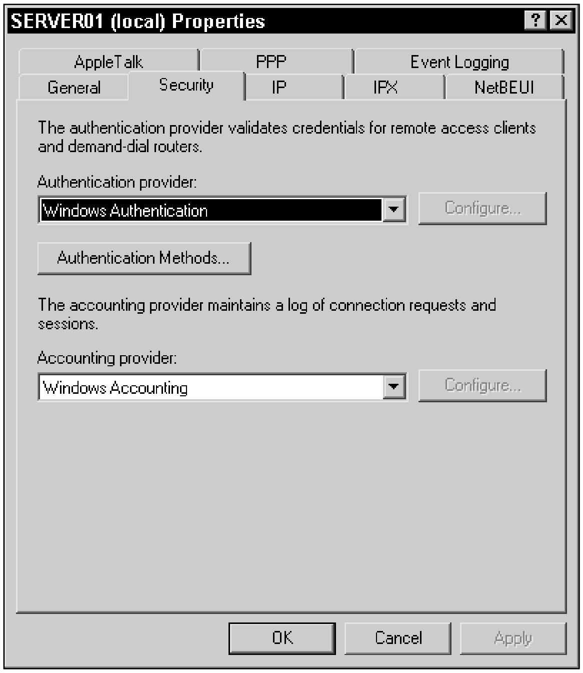
TO ACCESS A REMOTE ACCESS SERVER'S PROPERTIES DIALOG BOX

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, right-click the remote access server you want to configure, and select Properties from the menu that appears.
3. The remote access server's Properties dialog box is displayed. Figure 17-2 shows this dialog box. Once you access this dialog box, you can configure settings on its many tabs.

You can configure numerous properties of a Windows 2000 remote access server, including security options, settings for all transport protocols installed on the server, and event logging. I'll discuss each of these properties in the following sections.

Configuring Security

You can configure an authentication provider and an accounting provider on the Security tab in a Windows 2000 remote access server's Properties dialog box. You can also select the authentication methods this server will use. Figure 17-3 shows the Security tab.



SERVER01 (local) Properties

The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting

FIGURE 17-3 The Security tab

The first item you can configure on this tab is an authentication provider. An authentication provider determines if the remote user's credentials are valid, and whether the remote user has permission to connect to the remote access server. The possible choices in this drop-down list box are Windows Authentication and RADIUS Authentication.

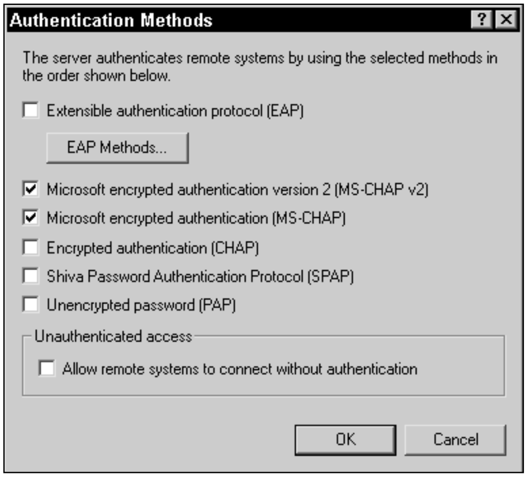
If Windows Authentication is selected, the Windows 2000 remote access server compares the user's name and password against information stored in the local user account database on the remote access server, or against information stored in Active Directory. Windows Authentication is the most commonly used authentication provider, and is always selected unless a RADIUS server is used.

If RADIUS Authentication is selected, this remote access server will use a specified RADIUS server to perform authentication of remote access clients. *RADIUS* (Remote Authentication Dial-In User Service) is an industry-standard authentication service. It is typically used by ISPs to maintain a centralized user accounts database. RADIUS is often used in an enterprise environment to provide centralized authentication and accounting services for multiple remote access servers. If you select RADIUS Authentication, you must configure this remote access server to use one or more RADIUS servers. To do this, click Configure.

Next, you need to select an accounting provider. An accounting provider logs all connection attempts and session activity on the remote access server. The possible choices in this drop-down list box are: None, Windows Accounting, and RADIUS Accounting.

If you don't want to track accesses and attempted accesses to the Windows 2000 remote access server, select None. Otherwise, select an accounting provider that *matches* the authentication provider you selected in the top part of this dialog box. If you select RADIUS Accounting, centralized accounting of activity on all remote access servers is maintained by the RADIUS server. If you select RADIUS Accounting, you must configure this remote access server to use one or more RADIUS servers. To do this, click Configure.

Finally, you can select the authentication methods that will be used by this remote access server to authenticate remote access clients. To select these methods, click Authentication Methods. Figure 17-4 shows the Authentication Methods dialog box. Notice that two versions of Microsoft encrypted authentication are selected by default.


Authentication Methods

The server authenticates remote systems by using the selected methods in the order shown below.

□ Extensible authentication protocol (EAP)

☑ Microsoft encrypted authentication version 2 (MS-CHAP v2)

☑ Microsoft encrypted authentication (MS-CHAP)

□ Encrypted authentication (CHAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Unencrypted password (PAP)

Unauthenticated access

□ Allow remote systems to connect without authentication

FIGURE 17-4 Selecting authentication methods

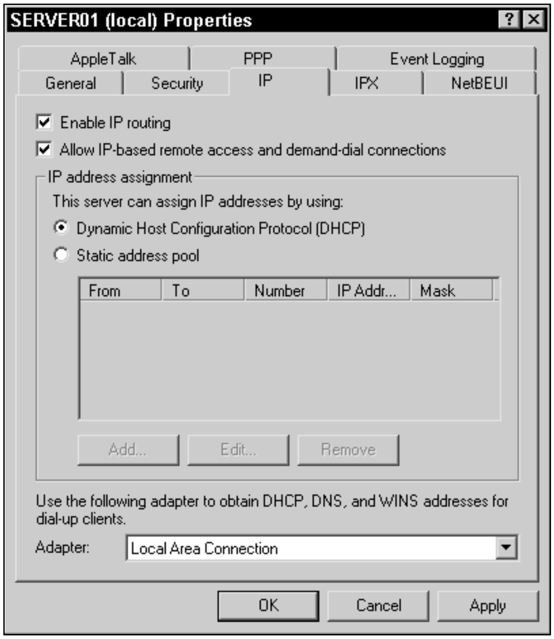
You can select one or more of the following authentication methods.

- **Extensible authentication protocol (EAP):** This protocol is designed to enable the remote access client and the remote access server to negotiate a common authentication method. EAP can be used with Transport Layer Security (TLS) to support the use of a smart card and PIN number to authenticate remote users. EAP can also be used with biometrics devices, such as a thumbprint reader.
- **Microsoft encrypted authentication version 2 (MS-CHAP v2):** This protocol uses a mutual authentication process that enables the remote access client to verify the server, and the remote access server to verify the client. This protocol causes the remote access server to send a challenge to the remote access client that includes a session key and a challenge key. Then the remote access client responds by encrypting and sending the remote user's name, password, session key, and challenge key to the remote access server. The remote access server (or RADIUS server) verifies the remote user's information and sends an authentication response back to the client. The client verifies the response, and completes the connection to the remote access server. Version 2 of Microsoft encrypted authentication is a more secure authentication method than the original version and provides stronger security.
- **Microsoft encrypted authentication (MS-CHAP):** This protocol causes the remote access server to send a challenge to the remote access client that includes a session key and a challenge key. Then the remote access client responds by sending the remote user's name in clear text format, and an encrypted version of the user's password, session key, and challenge key to the remote access server. The remote access server (or RADIUS server) verifies the remote user's information and authenticates the user.
- **Encrypted authentication (CHAP):** This protocol is similar to Microsoft encrypted authentication (MS-CHAP). However, it uses a different encryption scheme for passwords, called Message Digest 5 (MD5). This protocol is often used to support remote access clients that don't support MS-CHAP or MS-CHAP v2. If you select this authentication method, you must configure users to store their passwords in a reversibly encrypted form by configuring a password policy in Domain Security Policy or Group Policy.

- **Shiva Password Authentication Protocol (SPAP):** This provides support for remote users that use the Shiva LANRover client to connect to the remote access server. The protocol works similarly to CHAP but is generally less secure.
- **Unencrypted password (PAP):** This is a clear text credential exchange protocol that you should avoid unless the remote access client does not support any of the preceding encryption protocols, and security is not a major concern.
- **Allow remote systems to connect without authentication:** If you select this option, the remote access server is prevented from performing authentication — all remote access clients will be permitted to connect. This option is normally not recommended.

Configuring IP and DHCP Integration

You can configure several IP settings on the IP tab in a Windows 2000 remote access server's Properties dialog box. You can also configure the remote access server for DHCP integration on this tab. This tab is only available when TCP/IP is installed on the remote access server. Figure 17-5 shows the IP tab.



SERVER01 (local) Properties

☑ Enable IP routing

☑ Allow IP-based remote access and demand-dial connections

IP address assignment

This server can assign IP addresses by using:

● Dynamic Host Configuration Protocol (DHCP)

○ Static address pool

From	To	Number	IP Addr...	Mask

Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.

Adapter: Local Area Connection

FIGURE 17-5 The IP tab

The first item you can configure on this tab is a check box that enables IP routing on the remote access server. Select this check box to enable remote access clients to access services on the network (to which the remote access server is connected) by using TCP/IP. If you clear this check box (which is selected by default), remote access clients will only be able to use TCP/IP to access resources on the remote access server.

The next item you can configure on this tab is the "Allow IP-based remote access and demand-dial connections" check box. If you clear this check box (which is selected by default), remote access clients won't be able to use TCP/IP to connect to the remote access server.

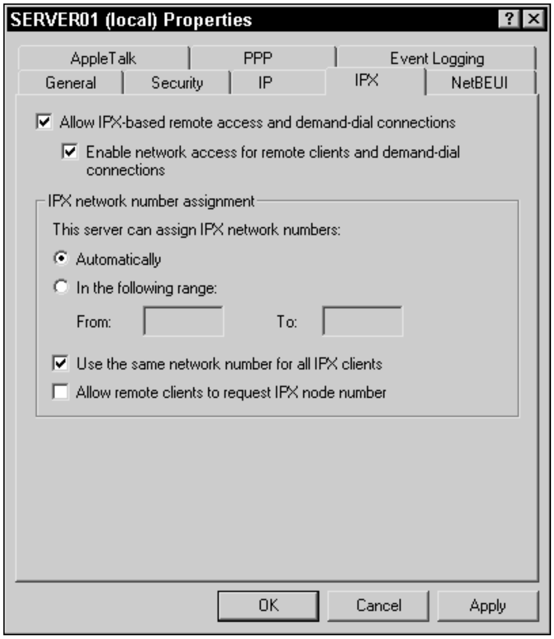
The next configuration option determines how the remote access server assigns IP addresses to remote access clients. If you select the Dynamic Host Configuration Protocol (DHCP) option, the remote access server will be configured for integration with the DHCP server on the network, and the DHCP server (not the remote access server) will automatically assign IP addresses to remote access clients. If you select this option and a DHCP server is not available when a remote access client connects, the remote access server will assign an IP address to the client by using the Windows 2000 automatic private IP addressing feature. If you select the "Static address pool" option, you can specify one or more ranges of IP addresses that the remote access server will use to assign to remote access clients.

Finally, in the Adapter drop-down list box, either select the Local Area Connection you want the remote access server to use to obtain DHCP, DNS, and WINS addresses for remote access clients, or select the option that enables the remote access server to automatically select a connection.

Configuring IPX

You can configure several IPX settings on the IPX tab in a Windows 2000 remote access server's Properties dialog box. This tab is only available when the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol is installed on the remote access server. Figure 17-6 shows the IPX tab.

The first item you can configure on this tab is the "Allow IPX-based remote access and demand-dial connections" check box. If you clear this check box (which is selected by default), remote access clients won't be able to use IPX-based protocols, such as NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, to connect to the remote access server.



☑ Allow IPX-based remote access and demand-dial connections

☑ Enable network access for remote clients and demand-dial connections

IPX network number assignment

This server can assign IPX network numbers:

● Automatically

○ In the following range:

From: To:

☑ Use the same network number for all IPX clients

□ Allow remote clients to request IPX node number

FIGURE 17-6 The IPX tab

The next item you can configure is a check box that enables network access for remote clients and demand-dial connections. Selecting this check box enables IPX routing on the remote access server. This check box is selected by default. Select this check box if remote access clients will access services on the network to which the remote access server is connected by using an IPX-based protocol. If you clear this check box, remote access clients will only be able to use IPX to access resources on the remote access server, but not the network.

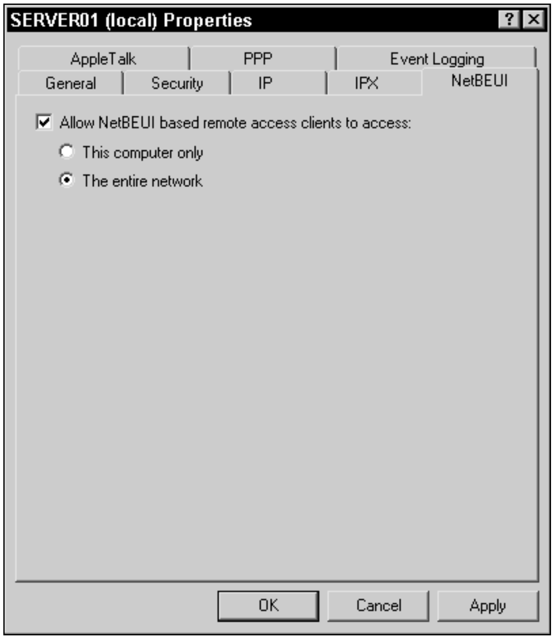
The next several options control how the remote access server assigns IPX network and node numbers to remote access clients. You can either configure the remote access server to automatically assign IPX network numbers, or configure the server to assign these numbers from a predefined range.

You can configure the remote access server to use the same IPX network number for all IPX remote access clients. (This option is selected by default.) If you clear this check box, the remote access server will assign a different IPX network number to each remote access client.

Finally, you can configure the remote access server to permit remote access clients to request a specific IPX node number.

Configuring NetBEUI

There are a couple of configurable options on the NetBEUI tab in a Windows 2000 remote access server's Properties dialog box. This tab is only available when NetBEUI is installed on the remote access server. Figure 17-7 shows the NetBEUI tab. Notice that by default, remote access clients that use NetBEUI are permitted to access the remote access server and the entire network to which the remote access server is connected.



☑ Allow NetBEUI based remote access clients to access:

○ This computer only

● The entire network

FIGURE 17-7 The NetBEUI tab

If you want to permit remote access clients to use NetBEUI to connect to the remote access server, but you don't want these clients to access resources on the network to which the remote access server is connected, select the "This computer only" option.

If you want to prevent remote access clients from using NetBEUI to connect to the remote access server, clear the check box next to "Allow NetBEUI based remote access clients to access."

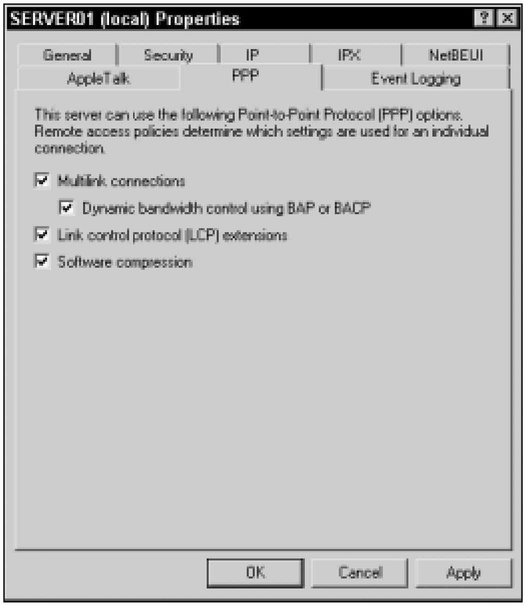
Configuring AppleTalk

There is only one configurable option on the AppleTalk tab in a Windows 2000 remote access server's Properties dialog box. This tab is only available when the AppleTalk protocol is installed on the remote access server.

By default, remote access clients are permitted to access the remote access server (and the network to which the remote access server is connected) by using AppleTalk. If you want to prevent remote access clients from using AppleTalk to connect to the remote access server, clear the check box next to "Enable AppleTalk remote access."

Configuring PPP

You can configure several PPP settings on the PPP tab in a Windows 2000 remote access server's Properties dialog box. Figure 17-8 shows the PPP tab. Notice that all of the options in this dialog box are selected by default.



This server can use the following Point-to-Point Protocol (PPP) options. Remote access policies determine which settings are used for an individual connection.

☑ Multilink connections

☑ Dynamic bandwidth control using BAP or BACP

☑ Link control protocol (LCP) extensions

☑ Software compression

FIGURE 17-8 The PPP tab

When the check box next to "Multilink connections" is selected, remote access clients are permitted to combine the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, digital link, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support. When this check box is selected, the Point-to-Point Multilink Protocol is enabled on the remote access server.

The next option on this tab is an additional setting that is only available when multilink connections are enabled. When the check box next to

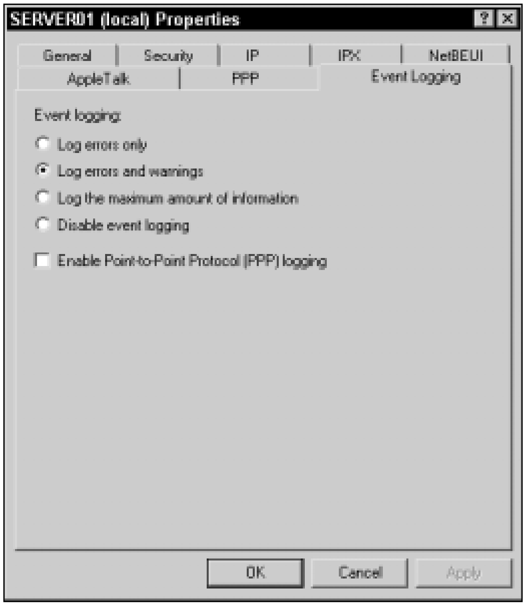
"Dynamic bandwidth control using BAP or BACP" is selected, the remote access server and remote access client are permitted to negotiate the dynamic addition and deletion of physical connections as bandwidth needs change during the remote access session.

When the check box next to "Link control protocol (LCP) extensions" is selected, the remote access server uses Link Control Protocol (LCP) extensions when communicating with remote access clients that use PPP. I recommend, for optimum remote access server functionality, that you leave this check box selected unless you have a specific need that requires you to clear it.

When the check box next to "Software compression" is selected, the remote access server will compress the data it sends to remote access clients. If you configure compression on this tab, you should disable modem compression for modems on the remote access server. Software compression is more efficient than modem compression.

Configuring Event Logging

You can configure the level of remote access event logging on the Event Logging tab in a Windows 2000 remote access server's Properties dialog box. Figure 17-9 shows the Event Logging tab. Notice that the "Log errors and warnings" option is selected by default.



Event logging:

○ Log errors only

● Log errors and warnings

○ Log the maximum amount of information

○ Disable event logging

□ Enable Point-to-Point Protocol (PPP) logging

FIGURE 17-9 The Event Logging tab

There are three levels of event logging you can select from: log errors only (this setting logs the least amount of information), log errors and warnings, and log the maximum amount of information. These logging events are written to the System log, which you can view by using Event Viewer. Or, you can disable event logging altogether.

Finally, you can choose whether to enable Point-to-Point Protocol (PPP) logging. If you select this check box, the remote access server will log information about the establishment of all PPP connections to the `*SystemRoot*\Tracing\ppp.log` file on the remote access server. If you select this option, you must stop and restart the Routing and Remote Access service before PPP logging will occur.

PPP logging can be used as an advanced troubleshooting tool when remote access clients are unable to establish PPP connections with the remote access server. You can use Notepad or your favorite text editor to view the `ppp.log` file.

Adding and Configuring Inbound Connection Ports

A remote access server must have one or more communications ports that accept inbound connections from remote access clients. A remote access server often has both hardware ports (such as modems, parallel ports, infrared ports, and so on) and VPN ports, including PPTP and L2TP ports.

In order to support VPN ports, the remote access server must have one or more network adapter cards. Typically, when VPN ports are used, the remote access server has two network adapter cards installed — one is used for incoming VPN connections (usually from the Internet) and the other is used to communicate with the local area network to which the remote access server is connected.

In the following sections I'll explain how to add and configure hardware ports and VPN ports.

Adding and Configuring Hardware Ports

By default, when you enable remote access on a Windows 2000 Server computer, Windows 2000 automatically enables all of the computer's existing hardware ports for remote access.

If you add hardware ports to a Windows 2000 Server computer after remote access is enabled, usually Windows 2000 (because of its Plug and Play capabilities) will automatically detect, install, configure, and enable the hardware ports for remote access.

If Windows 2000 doesn't automatically detect and install your newly installed modem (or other hardware device), you can use a Control Panel application, such as Add/Remove Hardware or the Phone and Modem Options application, to install and configure the device.

CROSS-REFERENCE

For more information on using Add/Remove Hardware, see Chapter 5. For detailed steps on installing and configuring modems by using Phone and Modem Options, see Chapter 15.

You can view and modify the configurable properties of *all* remote access ports (both hardware and VPN) by using Routing and Remote Access. However, not all options are available for each port type.

STEP BY STEP

CONFIGURING A REMOTE ACCESS PORT

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, click the + next to the server that contains the remote access port you want to configure. Right-click Ports, and select Properties from the menu that appears.
3. The Ports Properties dialog box appears, as shown in Figure 17-10. Notice that both hardware and VPN ports are listed. Also notice that there are five PPTP and five L2TP ports.

   Highlight the remote access port you want to configure, and click Configure.
4. The Configure Device dialog box for the port you selected appears, as shown in Figure 17-11.

   Ensure that the check box next to "Remote access connections (inbound only)" is selected if you want this port to be used for inbound connections from remote access clients.

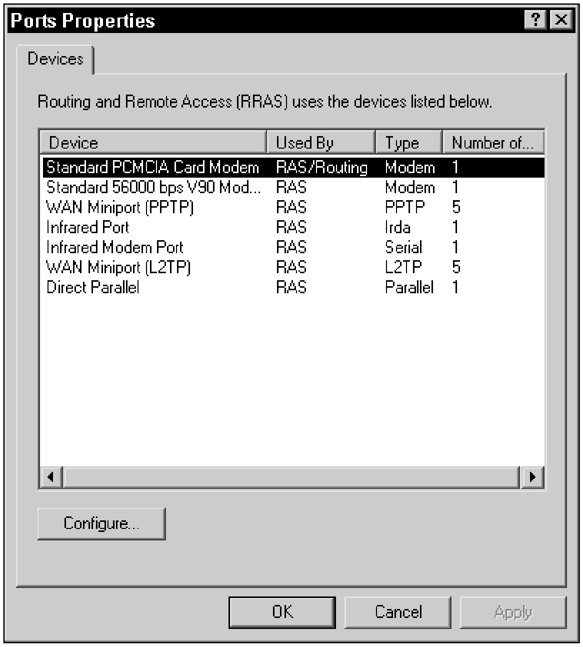
   Select the check box next to "Demand-dial routing connections (inbound and outbound)" if this computer also functions as a router and you want to enable this port for demand-dial connections.

   If you're configuring a modem port, enter the phone number of the modem.

   Finally, if you're configuring a PPTP port, an L2TP port, or a multiport hardware device, you can configure the maximum number of ports of this type that the Windows 2000 remote access server will support.

   When you finish configuring the port, click OK.

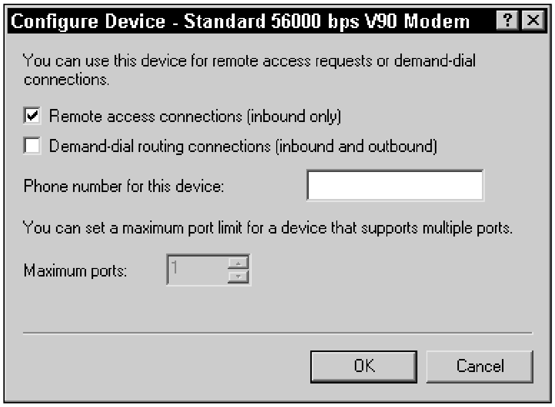
STEP BY STEP *Continued*



Routing and Remote Access (RRAS) uses the devices listed below.

Device	Used By	Type	Number of...
Standard PCMCIA Card Modem	RAS/Routing	Modem	1
Standard 56000 bps V90 Mod...	RAS	Modem	1
WAN Miniport (PPTP)	RAS	PPTP	5
Infrared Port	RAS	Irda	1
Infrared Modem Port	RAS	Serial	1
WAN Miniport (L2TP)	RAS	L2TP	5
Direct Parallel	RAS	Parallel	1

FIGURE 17-10 Viewing ports in Routing and Remote Access



You can use this device for remote access requests or demand-dial connections.

☑ Remote access connections (inbound only)

□ Demand-dial routing connections (inbound and outbound)

Phone number for this device:

You can set a maximum port limit for a device that supports multiple ports.

Maximum ports: 1

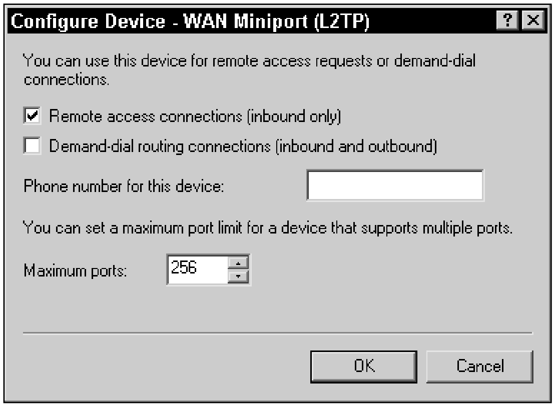
FIGURE 17-11 Configuring a remote access port

5. In the Ports Properties dialog box, click OK.
6. Close Routing and Remote Access.

Adding and Configuring VPN Ports

By default, when you configure your Windows 2000 Server computer as a remote access server, Windows 2000 automatically creates and enables five PPTP ports and five L2TP ports. If you configure the Windows 2000 Server computer as a VPN server, Windows 2000 automatically creates and enables 128 PPTP ports and 128 L2TP ports.

To configure PPTP or L2TP ports, use the steps in the previous section titled "Configuring a Remote Access Port." To add additional PPTP or L2TP ports, use the same steps, and in the Configure Device – WAN Miniport (PPTP or L2TP) dialog box, specify a larger number in the Maximum ports spin box. Figure 17-12 shows this dialog box after I have increased the number of L2TP ports to 256. A Windows 2000 remote access server can support up to 30,000 PPTP ports and up to 30,000 L2TP ports.



Configure Device - WAN Miniport (L2TP)

You can use this device for remote access requests or demand-dial connections.

☑ Remote access connections (inbound only)

□ Demand-dial routing connections (inbound and outbound)

Phone number for this device:

You can set a maximum port limit for a device that supports multiple ports.

Maximum ports: 256

FIGURE 17-12 Remote access server configured to support 256 L2TP ports

Using Remote Access Policies to Control Access

Security is a critical consideration when implementing remote access on your network. After all, you don't want to expose your remote access server, and potentially your entire local area network, to just anybody out there who happens to have a modem and the telephone number of your remote access server.

In Windows 2000, access to the remote access server is controlled by using remote access policies. A remote access policy has three components:

- **Conditions:** These are one or more predefined attributes that must be matched by the remote access client attempting to connect to the remote access server. Common conditions include: day and time restraints, telephone number from which the remote access connection is initiated, remote access client computer name, and so on. If more than one condition is specified, *all* conditions must be matched.
- **Permissions:** A remote access permission either specifically grants access or denies access to the remote access server.
- **Profile:** This is a collection of settings that specify numerous properties that are applied to the remote access connection established by a remote access client using the remote access policy that contains the profile. The available settings in a profile include dial-in constraints, IP address assignment options, multilink options, authentication methods, encryption options, and so on.

The elements contained in a remote access policy are applied to a remote access client in a predetermined order. First, the remote access client must meet *all* conditions specified in a remote access policy. If the remote access client meets all of the policy's conditions, then the remote access client must be granted permission to access the remote access server. Finally, if all conditions are met and permission is granted, the settings of the profile are applied to the connection the remote access client is establishing.

A user can connect to a Windows 2000 remote access server *only* if a remote access policy permits the user to do so. Windows 2000 creates a default remote access policy when remote access is enabled. The default remote access policy is a basic policy that permits any remote user that is allowed the dial-in remote access permission to connect to the remote access server. In addition, you can create multiple remote access policies for a remote access server.

Remote access policies are not stored in Active Directory, and should not be confused with Group Policy. Rather, remote access policies are stored on the Windows 2000 remote access server. Remote access policies, then, are applied on a server-by-server basis. In this way, administrators can place varying degrees of control on each remote access server, depending on the security requirements of their network. Optionally, if you use a RADIUS server for remote access authentication, you can centrally manage remote access policies by creating them on the RADIUS server (or on an Internet Authentication Service (IAS) server, which is the Windows 2000 implementation of RADIUS).

You can use the Routing and Remote Access administrative tool to create new remote access policies.

STEP BY STEP

CREATING A REMOTE ACCESS POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, click the + next to the server for which you want to create a new remote access policy. Right-click Remote Access Policies, and select New Remote Access Policy from the menu that appears.
3. The Add Remote Access Policy dialog box appears. Type in a name for the remote access policy. Click Next.
4. In the screens that follow, specify conditions, permissions, and a profile for the policy. (I'll cover details on each of these items in the next several sections.) After you complete these steps, click Finish.
5. Close Routing and Remote Access.

You can also use Routing and Remote Access to configure or edit any existing remote access policy.

STEP BY STEP

CONFIGURING A REMOTE ACCESS POLICY

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, click the + next to the server that has the remote access policy you want to configure. Highlight Remote Access Policies. Then, in the right pane, double-click the remote access policy you want to configure.
3. The policy's Properties dialog box appears. Configure conditions, permissions, and the policy's profile as appropriate. (I'll cover details on each of these items in the next several sections.) Click OK
4. Close Routing and Remote Access.

In the following sections I'll show you how to specify conditions for a remote access policy, how to configure remote access permission options, and how to configure a profile for a remote access policy. I'll also discuss the order in which multiple remote access policies are applied.

Specifying Conditions for a Remote Access Policy

A remote access policy must have at least one condition, and may have multiple conditions. You can specify a remote access policy's conditions either when you first create the remote access policy, or later in the policy's Properties dialog box. (To access a remote access policy's Properties dialog box, follow the steps titled "Configuring a Remote Access Policy" in the previous section.)

Table 17-1 lists and describes the conditions you can assign to a remote access policy.

TABLE 17-1 Remote Access Policy Conditions

Condition	Description
Called-Station-ID	Phone number dialed by the remote access client
Calling-Station-ID	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client (IAS only) (IAS is the Windows 2000 implementation of the RADIUS server standard.)
Client-IP-Address	IP address of RADIUS client (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS (IAS only) (NAS stands for network access server. A NAS is a proprietary, hardware-based remote access server.)
Day-And-Time-Restrictions	Time periods and days of the week during which the remote access client is permitted to connect
Framed-Protocol	The connection protocol to be used by the remote access client (PPP, AppleTalk Remote Access Protocol [ARAP], X.25, and so on)
NAS-Identifier	String identifying the NAS originating the request (IAS only)
NAS-IP-Address	IP address of the NAS originating the request (IAS only)
NAS-Port-Type	Type of physical port used by the NAS originating the request (IAS only)
Service-Type	Type of service the remote access client has requested (such as Login, Callback, and so on)

Condition	Description
Tunnel-Type	Tunneling protocols that can be used by the remote access client (such as PPTP, L2TP, and so on)
Windows-Groups	Windows security groups to which the remote access user belongs

Probably the two most commonly used conditions are Windows-Groups and Day-And-Time-Restrictions. Windows-Groups are used to allow (or deny) access to remote users that are members of a particular security group. Day-And-Time Restrictions allow you to specify which days and hours connections to the remote access server are permitted.

You may have noticed that the descriptions for several of the conditions listed in Table 17-1 indicate "IAS only." IAS, which stands for Internet Authentication Service, is a Windows 2000 Server service that enables a Windows 2000 Server computer to function as a RADIUS server. These conditions should only be used for remote access policies on a Windows 2000 Server computer that has IAS installed and is functioning as a RADIUS server.

Configuring Remote Access Permission Options

There are two methods of assigning permissions for remote access clients. You can assign permissions by modifying a user's account properties, or by configuring the properties of a remote access policy. The method you choose to assign permissions to remote access clients depends on the size of your network, and whether your Windows 2000 domain is operating in native-mode or mixed-mode.

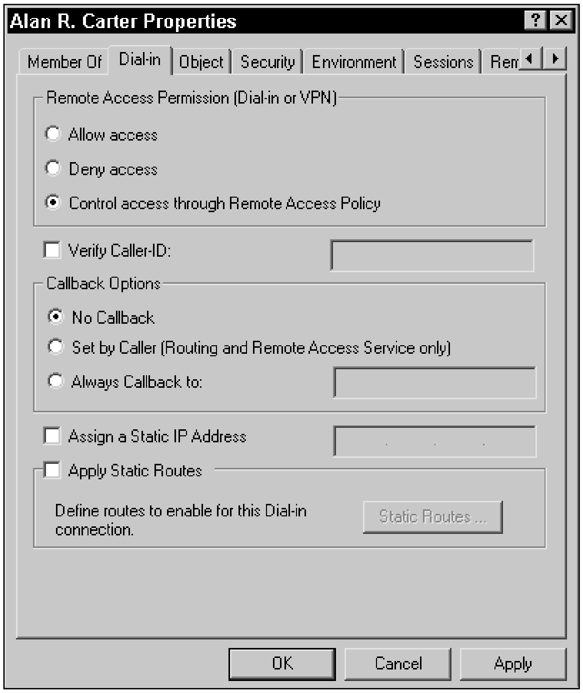
If you have a large network, you'll probably decide to manage permissions for remote access clients by using remote access policies. On a small network, you might decide to manage these permissions on a user-by-user basis.

When your Windows 2000 domain is operating in mixed-mode, you *must* manage permissions for remote access clients on a user-by-user basis — you can't use remote access policies to manage permissions. If your Windows 2000 domain is operating in native-mode, you can use either method to assign permissions to remote access clients.

STEP BY STEP

ASSIGNING REMOTE ACCESS PERMISSIONS TO USER ACCOUNTS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the user account you want to configure. Highlight the `Users` folder or the OU that contains that user account. In the right pane, double-click the user account. Or, you can right-click the user account, and select Properties from the menu that appears.
3. In the user's Properties dialog box, click the Dial-in tab.
4. The Dial-in tab appears, as shown in Figure 17-13. This figure shows a user account's properties in a Windows 2000 domain operating in native-mode. *In a Windows 2000 domain operating in mixed-mode, the Control access through Remote Access Policy, Verify Caller-ID, Assign a Static IP address, and Apply Static Routes options are grayed out and not available.*



Remote Access Permission (Dial-in or VPN)

○ Allow access

○ Deny access

● Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

FIGURE 17-13 Configuring remote access permissions for a user account

STEP BY STEP *Continued*

There are numerous options you can configure in this dialog box:

- **Allow access:** Select this option if you want to permit this user to connect to the remote access server.
- **Deny access:** Select this option if you want to prevent this user from connecting to the remote access server.
- **Control access through Remote Access Policy:** Select this option if you want the remote access policy—not the user account—to determine whether the user can connect to the remote access server.

TIP

Remote access permissions configured in a user's properties dialog box override permission settings in a remote access policy unless the user account is configured to "Control access through Remote Access Policy."

- **Verify Caller-ID:** Select this option if you want to prevent the user from using any telephone number—except the one number you specify—to initiate a connection with the remote access server. If you select this option, you'll need to enter the number from which the user is permitted to connect. Often this is a user's home telephone number.
- **No Callback:** Select this option if you want to prevent the user from requesting that the remote access server break the connection and call the user back. When this option is selected, it ensures that the user dialing in—not the server—is billed for any long-distance telephone charges.
- **Set by Caller (Routing and Remote Access Service only):** Select this option if you want to permit the user to request that the remote access server break the connection and call the user back at a user-specified telephone number.
- **Always Callback to:** Select this option if you want the remote access server to automatically break the connection and call the user back at a prespecified telephone number. This option provides a measure of security, because the remote access server will only call the user back at one prespecified number. If you select this option, you must specify the telephone number that the remote access server will call back.
- **Assign a Static IP Address:** Select this option when the user dialing in requires a specific static IP address. If you select this option, you must specify an IP address that will be assigned to the user during remote access connections. This option is often used when a user account is used to authenticate a demand-dial routing connection.

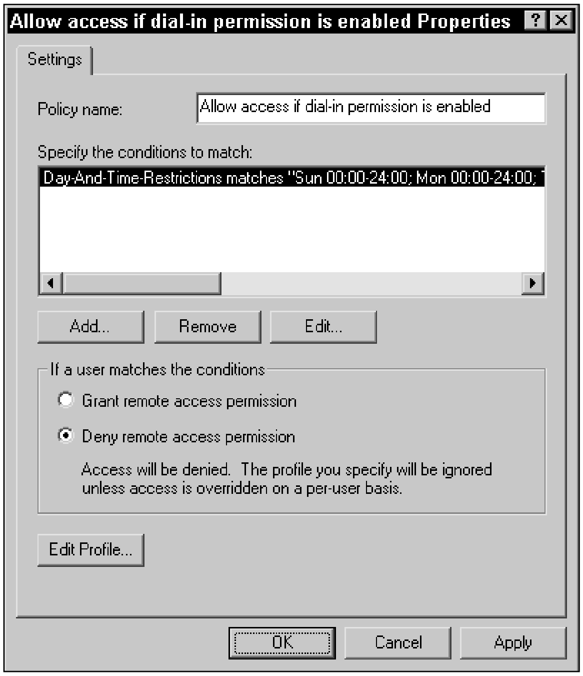
STEP BY STEP *Continued*

- ▶ **Apply Static Routes:** Select this option if this user account is used to authenticate a demand-dial routing connection, and you want to specify static routes that will be added to the remote router's routing table when the connection is established. If you select this option, you must also configure the static routes.

When you finish configuring options on this tab, click OK.

5. Close Active Directory Users and Computers.

You can specify a remote access policy's permissions either when you first create the remote access policy, or later in the policy's Properties dialog box. To access the policy's Properties dialog box in Routing and Remote Access, see the steps titled "Configuring a Remote Access Policy" in the "Using Remote Access Policies to Control Access" section earlier in this chapter. Figure 17-14 shows the Properties dialog box for the default remote access policy, which is named "Allow access if dial-in permission is enabled."



Allow access if dial-in permission is enabled Properties

Settings

Policy name: Allow access if dial-in permission is enabled

Specify the conditions to match:

Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

If a user matches the conditions

○ Grant remote access permission

● Deny remote access permission

Access will be denied. The profile you specify will be ignored unless access is overridden on a per-user basis.

FIGURE 17-14 Configuring remote access permissions in a remote access policy

As Figure 17-14 shows, there are only two permissions options in this dialog box:

- **Grant remote access permission:** If this option is selected, the user is permitted to connect to the remote access server as long as the remote access client meets the policy's conditions, unless the user's account properties are configured to "Deny access."
- **Deny remote access permission:** If this option is selected, the user is prevented from connecting to the remote access server if the remote access client meets the policy's conditions, unless the user's account properties are configured to "Allow access."

Configuring a Profile for a Remote Access Policy

Once you've specified conditions for a remote access policy and configured permissions, you're ready to configure a profile for the remote access policy.

A remote access policy's profile is a collection of settings that specify numerous properties that are applied to the remote access connection established by a remote access client using the remote access policy that contains the profile.

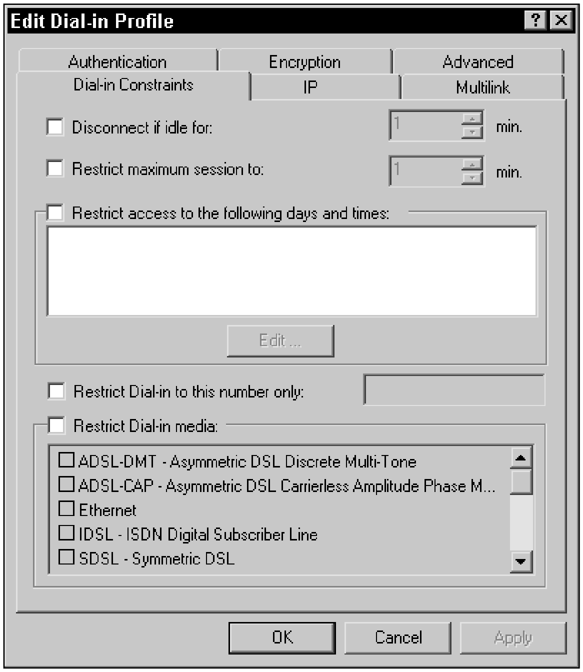
You might wonder why a remote access policy even needs a profile, because many of the profile settings mirror the types of settings you can define in a remote access policy's conditions. However, conditions only determine which policy is applied to the remote access client, while the profile specifies how the connection operates.

You can configure a remote access policy's profile either when you first create the remote access policy, or later in the policy's Properties dialog box. To access the policy's Properties dialog box in Routing and Remote Access, see the steps titled "Configuring a Remote Access Policy" in the "Using Remote Access Policies to Control Access" section earlier in this chapter. To configure a remote access policy's profile, click Edit Profile in the policy's Properties dialog box.

The available settings in a profile are contained on six tabs in this dialog box: Dial-in Constraints, IP, Multilink, Authentication, Encryption, and Advanced. I'll show you how to configure each of these tabs in the next several sections.

Configuring Dial-in Constraints

Dial-in constraint settings do what their name implies — they restrict certain aspects of the remote access connection. You can configure these settings on the Dial-in Constraints tab, which is shown in Figure 17-15.



□ Disconnect if idle for: 1 min.

□ Restrict maximum session to: 1 min.

□ Restrict access to the following days and times:

□ Restrict Dial-in to this number only:

□ Restrict Dial-in media:

□ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
□ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase M...
□ Ethernet
□ IDSL - ISDN Digital Subscriber Line
□ SDSL - Symmetric DSL

FIGURE 17-15 Configuring dial-in constraints

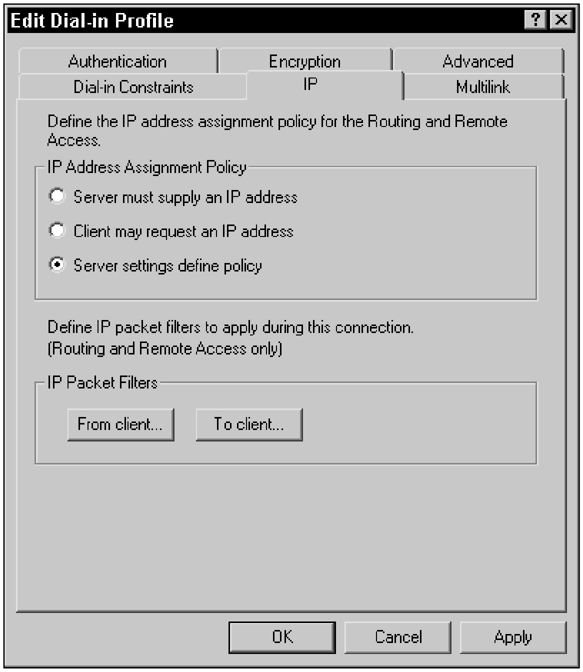
There are five configurable options on this tab:

- **Disconnect if idle for:** If you select this option, you can specify the number of minutes the remote access server will permit the connection to be idle before it disconnects the remote access client.
- **Restrict maximum session to:** If you select this option, you can limit the length of the dial-in connection to a specified number of minutes. When this time limit is reached, the remote access server disconnects the remote access client.
- **Restrict access to the following days and times:** If you select this option, you can specify the days of the week and the hours during the day when dial-in connections will be permitted.

- **Restrict Dial-in to this number only:** If you select this option, remote access clients are only permitted to establish a dial-up connection by using the one telephone number you specify in the corresponding text box.
- **Restrict Dial-in media:** If you select this option, you can specify the types of connections that will be permitted. For example, if you only want remote access clients to connect to the remote access server by using a modem, you can select this option and then select the Async (Modem) check box.

Configuring IP Address Assignment

You can configure IP address assignment policy and define IP packet filtering for the remote access connection on the IP tab, which is shown in Figure 17-16.



Define the IP address assignment policy for the Routing and Remote Access.

IP Address Assignment Policy

○ Server must supply an IP address

○ Client may request an IP address

● Server settings define policy

Define IP packet filters to apply during this connection. (Routing and Remote Access only)

IP Packet Filters

FIGURE 17-16 Configuring IP address assignment policy

There are three IP address assignment policy options on this tab:

- **Server must supply an IP address:** Select this option if you want the remote access server to assign an IP address to the remote access client for the connection.
- **Client may request an IP address:** Select this option if you want to permit the remote access client to request a specific IP address.
- **Server settings define policy:** Select this option if you want the IP settings configured in the remote access server's Properties dialog box to govern how IP addresses are assigned to remote access clients.

In addition to configuring IP address assignment policy, you can define IP packet filters that will apply during the remote access connection. To specify an IP packet filter that filters the IP traffic sent from the remote access client, click "From client" and configure a packet filter. To specify an IP packet filter that filters the IP sent from the remote access server to the remote access client, click "To client" and configure a packet filter.

CROSS-REFERENCE

Configuring TCP/IP packet filters was covered in Chapter 16.

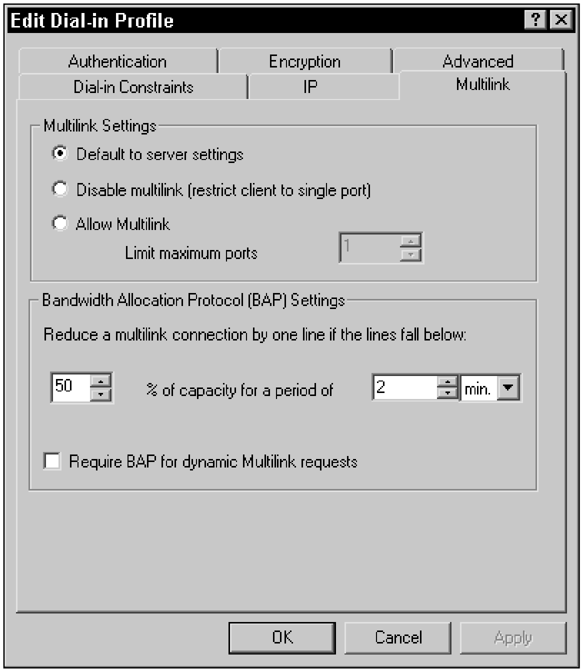
Configuring Multilink Connection Options

You can configure various multilink options on the Multilink tab, which is shown in Figure 17-17.

You may recall that multilink connections permit remote access clients to combine the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, digital link, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support.

There are three multilink options on this tab:

- **Default to server settings:** If you select this option, the multilink settings configured on the PPP tab in the remote access server's Properties dialog box will determine whether multilink is used for this remote access connection.
- **Disable multilink (restrict client to single port):** If you select this option, remote access clients won't be able to use multilink for the remote access connection.



Multilink Settings

● Default to server settings

○ Disable multilink (restrict client to single port)

○ Allow Multilink

Limit maximum ports 1

Bandwidth Allocation Protocol (BAP) Settings

Reduce a multilink connection by one line if the lines fall below:

50 % of capacity for a period of 2 min.

□ Require BAP for dynamic Multilink requests

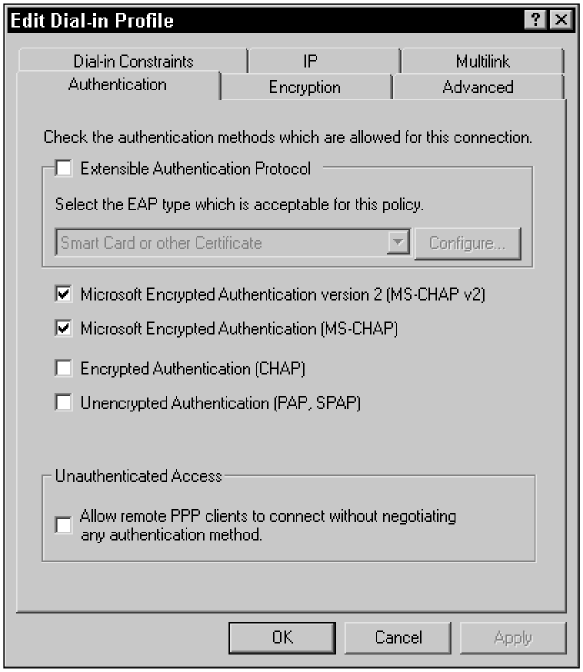
FIGURE 17-17 Configuring multilink options

- **Allow Multilink:** If you select this option, remote access clients will be permitted to use multilink for the remote access connection.

You can also specify Bandwidth Allocation Protocol (BAP) settings on the Multilink tab. If usage of the remote access connection falls below a specified capacity of the combined lines for the specified number of minutes, the remote access server will disconnect one of the lines used in the multilink connection. You can also require that BAP be used for requests made by the remote access client to dynamically add or remove lines during the multilink connection.

Configuring Authentication Methods

You can configure authentication methods for the remote access connection on the Authentication tab, which is shown in Figure 17-18. Only the authentication methods you select on this tab will be used to authenticate remote access users who connect by using the remote access policy that contains this profile.



Check the authentication methods which are allowed for this connection.

□ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Smart Card or other Certificate

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☑ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

FIGURE 17-18 Configuring authentication methods

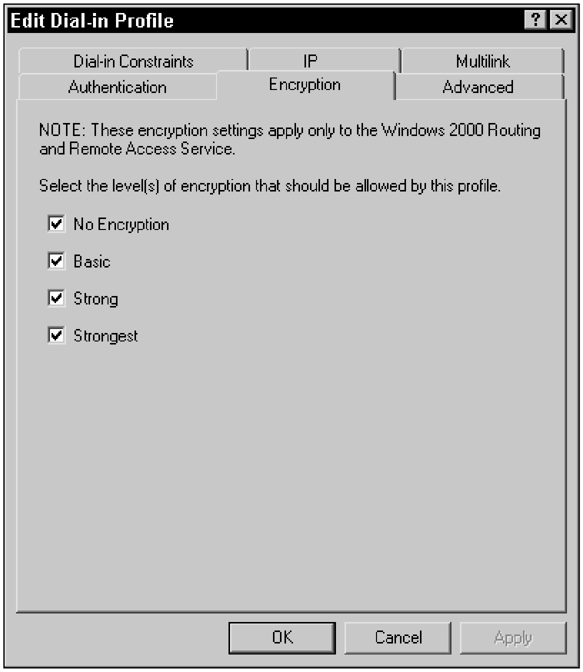
The options in this dialog box are virtually identical to the authentication methods that can be configured for the remote access server. If you need more information on any of the authentication methods listed on this tab, see the "Configuring Security" section earlier in this chapter.

Configuring Encryption

You can select one or more encryption options that the remote access client can choose to use on the connection. The remote access client *must* use one of the options selected. Figure 17-19 shows the Encryption tab. Notice the four options on this tab. The last option, Strongest, is only available after you've downloaded and installed the Windows 2000 High Encryption Pack from the Microsoft Web site (`http://www.microsoft.com/windows2000/downloads/`).

Here's a list of the encryption options and what each specifies:

- **No Encryption:** If you select this option, remote access clients can connect to the remote access server without using any encryption. If you want to require the remote access client to use encryption, ensure that this check box is cleared.



Edit Dial-in Profile

NOTE: These encryption settings apply only to the Windows 2000 Routing and Remote Access Service.

Select the level(s) of encryption that should be allowed by this profile.

☑ No Encryption

☑ Basic

☑ Strong

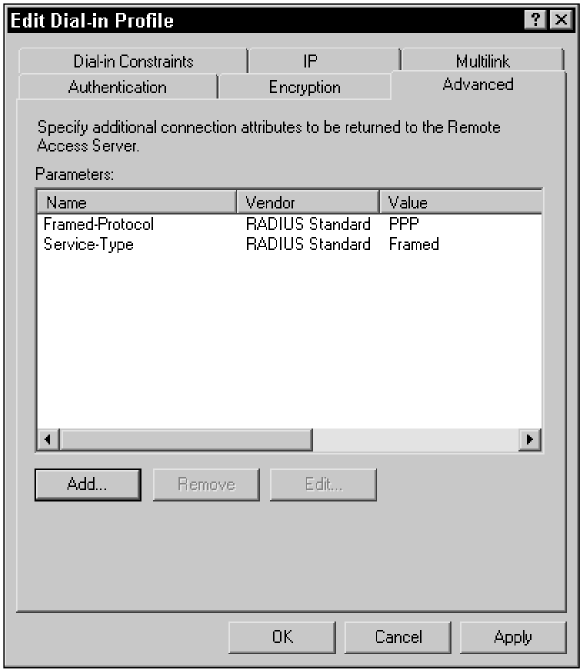
☑ Strongest

FIGURE 17-19 Selecting encryption options

- **Basic:** If you select this option, remote access clients can use IPSec 56-bit DES or MPPE 40-bit encryption. If the remote access client uses "basic" encryption, it will use IPSec for all L2TP VPN connections, and Microsoft Point-to-Point Encryption (MPPE) 40-bit encryption for all other types of remote access connections.
- **Strong:** If you select this option, remote access clients can use IPSec 56-bit DES or MPPE 56-bit encryption. If the remote access client uses "strong" encryption, it will use IPSec for all L2TP VPN connections, and MPPE 56-bit encryption for all other types of remote access connections.
- **Strongest:** If you select this option, remote access clients can use IPSec Triple DES (3DES) or MPPE 128-bit encryption. If the remote access client uses "strongest" encryption, it will use IPSec 3DES for all L2TP VPN connections, and MPPE 128-bit encryption for all other types of remote access connections.

Configuring Advanced Connection Attributes

The last tab in the profile's dialog box is the Advanced tab. On this tab, you can specify additional RADIUS attributes that will be sent from the RADIUS server to the remote access client during the connection establishment process. Figure 17-20 shows the Advanced tab.



Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed

FIGURE 17-20 Configuring advanced RADIUS options

To add additional parameters, click Add and select from the numerous available RADIUS attributes. As you might guess, you only need to configure options on this tab if you're using a RADIUS server for authentication.

How Remote Access Policies Are Applied

It's common for multiple remote access policies to exist on a remote access server. When a remote access client attempts to connect to the remote access server and multiple remote access policies exist, the remote access server performs the following actions:

1. The remote access server compares the conditions of each remote access policy, one at a time (in the order the policies are listed in the Routing and Remote Access console), with the conditions of the attempted

connection. When the remote access server locates a policy that has conditions that match the conditions of the attempted connection, that policy is applied to the attempted connection. If the conditions of the attempted connection don't match the conditions of any remote access policy, the remote access server rejects the connection attempt.

2. The remote access server evaluates the permissions in the policy and the remote user's remote access permissions and determines whether the remote user is granted or denied permission to the connection. If the remote user is denied permission to the connection, the remote access server rejects the connection attempt.
3. The remote access server applies the conditions and settings contained in the remote access policy's profile to the connection. If any conditions in the profile are not met, the remote access server rejects the connection attempt. Otherwise, the remote access server establishes the connection.

These steps assume that multiple policies exist on a remote access server. If only a single policy exists, such as the default remote access policy, the remote access client must meet the conditions of that policy or the remote access server will reject the connection attempt. If no policy exists (perhaps because an administrator has accidentally deleted all policies), the remote access server will reject all connection attempts from remote access clients.

Figure 17-21 is a flow chart that shows a graphical representation of the remote access connection process. This chart is a slightly more detailed version of the steps I outlined in the previous paragraphs.

EXAM TIP

After reading a detailed description *and* a flow chart, you're probably getting the idea that how remote access policies are applied is important. Make sure you completely understand and memorize this process, and don't be surprised if you see a couple of tough exam questions on this topic.

I want to emphasize that the remote access server processes remote access policies *in the order they're listed in the Routing and Remote Access console*. You might want to change the order in which policies are applied. Typically, administrators place the most specific policies at the top of the list, and the most general policies at the bottom of the list. If you don't order policies in this manner, but instead place policies with few conditions at the top of the list, remote users that have specially configured policies won't be assigned these policies because a more general policy will be applied *first*.

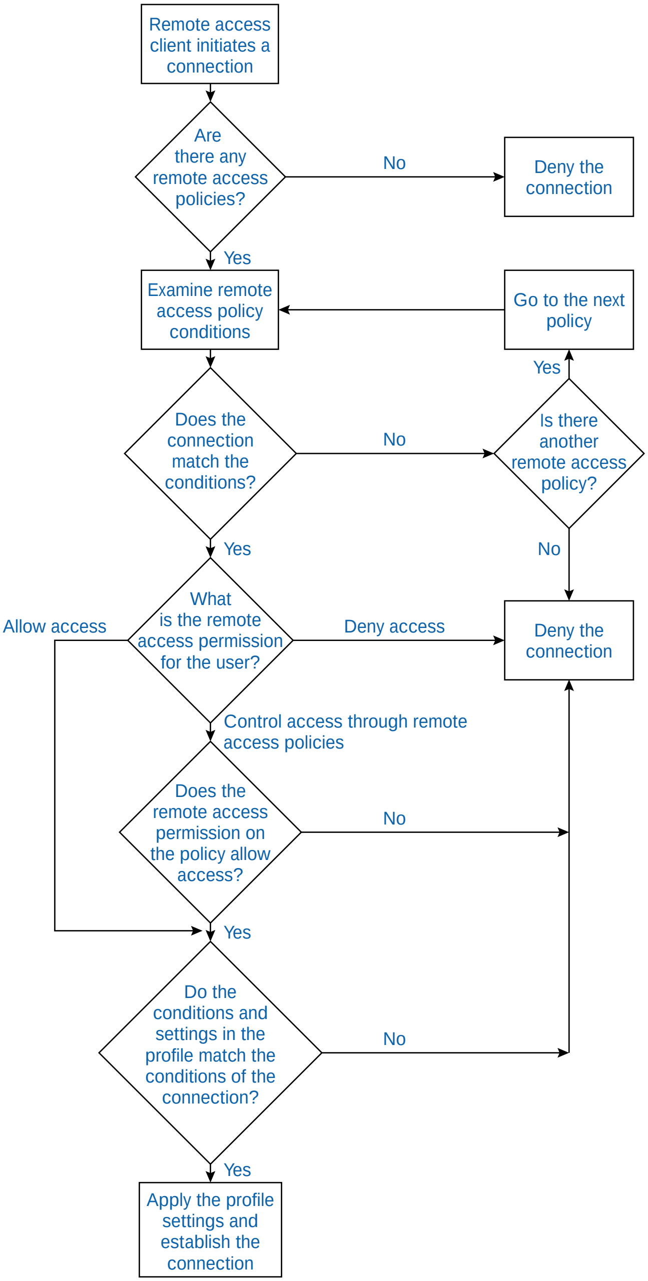
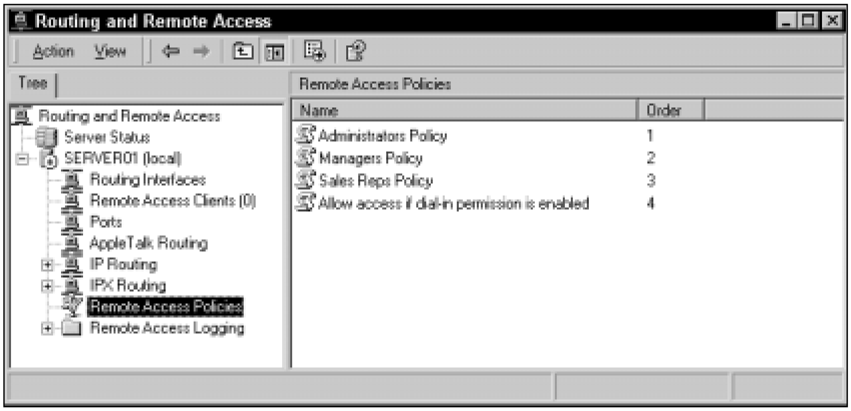

Remote access client initiates a connection
Are there any remote access policies?
No
Deny the connection
Yes
Examine remote access policy conditions
Go to the next policy
Yes
Does the connection match the conditions?
No
Is there another remote access policy?
Yes
No
Allow access
What is the remote access permission for the user?
Deny access
Deny the connection
Control access through remote access policies
Does the remote access permission on the policy allow access?
No
Yes
Do the conditions and settings in the profile match the conditions of the connection?
No
Yes
Apply the profile settings and establish the connection

FIGURE 17-21 The remote access connection process

STEP BY STEP

CHANGING THE ORDER IN WHICH REMOTE ACCESS POLICIES ARE APPLIED

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, click the + next to the remote access server on which you want to change the order of remote access policies. Highlight Remote Access Policies.
3. In the right pane, right-click any policy, and select Move Up or Move Down from the menu that appears. Continue this process until the policies are in the desired order. Figure 17-22 shows the Routing and Remote Access console after I've configured the order of several remote access policies. Notice the policy that matches the fewest number of remote access clients is at the top of the list, and the most general policy is at the bottom of the list.



Name	Order
Administrators Policy	1
Managers Policy	2
Sales Reps Policy	3
Allow access if dial-in permission is enabled	4

FIGURE 17-22 Ordering remote access policies

4. Close Routing and Remote Access.

Monitoring Remote Access

To ensure that your Windows 2000 remote access server is functioning at its best, you should periodically monitor this server. You can monitor and manage the remote access activity on the remote access server, and you can use monitoring to determine whether the server has sufficient resources (such as memory, processor, and disk) to handle its remote access tasks.

There are several valuable monitoring tasks you can perform in the Routing and Remote Access console. You can view the status of the remote access server, view a list of remote access clients currently connected to the server, send a pop-up message to one (or all) remote access users, disconnect a remote user, view the status of a remote access connection, view current connections by port, and configure remote access logging.

STEP BY STEP

MONITORING REMOTE ACCESS CONNECTIONS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, click the + next to the remote access server you want to monitor.
3. **To view the status of the Windows 2000 remote access server,** highlight Server Status. In the right pane, the current status of all remote access servers that have been added to this console is displayed. You can view the number of total ports and the number of ports in use on each server.
4. **To view a list of the remote access clients currently connected to the remote access server,** highlight Remote Access Clients. In the right pane, a list of remote access clients is displayed. You can view the remote user's name, the duration of the connection, and the number of ports used by this client.

   To send a pop-up message to the remote access user (or to all remote users currently connected), in the right pane, right-click the user, and select Send Message (or Send to All) from the menu that appears. In the Send Message dialog box, type in your message to the remote user(s) and click OK. The message is delivered immediately.

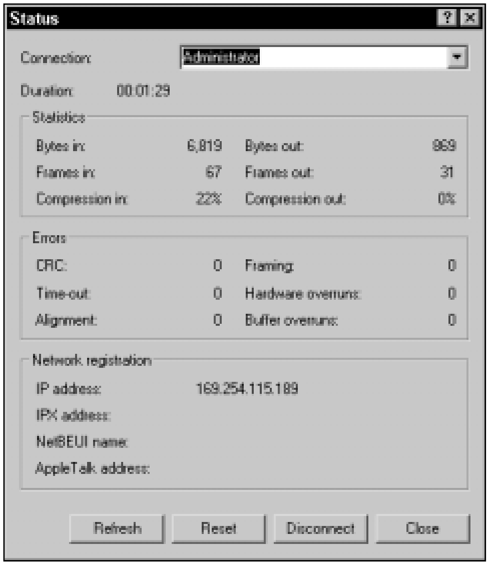
   To disconnect a remote user, in the right pane, right-click the user, and select Disconnect from the menu that appears. The user is disconnected immediately. Select Action ➪ Refresh to verify that the user is no longer connected.

   To view the status of a remote access connection, in the right pane, right-click the remote access user, and select Status from the menu that appears. The Status dialog box is displayed, as shown in Figure 17-23. Notice the various statistics you can view for a connection.

   Also notice that you can refresh the connection's statistics and disconnect the remote access client in this dialog box.

   Finally, notice that once this dialog box is displayed, you can view the statistics for any remote access connection by selecting the remote access client (by user name) from the Connection drop-down list box. When you finish viewing statistics, click Close.

STEP BY STEP *Continued*



Connection: Administrator

Duration: 00:01:29

Statistics

Bytes in:	6,819	Bytes out:	869
Frames in:	67	Frames out:	31
Compression in:	22%	Compression out:	0%

Errors

CRC:	0	Framing:	0
Time-out:	0	Hardware overruns:	0
Alignment:	0	Buffer overruns:	0

Network registration

IP address: 169.254.115.189

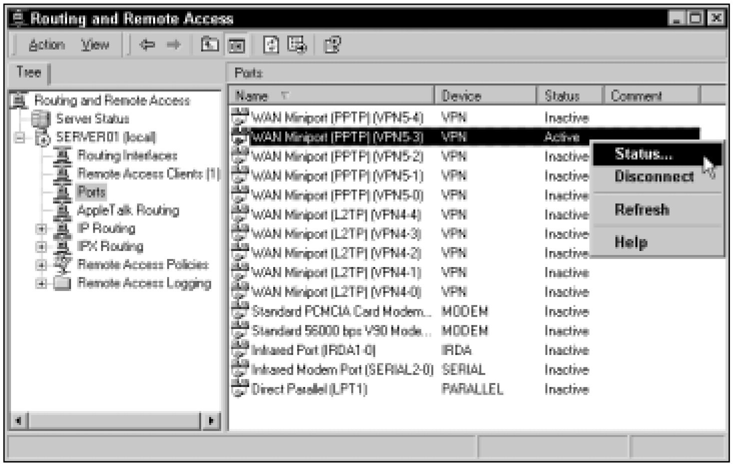
IPX address:

NetBEUI name:

AppleTalk address:

FIGURE 17-23 Monitoring a connection's status

5. **To view current remote access connections by port,** in the left pane of Routing and Remote Access, highlight Ports. In the right pane, a list of all ports on the remote access server is displayed. You can view the device used by each port, and whether each port is active or inactive. You can also right-click any port, and disconnect the remote access client or view the status of the connection, as shown in Figure 17-24.



Name	Device	Status	Comment
WAN Miniport (PPTP) (VPN5-4)	VPN	Inactive	
WAN Miniport (PPTP) (VPN5-3)	VPN	Active	
WAN Miniport (PPTP) (VPN5-2)	VPN	Inactive	
WAN Miniport (PPTP) (VPN5-1)	VPN	Inactive	
WAN Miniport (PPTP) (VPN5-0)	VPN	Inactive	
WAN Miniport (L2TP) (VPN4-4)	VPN	Inactive	
WAN Miniport (L2TP) (VPN4-3)	VPN	Inactive	
WAN Miniport (L2TP) (VPN4-2)	VPN	Inactive	
WAN Miniport (L2TP) (VPN4-1)	VPN	Inactive	
WAN Miniport (L2TP) (VPN4-0)	VPN	Inactive	
Standard PCMCIA Card Modem...	MODEM	Inactive	
Standard 56000 bps V90 Mode...	MODEM	Inactive	
Infrared Port (IRDA1-0)	IRDA	Inactive	
Infrared Modem Port (SERIAL2-0)	SERIAL	Inactive	
Direct Parallel (LPT1)	PARALLEL	Inactive	

FIGURE 17-24 Viewing a port's status

STEP BY STEP *Continued*

6. **To configure remote access logging** (so you can later use the log file), in the left pane of Routing and Remote Access, highlight Remote Access Logging. In the right pane, double-click Local File.
7. The Local File Properties dialog box appears. On the Settings tab, you can configure the types of information that Windows 2000 will write to the log file. You can select one or more of these options:
   - Log accounting requests (for example, accounting start or stop) – recommended
   - Log authentication requests (for example, access-accept or access-reject) – recommended
   - Log periodic status (for example, interim accounting requests)

   On the Local File tab in this dialog box, you can select either a database-compatible file format or an IAS format. If you select the IAS format, Windows 2000 creates a text file that uses comma-separated values. You can also specify how often a new log file will be created. Finally, you can select a location in which the log file will be stored. When you finish configuring logging, click OK.

   To view log files created in IAS format, use Notepad or any text editor.
8. Close Routing and Remote Access.

In addition to using Routing and Remote Access, you can use System Monitor, a Performance tool, to monitor the performance of the Windows 2000 remote access server. Remote access objects include RAS Port and RAS Total. Each of these objects has multiple counters associated with it. You can also use System Monitor to determine if your Windows 2000 remote access server has adequate memory, processor, and disk resources.

CROSS-REFERENCE

I'll cover how to use System Monitor in Chapter 21.

Troubleshooting Remote Access

Remote access is a complex topic. There are many connection protocols, networking protocols, authentication methods, encryption options, and remote access policies that combine to form your remote access solution.

While these features make the service very flexible, they can also make troubleshooting difficult when problems arise.

Table 17-2 lists some of the more common remote access problems you may encounter and some possible solutions to these problems.

TABLE 17-2 Remote Access Problems and Solutions

Problem	Recommended Solution
A remote access client can't establish a connection with a Windows 2000 remote access server.	If the remote access client is using a modem, verify that the correct telephone number is being dialed. If the modem doesn't have a speaker, use a regular telephone to dial the remote access server and verify that a modem answers. If the client is attempting to establish a VPN connection, make sure your Internet connection is working properly by pinging the FQDN of the VPN server.
A remote access user is denied access by the remote access server after the user provides a user name and password.	Ensure that the user has typed the user name and password correctly (remember, passwords are case-sensitive). Verify that the user has remote access permissions. Verify that there is at least one remote access policy defined on the remote access server. Verify that a remote access policy applies to this user, and that the policy's permission setting grants access.
You've configured Callback but the remote access server isn't calling the client back.	Make sure that the correct "Always Callback to" telephone number is configured on the Dial-in tab in the user's Properties dialog box. Verify that LCP extensions are enabled on the PPP tab in the remote access server's Properties dialog box.
When a remote access client uses L2TP to initiate a VPN connection, the user is unable to connect. However, the remote access client *can* establish a VPN connection by using PPTP.	Ensure that computer (machine) certificates are installed on both the remote access server and the remote access client. (Certificate Services is covered in Chapter 18.).
A remote access client can access a Web server on the remote access server's local area network, but can't access a NetWare server on that network.	Ensure that the IPX protocol has been installed and configured on both the remote access client and the remote access server. Ensure that the "Enable network access for remote access clients and demand-dial connections" check box is selected on the IPX tab in the remote access server's Properties dialog box.

Continued ▶

TABLE 17-2 *(continued)*

Problem	Recommended Solution
A remote access client can connect to the remote access server, but can't access resources on the remote access server's local area network.	Make sure that the network protocol used by the remote access client is installed and configured on the remote access server. If the remote access client is using TCP/IP, ensure that the "Enable IP routing" check box is selected on the IP tab in the remote access server's Properties dialog box. If the remote access client is using NetBEUI, ensure that the "Allow NetBEUI based remote access clients to access" check box and the "The entire network" option are selected on the NetBEUI tab in the remote access server's Properties dialog box. If the remote access client is using AppleTalk, ensure that the "enable AppleTalk remote access" check box is selected on the AppleTalk tab in the remote access server's Properties dialog box.

▼ KEY POINT SUMMARY ▼

This chapter introduced several important remote access topics:

- Remote access is a feature that enables client computers to use dial-up and VPN connections to connect to a remote access server. Remote access is implemented on Windows 2000 Server computers through the Routing and Remote Access Service.
- Although the Routing and Remote Access service is installed by default on Windows 2000 Server computers, you must enable remote access.
- A virtual private network (VPN) connection is a virtual connection that is tunneled inside of an existing TCP/IP network connection. VPN connections can be established by using either PPTP or L2TP, and are commonly used between two computers that communicate over the Internet.
- A multilink connection permits a remote access client to combine the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, digital link, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support.

- The connection protocols Windows 2000 supports for remote access include Point-to-Point Protocol (PPP), Point-to-Point Multilink Protocol, Point-to-Point Tunneling Protocol, Layer Two Tunneling Protocol (L2TP), Serial Line Internet Protocol (SLIP), and the Microsoft RAS protocol (also called AsyBEUI).
- You can use Routing and Remote Access to configure numerous properties of a Windows 2000 remote access server, including: security options, PPP options, event logging options, and specific remote access options for installed protocols, such as TCP/IP, IPX, NetBEUI, and AppleTalk.
- RADIUS is an industry standard authentication service. IAS, which stands for Internet Authentication Service, is a Windows 2000 Server service that enables a Windows 2000 Server computer to function as a RADIUS server.
- You can also use Routing and Remote Access to configure inbound connection ports for remote access, which may include hardware ports (such as modems, parallel ports, infrared ports, and so on) and VPN ports, including PPTP and L2TP ports.
- In Windows 2000, access to the remote access server is controlled by remote access policies. A remote access policy consists of conditions, permissions, and a profile.
- A user can connect to a Windows 2000 remote access server *only* if a remote access policy permits the user to do so.
- Remote access policies are not stored in Active Directory. They are stored on the Windows 2000 remote access server.
- There are numerous options you can configure in a remote access policy's profile, including dial-in constraints, IP address assignment options, multilink connection options, authentication methods, encryption options, and advanced connection attributes.
- When multiple remote access policies exist, the remote access server selects the policy to apply to the connection by matching conditions of the connection to conditions of a remote access policy. Remote access policies are examined by the server in the order in which they appear in the Routing and Remote Access console.
- You can use Routing and Remote Access to monitor many aspects of remote access, including server status, ports, and connections. You can also configure logging of remote access events in this console.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about deploying Windows 2000 and to help you prepare for the Professional, Server, and Directory Services exams:

- **Assessment Questions:** These questions test your knowledge of the remote access topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenarios, you are asked to troubleshoot remote access problems and answer the question or questions listed for each problem. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab Exercise:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice enabling, configuring, and using remote access.

Assessment Questions

1. Your Windows 2000 domain operates in native-mode. You recently enabled remote access on a Windows 2000 Server computer on the network. What must you do before remote access users can connect to the remote access server?

   A. Authorize the Windows 2000 remote access server in Active Directory.

   B. Restart the Windows 2000 remote access server.

   C. Change the default remote access policy so that it grants remote access permission.

   D. Change the Windows 2000 remote access server's authentication provider to Windows Authentication.

2. What components make up a remote access policy? (Choose all that apply.)
   - A. Profile
   - B. Conditions
   - C. Encryption Settings
   - D. Permissions
3. Which authentication method supports smart cards?
   - A. Encrypted authentication (CHAP)
   - B. Extensible authentication protocol (EAP)
   - C. Shiva Password Authentication Protocol (SPAP)
   - D. Microsoft encrypted authentication version 2 (MS-CHAP v2)
4. Which authentication method provides the highest level of security?
   - A. Microsoft encrypted authentication version 2 (MS-CHAP v2)
   - B. Microsoft encrypted authentication (MS-CHAP)
   - C. Encrypted authentication (CHAP)
   - D. Shiva Password Authentication Protocol (SPAP)
5. Which remote access options can be configured on the Dial-in tab of a user's Properties dialog box? (Choose all that apply.)
   - A. Static IP address assignment
   - B. Allowed encryption methods
   - C. Callback options
   - D. Remote access permissions
   - E. Telephone number from which the user must dial-in
6. A remote user is attempting to connect to a Windows 2000 remote access server at 9 P.M. The user has the "Allow access" permission. The remote access server has only one remote access policy. The policy's only condition is a Day-And-Time-Restriction that permits access daily between 06:00 to 18:00. The policy's profile restricts access to 12:00 to 23:00 daily. How will the remote access server respond to the remote user's connection attempt?
   - A. The server will establish the connection for the remote user.
   - B. The server will deny access to the remote user because the remote access policy's condition prohibits connections at 9:00 P.M.

C. The server will deny access to the remote user because the remote access policy's profile prohibits connections at 9:00 P.M.

D. The server will deny access to the remote user because both the condition and profile of the remote access policy prohibit connections at 9:00 P.M.

7. You recently configured encryption options within a profile of a remote access policy.You only selected the check box next to "Strongest." Which encryption method can be used by remote access clients that establish PPTP VPN connections by using this remote access policy?

   A. IPSec 56-bit DES

   B. IPSec 3DES

   C. MPPE 56-bit

   D. MPPE 128-bit

8. Which tool can you use to add hardware ports to a Windows 2000 remote access server?

   A. Routing and Remote Access

   B. Add/Remote Programs

   C. Add/Remove Hardware

   D. `Network and Dial-up Connections` folder

Scenarios

Troubleshooting remote access on your network can be a difficult task. For each of the following problems, consider the given facts and answer the question or questions that follow.

1. A remote user reports that she is initially able to dial up to a Windows 2000 remote access server on your network, but as soon as the connection is established, she receives a message indicating that the remote access server will call her back. The connection is broken. However, the user doesn't receive a call back. What would you do to resolve the problem?

2. A remote user reports that he can't establish a VPN connection with a Windows 2000 remote access server on your network. When he attempts to connect, after typing in his correct user name and password, the following error message is displayed: **Error: 649: The account does not have permission to dial in.** The remote user is not able to establish the VPN connection. What steps would you take to troubleshoot this problem?
3. A remote user reports that he can successfully connect to the Windows 2000 remote access server and can access TCP/IP resources on the remote access server's local area network. However, the user is not able to access resources on a NetWare server located on the same network.
   - A. What is the most likely cause of the problem?
   - B. What steps would you take to resolve the problem?

Lab Exercise

Lab 17-1 Enabling, Configuring, and Monitoring Remote Access

MCSE EXAM MATERIAL

► Server
► Networking

The purpose of this lab is to provide you with an opportunity to practice enabling, configuring, and monitoring remote access in a Windows 2000 Server environment.

There are four parts to this lab:

- Part 1: Enabling and Configuring Remote Access
- Part 2: Creating and Configuring a Remote Access Policy
- Part 3: Connecting to the Remote Access Server
- Part 4: Monitoring Remote Access

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Enabling and Configuring Remote Access

In this part, you enable remote access on your Windows 2000 Server computer and then configure the remote access server. Specifically, you configure the remote access server to support multilink connections, configure remote access for DHCP integration, and configure security and authentication protocols. Finally, you create and configure inbound connection ports, including VPN ports.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, right-click SERVER01 (local) and select Properties from the menu that appears.
3. In the server's Properties dialog box, select the check box next to "Remote access server." Click the Security tab.
4. On the Security tab, ensure that the Authentication provider is Windows Authentication, and that the Accounting provider is Windows Accounting. Click Authentication Methods.
5. In the Authentication Methods dialog box, ensure that Microsoft encrypted authentication version 2 (MS-CHAP v2) and Microsoft encrypted authentication (MS-CHAP) are selected. Also select the check box next to Encrypted authentication (CHAP). Click OK. Click the IP tab.
6. On the IP tab, ensure that the check boxes next to "Enable IP routing" and "Allow IP-based remote access and demand-dial connections" are selected. Select the Dynamic Host Configuration Protocol (DHCP) IP address assignment option. Click the IPX tab.
7. On the IPX tab, clear the check box next to "Allow IPX-based remote access and demand-dial connections." Click the PPP tab.
8. Ensure that all four PPP options, including multilink connections, are selected on this tab. Click OK.
9. A Routing and Remote Access warning message appears, indicating that you must restart the Routing and Remote Access service. Click Yes. Windows 2000 stops and restarts the service. If a Routing and Remote Access dialog box appears asking if you want to view a help topic on authentication methods, click No.

10. In the left pane of the Routing and Remote Access dialog box, right-click the Ports container, and select Properties from the menu that appears.
11. In the Ports Properties dialog box, highlight WAN Miniport (PPTP) and click Configure.
12. In the Configure Device – WAN Miniport (PPTP) dialog box, ensure that the check box next to "Remote access connections (inbound only)" is selected. To create five additional PPTP ports, change the "Maximum ports" spin box to 10. Click OK.
13. In the Ports Properties dialog box, notice that the number of WAN Miniport (PPTP) ports is now 10. Click OK. Continue to Part 2.

Part 2: Creating and Configuring a Remote Access Policy

In this part, you create a new remote access policy that enables members of the Domain Admins group to connect to the Windows 2000 remote access server. You configure the policy's profile to require the use of an encryption protocol. You also configure remote access permissions in a user's Properties dialog box.

1. In the left pane of the Routing and Remote Access dialog box, right-click Remote Access Policies, and select New Remote Access Policy from the menu that appears.
2. In the Add Remote Access Policy dialog box, type in a policy friendly name of **Grant Administrators Dial-in Access**. Click Next.
3. In the Conditions screen, click Add.
4. In the Select Attribute dialog box, highlight Windows-Groups. Click Add.
5. In the Groups dialog box, click Add.
6. In the Select Groups dialog box, double-click the Domain Admins group. Click OK.
7. In the Groups dialog box, click OK.
8. In the Conditions screen, click Next.
9. In the Permissions screen, select the "Grant remote access permission" option. Click Next.
10. In the User Profile screen, click Edit Profile.
11. In the Edit Dial-in Profile dialog box, click the Authentication tab.

12. On the Authentication tab, clear the check box next to “Microsoft Encrypted Authentication (MS-CHAP).” Ensure that the check box next to “Microsoft Encrypted Authentication version 2 (MS-CHAP v2)” is selected. Click the Encryption tab.
13. On the Encryption tab, clear the check box next to No Encryption. Click OK.
14. In the User Profile screen, click Finish.
15. In the right pane of the Routing and Remote Access dialog box, right-click the Grant Administrators Dial-in Access policy. Select Move Up from the menu that appears, so that this policy is the first policy listed.
16. Close Routing and Remote Access.
17. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
18. In the left pane of Active Directory Users and Computers, highlight the `Users` folder. Then, in the right pane, right-click the Administrator user account, and select Properties from the menu that appears.
19. In the Administrator Properties dialog box, click the Dial-in tab.
20. On the Dial-in tab, select the “Control access through Remote Access Policy.” Click OK.
21. Close Active Directory Users and Computers.

Part 3: Connecting to the Remote Access Server

In this part, you use a VPN connection to connect to the remote access server.

1. Select Start ➪ Settings ➪ Network and Dial-up Connections.
2. In the `Network and Dial-up Connections` folder, right-click Virtual Private Connection, and select Properties from the menu that appears.
3. In the Virtual Private Connection Properties dialog box, clear the check box next to “Dial another connection first.” Click OK.
4. In the `Network and Dial-up Connections` folder, double-click Virtual Private Connection.
5. In the Connect Virtual Private Connection dialog box, accept the user name of Administrator and type in a password of **password**. Click Connect.

6. A Network Protocol Connection Result dialog box appears, informing you that TCP/IP connected successfully, but IPX did not. Select the check box next to "Do not request the failed protocols next time." Click Accept. The connection is established.
7. Close the `Network and Dial-up Connections` folder.

Part 4: Monitoring Remote Access

In this part, you monitor a VPN remote access connection and disconnect the remote access client.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Routing and Remote Access.
2. In the left pane of the Routing and Remote Access dialog box, highlight Remote Access Clients (1). In the right pane, double-click DOMAIN1\Administrator.
3. The Status dialog box appears. View the various statistics for your current remote access connection. Click Disconnect. Click Close.
4. In the Routing and Remote Access dialog box, notice that the connection no longer appears in the right pane. Close Routing and Remote Access.

Answers to Chapter Questions

Chapter Pre-Test

1. A virtual private network (VPN) is not a physical connection type. Rather, it's a virtual connection that is tunneled inside of an existing TCP/IP network connection. VPNs can be established by using either PPTP or L2TP. Both of these protocols support encryption of the data sent over the VPN connection. Because a VPN uses an existing TCP/IP network connection, no additional hardware is required. VPN connections are commonly used between two computers that communicate over the Internet.
2. Both PPTP and L2TP permit a virtual private network (VPN) connection between two computers over an existing TCP/IP network connection. The major difference between PPTP and L2TP is that PPTP uses Microsoft Point-to-Point Encryption (MPPE) while L2TP

uses IPSec for encryption. In addition, L2TP is rapidly becoming the industry standard tunneling protocol. Currently, only Windows 2000 remote access clients and remote access servers support L2TP.

3. TCP/IP, IPX (including NWLink IPX/SPX/NetBIOS Compatible Transport Protocol), NetBEUI, and AppleTalk
4. A multilink connection permits a remote access client to combine the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, digital link, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support.
5. The Routing and Remote Access service supports both hardware ports (such as modems, parallel ports, infrared ports, and so on) and VPN ports, including PPTP and L2TP ports.
6. A remote access policy consists of conditions, permissions, and a profile. Remote access policies are used to control access to the remote access server.

Assessment Questions

1. **C.** By default, the default remote access policy is configured to deny remote access permission. You must either modify the default remote access policy to grant remote access permission, create another remote access policy that grants permission to remote access users, or configure each remote user account's dial-in settings to "Allow access."
2. **A, B, D.** Remote access policies are composed of conditions, permissions, and a profile. While you can configure encryption options within a profile, it is not considered a part of the remote access policy.
3. **B.** Only the Extensible authentication protocol (EAP) has the ability to support smart cards.
4. **A.** Microsoft encrypted authentication version 2 (MS-CHAP v2) is the most secure authentication method.
5. **A, C, D, E.** All answer choices except encryption can be configured in the user's Properties dialog box. Encryption settings are configured in the profile portion of a remote access policy.

6. **B.** When a remote access server processes a connection attempt, it examines the conditions of a remote access policy first. Because there is only one policy on the remote access server, and the condition of that policy doesn't match the conditions of the connection attempt, the remote access server denies the connection.
7. **D.** Both IPSEC 3DES and MPPE 128 bit are "Strongest", however only MPPE 128 bit can be used with PPTP.
8. **C.** To add hardware ports, you can use either Add/Remove Hardware, or a specialized application such as Phone and Modem Options.

Scenarios

1. Ensure that the correct "Always Callback to" telephone number is configured on the Dial-in tab in the user's Properties dialog box, and instruct the user to only call in from that number. (It's possible that the callback telephone number is configured correctly, but the user is not calling from this telephone number.)
2. The most likely cause of this problem is the remote user is explicitly denied remote access permission, either on the Dial-in tab in the user's Properties dialog box, or by the remote access policy that applies to the remote user. To enable the remote user to access the remote access server, either grant the user the "Allow access" permission on the Dial-in tab, or reconfigure a remote access policy (that grants remote access permission) to include the user.
3. The most likely cause of this problem is that the remote access client, the remote access server, or both, are not correctly configured to support IPX on the remote access connection. To resolve the problem, ensure that NWLink IPX/SPX/NetBIOS Compatible Transport Protocol is installed and configured on both the remote access client and the remote access server. Also ensure that the "Enable network access for remote access clients and demand-dial connections" check box is selected on the IPX tab in the remote access server's Properties dialog box.