

## EXAM OBJECTIVES

Professional ▶

### Exam 70-210

- Configure and troubleshoot the TCP/IP protocol.

Server ▶

### Exam 70-215

- Install, configure, and troubleshoot network protocols.
- Install and configure network services.

Network ▶

### Exam 70-216

- Install, configure and troubleshoot DHCP.
  - Install the DHCP Server service.
  - Create and manage DHCP scopes, superscopes, and multicast scopes.
  - Configure DHCP for DNS integration.
  - Authorize a DHCP server in Active Directory.
- Manage and monitor DHCP.
- Install, configure, and troubleshoot network protocols.
  - Install and configure TCP/IP.

- Configure TCP/IP packet filters.
- Configure and troubleshoot network protocol security.
- Configure and troubleshoot IPsec.
  - Enable IPsec.
  - Configure IPsec for transport mode.
  - Configure IPsec for tunnel mode.
  - Customize IPsec policies and rules.
  - Manage and monitor IPsec.
- Install, configure, and troubleshoot WINS.
- Configure WINS replication.
- Configure NetBIOS name resolution.
- Manage and Monitor WINS.
- Install, configure, and troubleshoot IP routing protocols.
  - Update a Windows 2000-based routing table by means of static routes.
  - Implement Demand-Dial Routing.

---

**EXAM OBJECTIVES** *(continued)*

- Manage and monitor IP routing.
    - Manage and monitor border routing.
    - Manage and monitor internal routing.
    - Manage and monitor IP routing protocols.
  - Install NAT.
  - Configure NAT properties.
  - Configure NAT interfaces.
-

# Networking with TCP/IP

# 16

**C**hapter 16 focuses on TCP/IP and several TCP/IP-related features as they are used on a Windows 2000 network. After a brief overview of TCP/IP, I'll discuss IP addressing and how to configure TCP/IP. Next, I'll cover how to install and configure a DHCP server, which is frequently used to automatically provide IP addressing information to client computers. Then I'll move on to the topic of NetBIOS name resolution, where I'll explain how to use `lmhosts` files or a WINS server to resolve NetBIOS names.

Next, I'll explore routing in a Windows 2000 Server environment. In this section you'll discover the differences between static and dynamic routing. Then I'll show you how to configure a router, as well as how to manage ports, routing interfaces, and demand-dial routing. I'll also introduce you to the numerous routing protocols that ship with Windows 2000 Server. Finally, I'll cover monitoring and troubleshooting TCP/IP routing.

In the last part of this chapter, I'll explain how to implement two TCP/IP security features: TCP/IP packet filtering and IPSec.

## *Chapter Pre-Test*

1. What is TCP/IP?
2. True or False: All computers located on the same network segment should have the same network ID.
3. What does a default gateway address specify?
4. What are the two ways in which you can assign an IP address to a Windows 2000 computer?
5. What is a DHCP scope?
6. What is WINS?
7. How can you enable routing on a Windows 2000 Server computer?
8. What are the five routing protocols that ship with Windows 2000 Server?
9. What are two security features of TCP/IP in Windows 2000?

## Overview of TCP/IP

The Transmission Control Protocol/Internet Protocol (*TCP/IP*) is a widely used transport protocol that provides robust capabilities for Windows 2000 networking.



### TIP

In the Windows 2000 interface, TCP/IP is called “Internet Protocol (TCP/IP).” But I prefer to simply call it what it is – TCP/IP.

TCP/IP is a fast, routable enterprise protocol that is used on the Internet. In addition to being supported by Windows 2000, TCP/IP is supported by many other operating systems, including: Windows 95, Windows 98, Windows NT, NetWare, Macintosh, UNIX, MS-DOS, and IBM mainframes. TCP/IP is typically the recommended protocol for large, heterogeneous networks.

Microsoft includes several TCP/IP-based protocols and services with Windows 2000 that enhance networking, including: the Dynamic Host Configuration Protocol (DHCP) service, the Domain Name System (DNS) service, Windows Internet Name Service (WINS), RIP Version 2 for Internet Protocol, Open Shortest Path First (OSPF), Network Address Translation (NAT), IGMP, and IPsec. I’ll discuss each of these protocols and services in this chapter.

By now, you’re probably getting the idea that TCP/IP is a huge topic — and you’re right. Although volumes have been written on this subject, this chapter covers only the basics of TCP/IP that are required for the Network exam, and also for the Professional and Server exams.

A good place to begin a basic discussion of TCP/IP is with IP addressing, including subnet masks, default gateway addresses, and DNS server addresses.

## IP Addressing

An *IP address* is a 32-bit binary number, broken into four 8-bit sections (often called octets), that uniquely identifies a computer or other network device on a network that uses TCP/IP. IP addresses must be unique — *no two computers or other network devices on an internetwork should have the same IP address*. If two computers have the same IP address, one or both of the computers may be unable to communicate over the network. An IP address is not the same as a network adapter card’s hardware (or MAC) address.

Although an IP address is a 32-bit binary number, it is normally represented in a dotted decimal format. Each 8-bit octet is represented by a whole decimal number between 0 and 255. The following numbers are sample IP addresses:

192.168.59.5

172.31.151.1

An IP address contains two important identifiers: a network ID and a host ID. One portion of each IP address identifies the network segment on which a computer (or other network device) is located. This portion is called the *network ID*. All computers located on the same network segment should have the *same* network ID. The portion of the IP address used for the network ID is variable and is specified by the subnet mask used in conjunction with the IP address. (I'll discuss subnet masks in more detail in the next section.)

The second portion of each IP address identifies the individual computer or network device. This portion is called the host ID. Each computer or other network device on a given network segment *must* have a unique host ID.

To ensure that unique IP addresses are used, if you plan to connect your network to the Internet, you should contact your Internet service provider (ISP) to obtain a range of valid IP addresses for your network.

## Subnet Masks

A *subnet mask* specifies which portion of an IP address represents the network ID and which portion represents the host ID. A subnet mask allows TCP/IP to determine whether network traffic destined for a given IP address should be transmitted on the local subnet, or whether it should be routed to a remote subnet. A subnet mask should be the *same* for all computers and other network devices on a given network segment.

A subnet mask is a 32-bit binary number, broken into four 8-bit sections (octets), that is normally represented in a dotted decimal format. Each 8-bit section is represented by a whole number between 0 and 255.

A common subnet mask is 255.255.255.0. This particular subnet mask specifies that TCP/IP will use the first three octets of an IP address as the network ID, and will use the last octet as the host ID. This subnet mask is some-

times referred to as a 24-bit subnet mask, because when 255.255.255.0 is converted to a 32-bit binary number, the first 24 bits of this number are all 1's.

Another common subnet mask is 255.255.0.0. This subnet mask specifies that TCP/IP will use the first two octets of an IP address as the network ID, and will use the last two octets as the host ID. This subnet mask is sometimes referred to as a 16-bit subnet mask, because when 255.255.0.0 is converted to a 32-bit binary number, the first 16 bits of this number are all 1's.

There are two ways that subnets masks are commonly presented. First, a subnet mask can be presented in dotted decimal format in conjunction with its network ID. An example of this presentation is 192.168.59.0 255.255.255.0. In this example, 192.168.59.0 specifies the network id, and 255.255.255.0 specifies that 24 bits (the first three octets) are used as the subnet mask. Recently, a shortcut notation has come into common use, where the network id and subnet mask combination in the previous example would be expressed as 192.168.59.0/24. In this shortcut notation, 192.168.59.0 specifies the network ID, and /24 specifies that a 24-bit subnet mask (255.255.255.0) is used.

Without getting into too much binary math, an octet number of 255 specifies that the *entire* octet is part of the network ID, and an octet number of 0 specifies that the *entire* octet is part of the host ID. Numbers between 0 and 255 specify that part of the octet corresponds to the network ID, and the remaining part corresponds to the host ID.



#### TIP

For more information on subnetting and subnet masks, see *Network+ Certification Study System*, by Joseph J. Byrne (IDG Books Worldwide).

Table 16-1 lists all of the subnet masks normally used on TCP/IP networks, the number of bits specified by each subnet mask, and the maximum number of host IDs that can be used on a single subnet with that subnet mask.

**TABLE 16-1 Common Subnet Masks**

Subnet mask	Number of bits specified by the subnet mask	Maximum number of host IDs that can be used on a single subnet with this subnet mask
255.0.0.0	8	16,777,214
255.128.0.0	9	8,388,606

*Continued* ►



TABLE 16-1 (continued)

Subnet mask	Number of bits specified by the subnet mask	Maximum number of host IDs that can be used on a single subnet with this subnet mask
255.192.0.0	10	4,194,302
255.224.0.0	11	2,097,150
255.240.0.0	12	1,048,574
255.248.0.0	13	524,286
255.252.0.0	14	262,142
255.254.0.0	15	131,070
255.255.0.0	16	656,534
255.255.128.0	17	32,766
255.255.192.0	18	16,382
255.255.224.0	19	8,190
255.255.240.0	20	4,094
255.255.248.0	21	2,046
255.255.252.0	22	1,022
255.255.254.0	23	510
255.255.255.0	24	254
255.255.255.128	25	126
255.255.255.192	26	62
255.255.255.224	27	30
255.255.255.240	28	14
255.255.255.248	29	6
255.255.255.252	30	2

If subnet masks are incorrectly configured, network communications problems due to routing errors may occur. For example, TCP/IP may incorrectly determine that a computer on the local subnet is located on a remote subnet and attempt to route a packet to the remote subnet. In this instance, the computer on the local subnet would never receive the packet intended for it.

## Default Gateway Addresses

A *default gateway* address specifies the IP address of a router on the local network segment. When a computer that uses TCP/IP determines that the computer it wants to communicate with is located on a remote subnet, it sends all network messages intended for the remote computer to the default gateway address, instead of directly to the destination computer. Then the router on the local subnet specified by the default gateway address forwards the messages to the destination computer on the remote subnet, either directly or via other routers.

If a computer's default gateway address does not specify a router on the local subnet, then that computer will be unable to communicate with computers or other network devices located on other network segments.

When a router is used to connect two network segments, it has two network adapter cards and two IP addresses. Figure 16-1 illustrates how default gateway addresses are used to specify the IP address of a router on the local subnet.

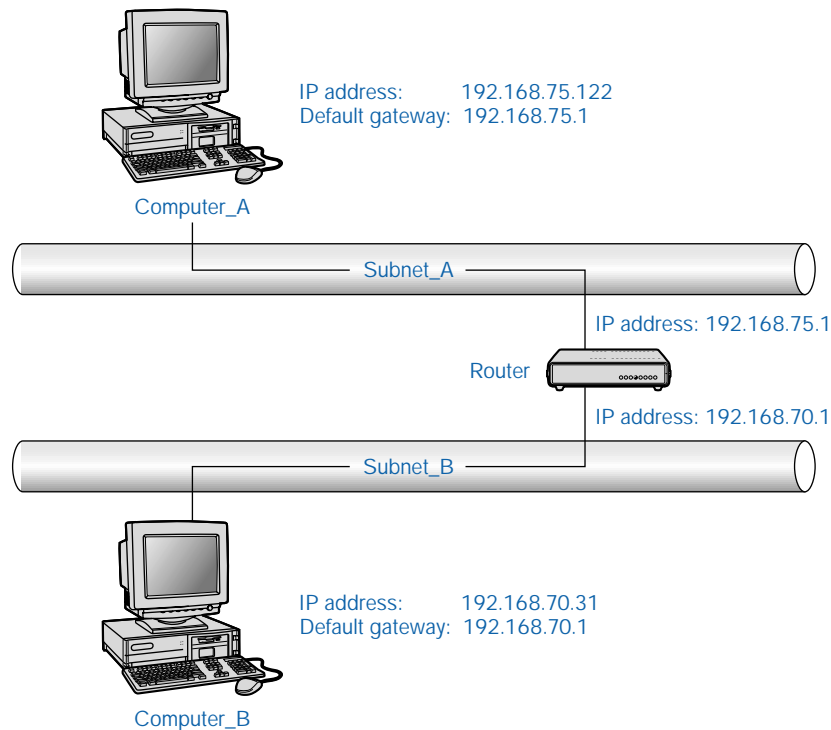


FIGURE 16-1 Default gateway addresses specify a local router

Notice in Figure 16-1 that the default gateway address of Computer\_A matches the IP address of its local router, and the default gateway address of Computer\_B matches the IP address of its local router.

## DNS Server Addresses

A DNS server address specifies the IP address of a DNS server on your company's network. The DNS server does not have to reside on the local network segment. A DNS server address, like all other IP addresses, is a 32-bit binary number, broken into four 8-bit sections (octets), that is normally represented in a dotted decimal format.

When a Windows 2000 computer wants to resolve a host name or an FQDN to an IP address, it sends the host name or FQDN to the DNS server for name resolution. The DNS server then performs the resolution and returns the IP address of the host name or FQDN to the requesting computer.

All client computers on a Windows 2000 network use DNS servers to locate Active Directory domain controllers. Because of this, if a client computer is not configured with the address of a DNS server, it won't be able to function on the network.

## Configuring TCP/IP

IP addresses must be configured on each connection in a Windows 2000 computer when TCP/IP is installed. Because TCP/IP is automatically installed during most installations of Windows 2000, IP address configuration is often done as part of the installation process. After the installation of Windows 2000, when a new connection is created, it is configured, by default, to receive its IP addressing information from a DHCP server.

You can assign an IP address to a Windows 2000 computer in one of two ways: by manually specifying a computer's IP address configuration, or by configuring a computer to obtain IP addressing information automatically from a DHCP server.

### Manually Configuring TCP/IP

IP addresses are typically configured manually only when a DHCP server is not available, or when the computer being configured requires a static IP

address. Configuring IP addresses manually is both more time-consuming than using a DHCP server and more prone to error, because an IP address must be manually typed for each connection on each individual computer. However, configuring an IP address manually is sometimes the only way to get the job done.

## STEP BY STEP

### CONFIGURING AN IP ADDRESS MANUALLY

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the **Network and Dial-up Connections** folder, right-click the connection for which you want to configure IP addressing information, and select Properties from the menu that appears.



#### TIP

When you're configuring TCP/IP addressing information on a Windows 2000 computer so it can function on your company's local area network, you would normally select the computer's Local Area Connection during this step.

3. If the connection you selected is not a local area connection, in the connection's Properties dialog box, click the Networking tab.  
Then, for all connection types, highlight Internet Protocol (TCP/IP) and click Properties.
4. The Internet Protocol (TCP/IP) Properties dialog box appears, as shown in Figure 16-2. Notice the IP address, Subnet mask, Default gateway, and Preferred DNS server text boxes.

Ensure that the "Use the following IP address" option is selected. Then complete the following text boxes:

- ▶ **IP address:** Enter the IP address you want to assign to this connection. This is a mandatory setting.
- ▶ **Subnet mask:** Enter the subnet mask you want to assign to this connection. This is a mandatory setting.
- ▶ **Default gateway:** Enter the default gateway address that will be used by this connection. This is an optional setting. However, if you don't configure this setting, this computer won't be able to communicate with computers located on other network segments.

If you want the computer to use a DNS server, complete the following text boxes:

- ▶ **Preferred DNS server:** Enter the IP address of the DNS server you want this connection to use.

## STEP BY STEP

Continued

- **Alternate DNS server:** Optionally, you can enter the IP address of an additional DNS server that will be used by this connection if the preferred DNS server is not available.

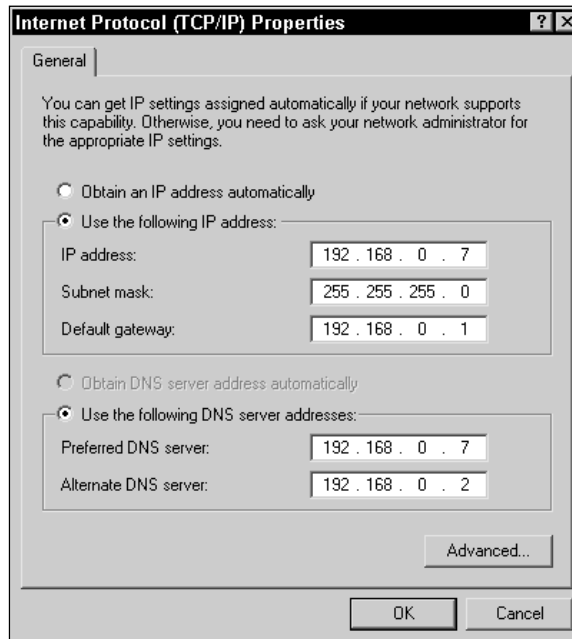


FIGURE 16-2 Manually configuring IP addressing information

Click OK.

5. In the connection's Properties dialog box, click OK.
6. Close the **Network and Dial-up Connections** folder.

## Configuring TCP/IP by Using a DHCP Server

The most convenient method for assigning IP addresses to multiple computers, in terms of administration time required, is to configure each of the computers to obtain its IP address from a Dynamic Host Configuration Protocol (DHCP) server. When a client computer obtains an IP address from a DHCP server, the DHCP server assigns that client computer the next available IP address. That IP address is leased to the client computer for a specific period of time, usually several days. The client computer can

then renew that lease, enabling a client computer to use the same IP address indefinitely, unless the computer is turned off for several days (long enough for the lease to expire).

Assigning IP addresses by using a DHCP server is the preferred method because:

- Using a DHCP server makes it possible for you to manage IP addresses centrally, thus ensuring that addresses are valid and not duplicated.
- Using a DHCP server reduces the amount of administration time required to manage and maintain IP addresses for each connection on each computer on the network.
- Using a DHCP server reduces the likelihood of human error when IP addresses are assigned, because no need exists to enter an IP address manually for each connection on every individual computer.
- Using a DHCP server enables an administrator to centrally change the IP address that each client computer uses to contact a DNS or WINS server, instead of having to manually reconfigure each client computer.
- Using a DHCP server enables you to regain the use of an IP address no longer assigned to a host when the DHCP lease period for this IP address expires.

Before you can assign an IP address to a connection on a Windows 2000 computer by using a DHCP server, you must have a DHCP server on your network. (I'll explain how to install and configure a DHCP server a little later in this chapter.)

## STEP BY STEP

### CONFIGURING A COMPUTER TO OBTAIN AN IP ADDRESS FROM A DHCP SERVER

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the **Network and Dial-up Connections** folder, right-click the connection for which you want to configure automatic IP addressing, and select Properties from the menu that appears.
3. If the connection you selected is not a local area connection, in the connection's Properties dialog box, click the Networking tab.

## STEP BY STEP

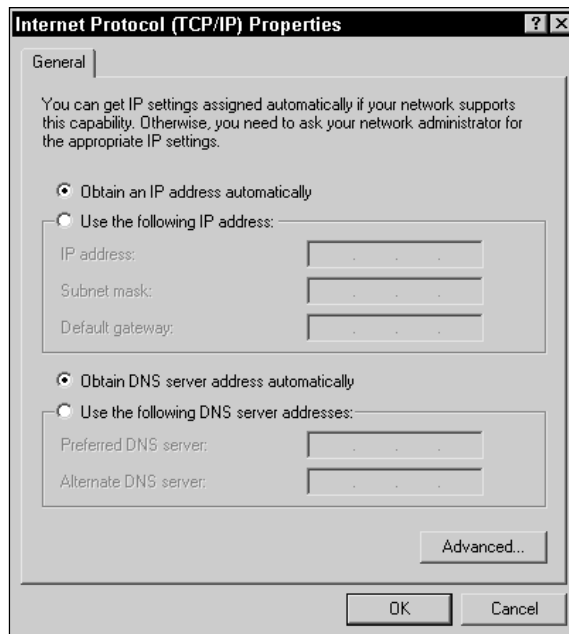
Continued

Then, for all connection types, highlight Internet Protocol (TCP/IP) and click Properties.

4. In the Internet Protocol (TCP/IP) Properties dialog box, select the “Obtain an IP address automatically” option.

If you also want a DNS server address to be automatically assigned, select the “Obtain DNS server address automatically” option.

Figure 16-3 shows a connection configured to receive both its IP addressing information and its DNS server address automatically. Click OK.



**FIGURE 16-3** Configuring a connection to automatically obtain IP addressing information

5. In the connection's Properties dialog box, click OK.
6. Close the **Network** and **Dial-up Connections** folder.

## Troubleshooting TCP/IP Configuration Problems

There are several common TCP/IP connectivity problems. Most TCP/IP connectivity problems are caused by incorrectly configured TCP/IP settings on the computer that is experiencing the problem.

TCP/IP connectivity problems commonly reported by users include:

- A user is unable to access a computer located on another subnet.
- A user is unable to access the Internet.
- A user is unable to access computers on both the local and remote subnets.
- TCP/IP fails to initialize on the user's computer.

When troubleshooting a TCP/IP connectivity problem, carefully check the TCP/IP settings on the computer experiencing the problem, including the IP address, subnet mask, default gateway, and DNS server address.

- **IP address:** Make sure the computer's IP address is not a duplicate of another IP address used on the network, and that it is an appropriate IP address for the local subnet. Remember that the network ID portion of the IP address must be the same for all computers on the local subnet.
- **Subnet mask:** Ensure that the computer's subnet mask is the same subnet mask used by all computers and routers located on that subnet.
- **Default gateway:** Ensure that the computer's default gateway address matches the IP address of a router on the local subnet.
- **DNS server address:** Ensure that the computer's DNS server address matches the IP address of your company's DNS server.

Two command-line utilities that can help when you're troubleshooting TCP/IP connectivity problems are `ipconfig.exe` and `ping.exe`.

`ipconfig.exe` displays the computer's current IP configuration settings, including IP address, subnet mask, and default gateway. To use `ipconfig.exe`, select Start ⇨ Programs ⇨ Accessories ⇨ Command Prompt. At the command prompt, type **ipconfig** and press Enter. To view detailed IP addressing for all connections on the computer, at the command prompt, type **ipconfig /all** | **more** and press Enter.

`Ping.exe` verifies network communications between the local computer and any other computer specified on the network. To use `ping.exe`, select Start ⇨ Programs ⇨ Accessories ⇨ Command Prompt. At the command prompt, type **ping IP\_address** and press Enter. (The IP address entered should be the IP address of the computer with which you are attempting to communicate. Alternatively, instead of typing an IP address



you can type the host name or FQDN of the computer with which you are trying to communicate.) If your computer is able to communicate with the remote computer specified, `ping.exe` displays four replies from the remote computer. The following is an example of a successful ping response.

```
Reply from 192.168.59.5: bytes=32 time<10ms TTL=128
Reply from 192.168.59.5: bytes=32 time<10ms TTL=128
Reply from 192.168.59.5: bytes=32 time<10ms TTL=128
Reply from 192.168.59.5: bytes=32 time<10ms TTL=128
```

If your computer is unable to communicate with the remote computer specified, `ping.exe` usually displays “Request timed out.” four times.

You can ping your own computer’s IP address to determine whether TCP/IP is correctly configured and initialized on the local computer. If TCP/IP is correctly configured on the local computer, `ping.exe` will display four replies from the local computer.

## Installing and Configuring a DHCP Server

Microsoft includes a DHCP server product with Windows 2000 Server (and Advanced Server), called the Dynamic Host Configuration Protocol (DHCP) service. (I’ll call this the DHCP service for short.) The DHCP service provides centralized management of IP address assignment. The DHCP service can be installed on any Windows 2000 Server computer that has a manually assigned static IP address for each connection on the computer. When the DHCP service is installed and configured on a Windows 2000 Server computer, that computer becomes a DHCP server.



### EXAM TIP

The Network exam has six objectives on DHCP. Be sure you’re good and comfortable with all facets of DHCP before you take the Network exam.

In the next few sections I’ll show you how to install the DHCP service; how to authorize a DHCP server in Active Directory; how to configure DHCP for integration with a DNS server; how to configure DHCP scopes, superscopes, and multicast scopes; and how to monitor a DHCP server. I’ll also provide you with some tips for troubleshooting DHCP.

## Installing the DHCP Service

Before you can install the DHCP service on a Windows 2000 Server/Advanced Server computer, TCP/IP must be installed on the computer, and a static IP address must be manually configured for each connection in the Windows 2000 computer.

### STEP BY STEP

#### INSTALLING DHCP

1. Select Start ⇨ Settings ⇨ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, highlight Networking Services, and click Details.
5. In the Networking Services dialog box, select the check box next to Dynamic Host Configuration Protocol (DHCP), and click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. Windows 2000 configures components and installs DHCP. In the Completing the Windows Components Wizard screen, click Finish.
8. Close Add/Remove Programs. Then close Control Panel.

## Authorizing a DHCP Server in Active Directory

When the DHCP service is installed on a Windows 2000 Server computer that is a member of a domain (either a member server or a domain controller), before the service can start, the service must be authorized in Active Directory for that specific computer. This is referred to as “authorizing a DHCP server in Active Directory.”

The purpose of authorizing DHCP servers in Active Directory is to prevent nonauthorized DHCP servers from disrupting network communications. Only Windows 2000 DHCP servers that are installed, configured, and authorized by an Administrator are permitted to start and run on the network. This feature can prevent an employee from accidentally creating a DHCP server containing inappropriate IP address assignments,

which could wreak havoc on your company's network. Such an unauthorized DHCP server is sometimes referred to as a "rogue" DHCP server.

Only Windows 2000 DHCP servers must be authorized in Active Directory — DHCP servers on computers that run Windows NT, UNIX, or other operating systems don't need to be authorized.

When the DHCP service is installed on a Windows 2000 Server computer that is *not* a member of a domain, the DHCP server does not need to be authorized in Active Directory.

You can use the DHCP administrative tool to authorize a DHCP server in Active Directory, as the steps that follow explain. You can also perform this task in Computer Management.

## STEP BY STEP

### AUTHORIZING A DHCP SERVER

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, highlight the DHCP server you want to authorize. Select Action ⇨ Authorize.
3. Wait a minute or two, then select Action ⇨ Refresh.
4. The DHCP Server is now authorized. Notice that the icon next to the DHCP server now contains a green, upward pointing arrow (instead of a red, downward pointing arrow).
5. Close DHCP.

## Configuring DHCP for DNS Integration

By default, all Windows 2000 computers that have TCP/IP installed automatically register their IP address and host name information with the DNS server on the network (if the DNS server supports dynamic updates). Not all computers support this feature. For example, Windows NT, Windows 95, and Windows 98 computers aren't capable of dynamically registering their IP address and host name information with a DNS server.

To overcome this limitation, you can configure your Windows 2000 DHCP server to dynamically register the IP address and host name information of Windows-based client computers with a DNS server on the network. This is often called "configuring a DHCP server for DNS integration."

**TIP**

Windows 2000 computers only register their host name to IP address information (called forward lookup information) with the DNS Server. Windows 2000 computers do not register their IP address to Host name information (called reverse lookup information) with the DNS server. If you want to register reverse lookup information, you must configure the DHCP server to perform DNS registration.

In order for this feature to be implemented, the DNS server must support dynamic updates. If your DNS server is a Windows 2000 Server computer running the Windows 2000 Domain Name System (DNS) service, you shouldn't have any problems here, because the Windows 2000 DNS service fully supports dynamic updates.

**STEP BY STEP****CONFIGURING A DHCP SERVER FOR DNS INTEGRATION**

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, highlight the DHCP server you want to configure for DNS integration. Select Action ⇨ Properties.
3. In the DHCP server's Properties dialog box, click the DNS tab.
4. The DNS tab appears, as shown in Figure 16-4. Notice the blank check box next to "Enable updates for DNS clients that do not support dynamic update."

To configure the DHCP server to provide IP address and host name information of Windows-based (but non-Windows 2000) client computers to the DNS server, select the check box next to "Enable updates for DNS clients that do not support dynamic update."

In addition, if you want the DHCP server to update the DNS server for Windows 2000 client computers, even if the clients don't request this update, select the "Always update DNS" option. Selecting this option ensures that the DNS server has the most recent IP address and host name information for Windows 2000 client computers, and it also registers reverse lookup information for Windows 2000 client computers.

Click OK.

5. Close DHCP.

## STEP BY STEP

Continued

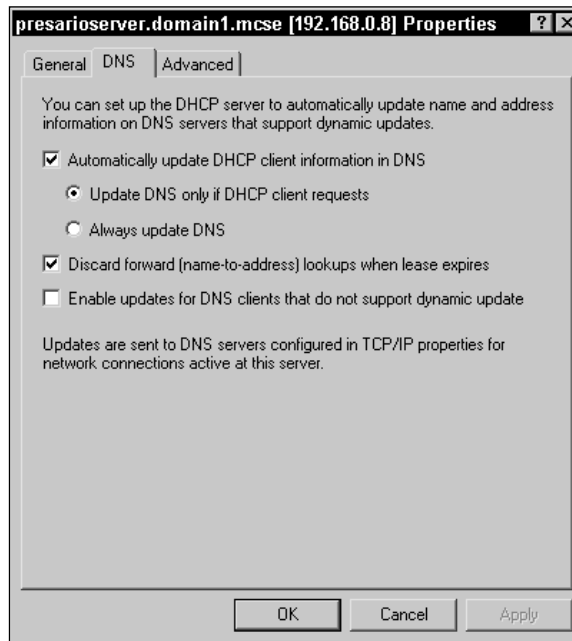


FIGURE 16-4 The DNS tab

## DHCP Scopes, Superscopes, and Multicast Scopes

A DHCP *scope* is a range of IP addresses on a DHCP server that can be assigned to DHCP clients that reside on a single subnet. You must create at least one scope on a DHCP server before it can assign IP addresses to DHCP clients. In addition to a regular DHCP scope, there are two special kinds of DHCP scopes you should know about:

- **Superscope:** This type of scope contains a range of IP addresses that spans several subnets. In fact, a superscope actually contains several scopes — one for each subnet spanned by the superscope's range. Because of this, a superscope can be used to assign IP addresses to client computers on multiple subnets.

- **Multicast scope:** This type of scope contains a range of Class D multicast IP addresses, and is used to assign these addresses to client computers that request them. I'll get into more details about this type of scope a little later in this chapter.

By default, no scopes exist on a Windows 2000 DHCP server. Until you create at least one scope, the DHCP server can't assign IP addresses to client computers, because it doesn't have any IP addresses to assign. I'll show you how to create these different types of scopes in the sections that follow.

## Creating DHCP Scopes and Superscopes

The task of creating a DHCP scope or superscope is fairly straightforward. The only difference between creating a scope and a superscope is the range of IP addresses you assign to the scope — a scope is assigned a range of IP addresses that can be assigned to DHCP clients that reside on a single subnet, and a superscope is assigned a range of IP addresses that can be assigned to DHCP clients that reside on multiple subnets.

You can use the DHCP administrative tool (or Computer Management) to create scopes.

### STEP BY STEP

#### CREATING A SCOPE

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, highlight the DHCP server on which you want to create a scope. Select Action ⇨ New Scope.
3. The New Scope wizard starts. Click Next.
4. In the Scope Name screen, type in a name and a description for the scope in the text boxes provided. Click Next.
5. The IP Address Range screen appears. In the "Start IP address" and "End IP address" text boxes, enter the IP addresses that will define the range of the scope.

To configure the subnet mask for the scope, you can either type in the subnet mask in the "Subnet mask" text box, or you can specify the length of the subnet mask as whole number between 1 and 31. If you enter a number in the Length spin box, the subnet mask is automatically calculated for you. Click Next.

Figure 16-5 shows the IP Address Range screen after it has been configured with a range of IP addresses that spans multiple subnets, and after its subnet mask has been configured.

## STEP BY STEP

Continued

6. If you configured a range of IP addresses in Step 5 that spans *more than one subnet*, the Create Superscope screen is displayed. If you want to create a superscope, select the Yes option and click Next. If you don't want to create a superscope, click Back and reconfigure your IP address range to only include IP addresses from a single subnet.

**New Scope Wizard**

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length:

Subnet mask:

< Back   **Next >**   Cancel

**FIGURE 16-5** Configuring the IP address range of a scope

If you configured a range of IP addresses in Step 5 from *only one subnet*, the Add Exclusions screen is displayed. In this screen, you can specify IP addresses (or ranges of IP addresses) within the scope that will not be assigned to DHCP client computers by the DHCP server.



## TIP

You should exclude from the scope IP addresses of any computers, such as routers and DHCP servers, that have been assigned static IP addresses.

To exclude IP addresses, enter the start and end IP address of the range you want to exclude and click Add. (If you only want to exclude a single IP address, use this IP address as both the start and end IP address of the exclusion range.) When you finish configuring exclusions, click Next.

7. In the Lease Duration screen, either accept the default DHCP lease duration of eight days, or configure a custom lease duration. Click Next.

## STEP BY STEP

Continued

8. In the Configure DHCP Options screen, choose whether to configure DHCP options for this scope (such as routers, DNS, and WINS settings) now. For completeness, I'll assume you choose the Yes option. Click Next.
9. In the Router (Default Gateway) screen, enter the IP address of the router that will function as the default gateway for this scope and click Add. Click Next.
10. In the Domain Name and DNS Servers screen, in the "Parent domain" text box, enter the name of the domain that DHCP client computers that obtain IP addresses from this scope are members of.  
  
Then, either specify the name of the DNS server on your network and click Resolve, or enter the IP address of the DNS server. Click Add. If you have more than one DNS server, you can repeat this process and click Add again. If you have more than one DNS server, the first DNS server in the list becomes the primary DNS server for the DHCP client computers. Click Next.
11. In the WINS Servers screen, either specify the name of the WINS server on your network and click Resolve, or enter the IP address of the WINS server. Click Add. If you have more than one WINS server, you can repeat this process and click Add again. If you have more than one WINS server, the first WINS server in the list becomes the primary WINS server for the DHCP client computers. Click Next.  
  
Or, if you don't have a WINS server on your network, just click Next.
12. In the Activate Scope screen, select whether to activate this scope now. Your options are Yes or No. A DHCP server can't assign addresses from a scope until the scope is activated. Make your selection and click Next.
13. In the Completing the New Scope Wizard screen, click Finish.
14. Windows 2000 creates the scope. It is displayed in the right pane of the DHCP dialog box. Close DHCP.

---

Another way to create a superscope is to first create multiple scopes, and then to use the New Superscope wizard to combine these existing scopes into a superscope. You can start this wizard by selecting Action ⇨ New Superscope in DHCP. This method is sometimes preferred if the ranges of IP addresses you want to include in the superscope are not contiguous.

### Creating DHCP Multicast Scopes

*Multicasting* is the process of sending packets to all client computers on a routed (or nonrouted) TCP/IP network that have joined a specific multicast group. A multicast group is defined by a single multicast IP address.



The purpose of multicasting is to enable a computer to send data once, and to have that data delivered to all computers on a network that are members of the multicast group. Multicasting is primarily used to transmit multimedia data, such as a televised speech or a radio program, to multiple users on a routed TCP/IP network.

IP addresses that are reserved specifically for multicasting are called *Class D IP addresses*. Only IP addresses from 224.0.0.0 to 239.255.255.255 may be used in a multicast scope. A DHCP server can then use this multicast scope to assign these addresses to client computers that request them. For example, a multimedia application on a server might request a multicast IP address from the DHCP server in order to establish a multicast group. Then the multimedia application can transmit multimedia data to members of that group.

The multimedia application must use the Multicast Address Dynamic Client Allocation Protocol (MADCAP) when it requests a multicast IP address from the DHCP server. A DHCP server that is configured with a multicast scope is also referred to as a MADCAP server.

You can use the DHCP administrative tool (or Computer Management) to create multicast scopes.

## STEP BY STEP

### CREATING A MULTICAST SCOPE

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, highlight the DHCP server on which you want to create a multicast scope. Select Action ⇨ New Multicast Scope.
3. The New Multicast Scope wizard starts. Click Next.
4. In the Multicast Scope Name screen, type in a name and a description for the multicast scope in the text boxes provided. Click Next.
5. The IP Address Range screen appears. In the "Start IP address" and "End IP address" text boxes, enter the IP addresses that will define the range of this multicast scope. Only Class D IP addresses from 224.0.0.0 to 239.255.255.255 may be used.

In the TTL (Time to Live) spin box, enter the maximum number of routers through which multicast packets can pass. The default TTL is 32. The range is from 1 to 255. Click Next.

6. The Add Exclusions screen is displayed. In this screen, you can specify IP addresses (or ranges of IP addresses) within the multicast scope that will not be assigned to DHCP client computers by the DHCP server.

**STEP BY STEP***Continued*

To exclude IP addresses, enter the start and end IP address of the range you want to exclude and click Add. (If you only want to exclude a single IP address, use this IP address as both the start and end IP address of the exclusion range.) When you finish configuring exclusions, click Next.

7. In the Lease Duration screen, either accept the default DHCP multicast lease duration of 30 days, or configure a custom lease duration. Click Next.
8. In the Activate Multicast Scope screen, select whether to activate this multicast scope now. Your options are Yes or No. A DHCP server can't assign addresses from a multicast scope until the scope is activated. Make your selection and click Next.
9. In the Completing the New Multicast Scope Wizard screen, click Finish.
10. Windows 2000 creates the multicast scope. It is displayed in the right pane of the DHCP dialog box. Close DHCP.

## Configuring DHCP Options

DHCP options are additional configuration settings, such as IP addresses for routers, DNS servers, and WINS servers. You can set DHCP options by using either Server Options or Scope Options within the DHCP administrative tool.

When you use Server Options, all configuration settings apply to all scopes on the DHCP server. When you use Scope Options, all configuration settings apply only to the specific scope you're configuring. Settings made by using Scope Options will override conflicting settings made by using Server Options.

The steps involved in configuring DHCP options are the same regardless of whether you use Server Options or Scope options.

**STEP BY STEP**

### CONFIGURING DHCP OPTIONS

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, expand the DHCP server (and its scopes) until the **Scope Options** and **Server Options** folders are displayed.

## STEP BY STEP

Continued

If you want to configure *server* options, right-click the **Server Options** folder and select **Configure Options** from the menu that appears.

If you want to configure *scope* options, right-click the **Scope Options** folder, and select **Configure Options** from the menu that appears.

3. The **Server Options** or **Scope Options** dialog box appears. In the **Available Options** list, select the check box next to the option you want to configure. Once you select the check box, the configurable options for this item are displayed in the bottom portion of the dialog box, as shown in Figure 16-6.

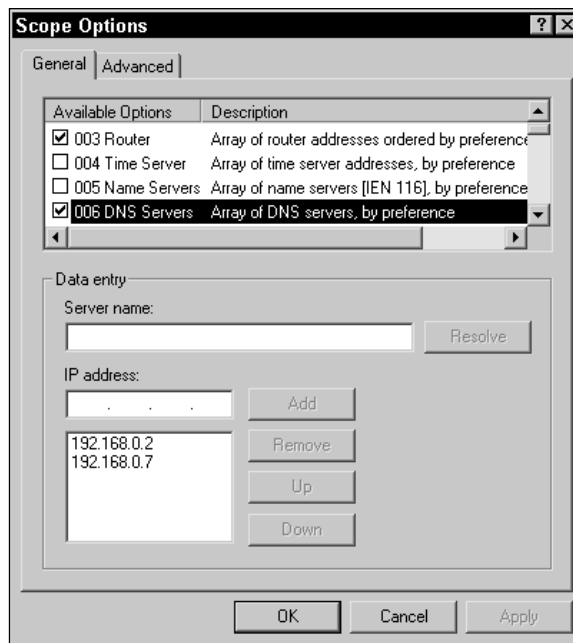


FIGURE 16-6 Configuring scope options

Enter the appropriate information (such as server name or IP address) for the option you selected.

Repeat this step until you have configured all of the server options or scope options you need to configure. When you finish configuring options, click **OK**.

4. The **DHCP** dialog box appears, with your scope or server options displayed in the right pane, as shown in Figure 16-7. Close **DHCP**.

## STEP BY STEP

Continued

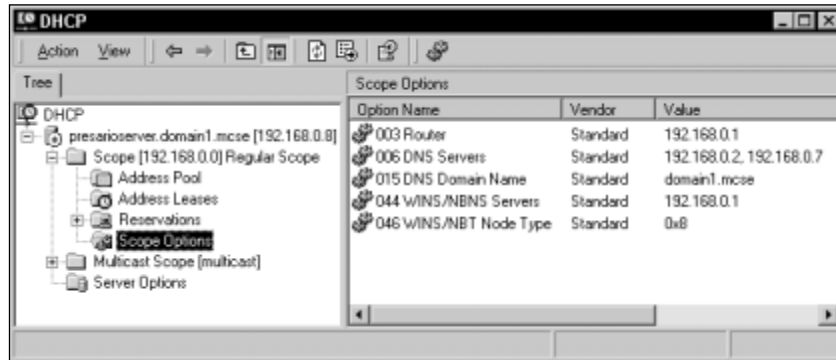


FIGURE 16-7 Scope Options configured

Notice the scope options I've configured in figure 16-7: a router, a DNS server, a DNS domain name, a WINS server, and a WINS/NBT node type. These are the most commonly used DHCP options on a Windows 2000 network, and the options on which you're most likely to be tested on the Windows 2000 exams.

I'll get into WINS a little later in this chapter, but for now you should know that if you want your DHCP server to provide client computers with the information they need to use a WINS server, you need to configure the following two options:

- **044 WINS/NBNS Servers:** This option is used to specify the IP address of one or more WINS servers for client computers. This option provides DHCP clients with the IP addressing information they need to be able to use a WINS server. This option is commonly configured on a DHCP server so that the administrator doesn't have to manually configure each client computer to use a WINS server.

- **046 WINS/NBT Node Type:** This option is used to specify the method client computers use to resolve computer names to IP addresses. The possible methods are: by broadcasting on the local network, by contacting a WINS server, or both. The preferred method for a Windows 2000 client computer is to first contact a WINS server, and then, if that fails, to broadcast on the local network. Client computers that use this method are referred to as H-nodes, and the value entry for this method is 0x8.

## Configuring DHCP Address Reservations

A DHCP address reservation is an IP address that can only be assigned to a specific network adapter card — the IP address is said to be *reserved* for that network adapter card. An IP address reservation is commonly used when a DHCP client computer, such as a Web server or mail server, must have the same IP address for a long period of time, so that other computers can access that server by its known IP address.

DHCP address reservations are configured for the specific scope that contains the IP address being reserved.

### STEP BY STEP

#### CONFIGURING A DHCP ADDRESS RESERVATION

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, expand the DHCP server that contains the scope for which you want to configure a reservation. Then expand the scope. Highlight Reservations and select Action ⇨ New Reservation.
3. The New Reservation dialog box appears, as shown in Figure 16-8.

Type in a name for the reservation in the “Reservation name” text box. The host name of the computer for which the reservation is being made is often used.

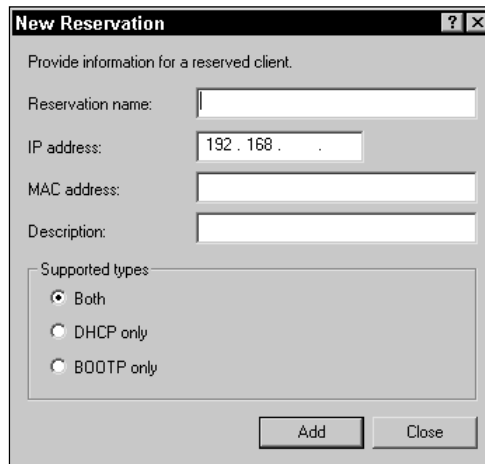
Then, in the “IP address” text box, configure the IP address that you want to be reserved.

Next, enter the MAC address of the network adapter card in the computer for which the reservation is being made in the text box provided. Enter the MAC address as a 12-digit hexadecimal number, without any dashes. If you don't know the MAC address of the network adapter card, type **ipconfig /all** at the command prompt on the computer that contains the network adapter card. The physical address information displayed, less the dashes in the number, is the MAC address of the network adapter card.

Enter a description for the reservation if you want to.

## STEP BY STEP

Continued

**FIGURE 16-8** Configuring an IP address reservation

Finally, select one of the three options in the “Supported types” section:

- ▶ **DHCP only:** Select this option if you only want to permit the DHCP client (for which an IP address is reserved) to request that address by using the DHCP protocol.
- ▶ **BOOTP only:** Select this option if you only want to permit the DHCP client (for which an IP address is reserved) to request that address by using the BOOTP protocol. The BOOTP protocol is an older protocol that is considered the predecessor to DHCP.
- ▶ **Both:** Select this option if you want to permit the DHCP client (for which an IP address is reserved) to request that address by using either the DHCP or BOOTP protocol. This is the default selection.

Click Add.

4. Repeat Step 3 until all desired IP address reservations are configured. Click Close.
5. Close DHCP.

---

## Monitoring a DHCP Server

An administrator should periodically monitor the DHCP server to ensure that it has an adequate supply of unassigned IP addresses, and that the DHCP server has adequate system resources (such as memory, processor, and disk) to handle all of its client requests.

You can use the DHCP administrative tool to provide you with a great deal of information about how your DHCP server is functioning. In DHCP you can display statistics about each DHCP server, such as the number of scopes and IP addresses it has, and how many of those IP addresses are in use. To view these statistics, in the DHCP dialog box, right-click the DHCP server for which you want to view statistics, and select Display Statistics from the menu that appears. Figure 16-9 shows statistics for a DHCP server.

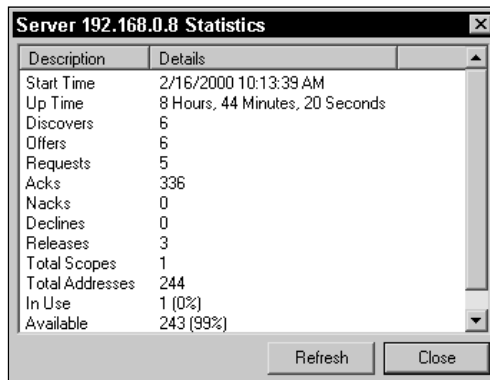


FIGURE 16-9 Viewing DHCP server statistics

You can also view information about address leases. When a DHCP client computer obtains an IP address from a DHCP server, the client computer is said to lease that IP address for a preset period of time, called a *lease duration*. In DHCP, you can view a list of all IP addresses assigned to DHCP clients, the host name of the client computer to which each IP address is assigned, and lease expiration information for each lease. Lease information is provided on a scope-by-scope basis. To view IP address lease information, in the DHCP dialog box, expand the scope for which you want to view lease information, and highlight the **Address Leases** folder. Lease information is displayed in the right pane, as shown in Figure 16-10.

You can also use System Monitor, a Performance tool, to monitor the DHCP Server object and its many counters. The DHCP Server object and its counters are available in System Monitor after DHCP is installed on a Windows 2000 Server computer. You can also use System Monitor to determine if your DHCP server has adequate memory, processor, and disk resources.

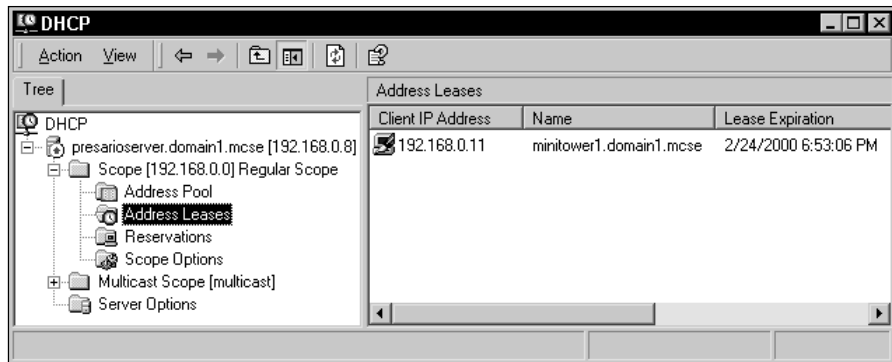


FIGURE 16-10 Viewing address leases for a scope



#### CROSS-REFERENCE

I cover how to use System Monitor in Chapter 21.

## Troubleshooting DHCP

Typically, DHCP servers don't require much troubleshooting. Once your DHCP server is up and running, it normally just works.

Two of the most common DHCP problems reported by users include the inability to lease an address from the DHCP server, and the inability to renew a leased address. If you face either of these two problems, try one or more of the following tips to resolve the problem:

- Use the Services tool in Computer Management to verify that the DHCP Server service is started. If it's not, start this service.
- If the DHCP server was recently installed and configured, ensure that the DHCP server has been authorized in Active Directory.
- Use the DHCP administrative tool to verify that a scope exists on the DHCP server, that the scope contains an adequate number of IP addresses, and that the IP addresses are appropriate for the network segment.
- Use the DHCP administrative tool to verify that the scope is active. A scope can't be used to assign IP addresses until it is activated.
- Verify that the DHCP client computer has been configured to use a DHCP server, and that its physical connection to the network (including network adapter card, cable, hub, and so on) is functioning.



- If the DHCP client computer is located on a different subnet than the DHCP server, verify that the router is configured to forward DHCP requests to the DHCP server.

## NetBIOS Name Resolution

A NetBIOS name is the computer name, up to 15 characters in length, assigned during the installation of all Windows-based operating systems. NetBIOS names are used to connect to resources located on other computers when a user browses the network, maps to a network drive, or uses the `net use` command from the command prompt.

When a user attempts to connect to a computer selected from a browse list by the remote computer's NetBIOS name, the user's computer must first obtain the IP address associated with the remote computer's NetBIOS name. This process is called *NetBIOS name resolution*. Once the user's computer has resolved the remote computer's NetBIOS name to its IP address, it can then establish TCP/IP network communications with the remote computer.

NetBIOS name resolution is not the same as host name resolution. A computer's host name is often the same as its NetBIOS name, but this is not always the case. In addition, a host name can be up to 63 characters in length. NetBIOS name resolution is initiated by programs and applications that use the NetBIOS protocol. Host name resolution is initiated by programs and applications that use Windows Sockets (also called Winsock).

A pure Windows 2000 network doesn't need to use NetBIOS name resolution, because it can perform all name resolution functions by using DNS servers. However, because very few of us have pure Windows 2000 networks, and because all previous versions of Windows require NetBIOS name resolution, you'll probably still have to configure NetBIOS name resolution on your network.

NetBIOS name resolution can be performed in several ways. The two most common methods are manually configuring an `lmhosts` file on each individual computer on the network, and installing a WINS server and configuring the client computers on the network to use it.

## Using Lmhosts Files to Resolve NetBIOS Names

An `lmhosts` file is a text file that contains a list that maps the IP addresses of all servers on the network to their associated NetBIOS names.

Using an `lmhosts` file for NetBIOS name resolution is a manual method that requires a great deal of administrator time. When an `lmhosts` file is used to perform NetBIOS name resolution, every time a server is added to or removed from the network, the `lmhosts` file on each individual computer on the network must be manually updated. Because of the amount of time required to keep `lmhosts` files up-to-date, their use has declined since WINS servers have become available.

By default, all Windows 2000 computers have an `lmhosts` file that contains instructions for constructing an `lmhosts` file that would be appropriate for your network. The default `lmhosts` file does not contain any mapping entries. You can use Notepad (or your favorite text editor) to create and edit an `lmhosts` file. When you create an `lmhosts` file, be sure to save it without a file extension — programs such as Notepad often automatically add a file extension to a filename when it is saved.

On Windows 2000 (and Windows NT) computers, the `lmhosts` file is stored in `SystemRoot\system32\drivers\etc`. On Windows 95 and Windows 98 computers, the `lmhosts` file is stored in the `C:\windows` folder.

Listing 16-1 shows a sample `lmhosts` file.

### LISTING 16-1 Sample `lmhosts` file

```
192.168.0.1 wolf #DOM:domain2
192.168.0.2 server01 #DOM:domain1
192.168.0.3 lotsadisks
192.168.0.4 nat #DOM:domain1
192.168.0.5 minitower1
192.168.0.6 alan
192.168.0.7 presarioserver
```



Notice the `#DOM:` portion of the entries for `wolf`, `server01`, and `nat`. The `#DOM:` portion is used to specify that the computer is a domain controller for the domain whose name immediately follows `#DOM`. In this example, `wolf` is a domain controller for `domain2`, and `server01` and `nat` are domain controllers for `domain1`.

## Using a WINS Server to Resolve NetBIOS Names

Windows Internet Name Service (*WINS*) is a Windows 2000 Server service that provides NetBIOS name resolution services to client computers. A Windows 2000 Server computer that has WINS installed on it is called a WINS server.

Installing a WINS server and configuring client computers to use it is the preferred method of handling NetBIOS name resolution on Windows 2000 networks. When this method is used, the WINS server dynamically updates its NetBIOS name to IP address tables whenever computers are added to or removed from the network. Using a WINS server requires a lot less administrator time than using `lmhosts` files.

WINS can only be installed on Windows 2000 Server computers. On small networks, WINS is often installed on the domain controller. On larger networks, WINS is often installed on multiple Windows 2000 Server computers.

In the next sections I'll discuss how to install and configure WINS, how to configure WINS proxies, how to plan and configure WINS replication, and how to monitor and troubleshoot WINS.

### Installing WINS

Before you can install WINS on a Windows 2000 Server computer, TCP/IP must be installed, and the computer's local area connection must be configured with a static IP address.

## STEP BY STEP

### INSTALLING A WINS SERVER

1. Select Start ⇨ Settings ⇨ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.

**STEP BY STEP***Continued*

4. In the Windows Components Wizard dialog box, highlight Networking Services, and click Details.
5. In the Networking Services dialog box, select the check box next to Windows Internet Name Service (WINS), and click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. When prompted, insert your Windows 2000 Server compact disc into your computer's CD-ROM drive and click OK. Close the Microsoft Windows 2000 CD dialog box. Windows 2000 configures components and installs WINS. In the Completing the Windows Components Wizard screen, click Finish.
8. Close Add/Remove Programs. Then close Control Panel.

---

Before your newly installed WINS server will do you any good, you'll need to configure each client computer on the network to use the WINS server for NetBIOS name resolution. You can either accomplish this task by manually configuring each client computer to use the WINS server, or by configuring a DHCP server to supply each client computer with the IP addressing information it needs to use the WINS server. I'll discuss how to configure NetBIOS name resolution options on client computers a little later in this chapter.

### Configuring WINS Proxies

A *WINS proxy* is a computer on a subnet that forwards NetBIOS name resolution broadcasts that come from client computers that don't support WINS, to a WINS server on another subnet, and broadcasts the name resolution response back to the client computer. Since all Microsoft Windows clients support WINS, WINS proxies are rarely used. However, there are still client operating systems that use NetBIOS, and do not support WINS. A WINS proxy should be configured on each subnet that contains client computers that don't support WINS.

Windows 2000 Professional and Server computers can be configured to function as WINS Proxies. You have to manually edit the Registry to configure a Windows 2000 computer as a WINS Proxy.

 STEP BY STEP**CONFIGURING A WINDOWS 2000 COMPUTER TO FUNCTION AS A WINS PROXY.**

1. Select Start → Run.
2. In the Run dialog box, type **Regedt32** in the Open drop-down list box. Click OK.
3. In the Registry Editor dialog box, select Windows → HKEY\_LOCAL\_MACHINE on Local Machine.
4. Maximize the HKEY\_LOCAL\_MACHINE on Local Machine window.
5. Double-click the **System** Folder. Under the **SYSTEM** folder, double-click the **CurrentControlSet** folder. Double-click the **Services** folder. Double-click the **NetBT** folder. Click the Parameters folder. Select Edit → Add Value.
6. The Add Value dialog box appears. Type **EnableProxy** in the Value Name text box. Select REG\_SZ from the Data Type drop-down list box. Click OK.
7. The String Editor dialog box appears. Type **1** in the String text box and click OK.
8. Close Registry Editor. The computer will function as a WINS proxy after it is rebooted.

---

## Planning and Configuring WINS Replication

WINS replication is the process of keeping the NetBIOS name to IP address databases on multiple WINS servers synchronized. If you have a small network with a single WINS server, you'll never have to worry about WINS replication — except, of course, when you take the Network exam.

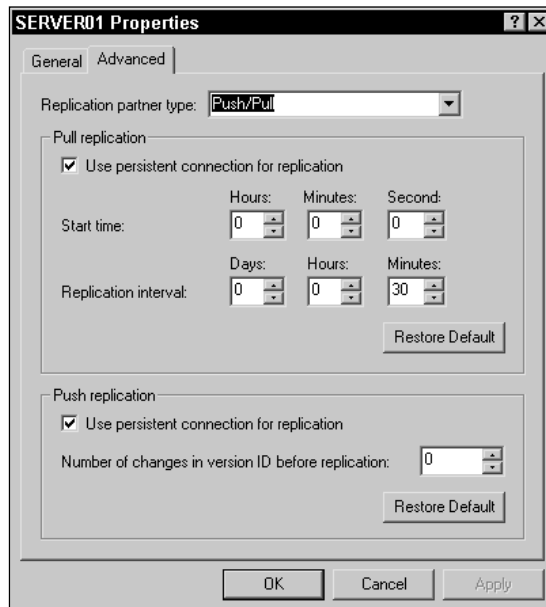
Where WINS replication, and the managing of this replication, becomes important is in a large network that has multiple WINS servers in multiple locations that are connected by slow WAN links. If you have a network like this, you'll want to have a WINS server on each side of the slow WAN link so that client computers are able to obtain NetBIOS name resolution services from the local network, instead of tying up precious bandwidth by using the WAN link. You'll also probably want to configure replication on each of these WINS servers so that replication traffic over the WAN link only occurs during nonbusiness hours, when network traffic on the WAN link is at a minimum.

In order to configure WINS replication, you must have at least two WINS servers. You can configure WINS replication by using the WINS administrative tool, as the following steps explain.

## STEP BY STEP

## CONFIGURING WINS SERVER REPLICATION

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ WINS.
2. In the left pane of the WINS dialog box, click the + next to the WINS server for which you want to configure replication. Then highlight Replication Partners. Select Action ⇨ New Replication Partner.
3. In the New Replication Partner dialog box, type the name or IP address of the other WINS server with which you want this WINS server to replicate. You can browse for this server if necessary. Click OK.
4. The WINS server that this server will replicate with (the replication partner) appears in the right pane. At this point, replication is configured to take place automatically whenever a change to the IP address to NetBIOS name database takes place.
5. To configure replication to occur at a specified time, in the right pane, highlight the replication partner, and select Action ⇨ Properties.
6. The replication partner's Properties dialog box appears. Click the Advanced tab.
7. The Advanced tab appears, as shown in Figure 16-11.



**FIGURE 16-11** Configuring properties of the WINS replication partner

## STEP BY STEP

Continued

This is an important dialog box that contains all of the settings that need to be configured for WINS replication:

In the “Replication partner type” drop-down list box, select one of the three available options:

- ▶ **Push/Pull:** Selecting this option configures the replication partner to notify this WINS server when its database changes (this is called a *push*), and to request database changes from this WINS server (this is called a *pull*). This is the default option and should be used between two WINS servers that are connected by a local area network or other high-speed link.
- ▶ **Push:** Selecting this option configures the replication partner to notify this WINS server when its database changes (but *not* to request database changes from this WINS server). This setting is often used when the WINS server you’re configuring (not the replication partner) is located on the other side of a remote WAN link where no other servers (other than the WINS server itself) exist. Because NetBIOS name resolution is primarily concerned with resolving server IP addresses, and there are no other servers on the remote network with the isolated WINS server, there’s no need to update the replication partner with this WINS server’s database changes.
- ▶ **Pull:** Selecting this option configures the replication partner to request database changes from this WINS server (but *not* to notify this WINS server when its database changes). This setting is often used when the two WINS servers are separated by a slow WAN link, and when the replication partner needs to be updated with this WINS server’s database changes.

8. If you selected a replication partner type of Push/Pull or Pull, complete the “Pull replication section” of this dialog box.

If you want this WINS server to maintain a constant connection with its replication partner, accept the default selection of the check box next to “Use persistent connection for replication.” This option should only be selected when the two WINS servers are connected by a high-speed link or are on a local area network. This option speeds up the replication process between the WINS servers, because they don’t have to take time to establish a connection each time replication occurs.

By default, WINS replication occurs every 30 minutes. If you want to schedule when replication occurs, in the “Start time” section, configure the time of day you want WINS replication to start. Then, configure the frequency of WINS replication by configuring the “Replication interval” section.

9. If you selected a replication partner type of Push/Pull or Push, complete the “Push replication” section of this dialog box.

If you want this WINS server to maintain a constant connection with its replication partner, accept the default selection of the check box next to “Use persistent connection for replication.” This option should only be selected when the two WINS servers are connected by a high-speed link or are on a local area network.

## STEP BY STEP

*Continued*

Then, in the “Number of changes in version ID before replication” spin box, specify the number of database changes that must occur before the replication partner will notify this WINS server of its database changes.


10. When you finish configuring the properties of the replication partner, click OK.

In order for bidirectional replication between the two WINS servers to occur, you need to repeat this process on the replication partner. When you repeat these steps on the replication partner, keep in mind that the configurations you make must complement the settings you configured on the first WINS server.

### Monitoring a WINS Server

An administrator should periodically monitor the WINS server to ensure that replication (if configured) is occurring at appropriate intervals, and that the WINS server has adequate system resources (such as memory, processor, and disk) to handle all of its client requests.

You can use the WINS administrative tool to provide you with information about how your WINS server is performing. In WINS you can display statistics about each WINS server, such as the date and time of the last replication, the total number of queries for NetBIOS name resolution the WINS server has received from client computers, and so on. To view these statistics, in the WINS dialog box, right-click the WINS server for which you want to view statistics, and select Display Server Statistics from the menu that appears. Figure 16-12 shows statistics for a WINS server.



Description	Details
Server start time	2/17/2000 10:48:59 AM
Database initialized	...
Statistics last cleared	...
Last periodic replication	2/17/2000 12:16:00 PM
Last manual replication	2/17/2000 1:41:19 PM
Last net update replication	...
Last address change replication	...
Total queries	16
Records found	0
Records not found	16
Total releases	0

FIGURE 16-12 Viewing WINS server statistics



You can also view the WINS server database that contains the NetBIOS name to IP address mappings for servers and client computers that are configured to use this WINS server.

## STEP BY STEP

### VIEWING THE WINS SERVER DATABASE

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ WINS.
2. In the left pane of the WINS dialog box, click the + next to the WINS server that contains the database you want to view. Then highlight the **Active Registrations** folder. Then right-click this folder and select Find by Owner from the menu that appears.
3. In the Find by Owner dialog box, select one of the two options:
  - ▶ **All owners:** Select this option if you want to view WINS records for all computers that are configured to use this WINS server or one of its replication partners.
  - ▶ **This owner:** Select this option if you want to view WINS records for only those computers that are configured to use this WINS server. If you select this option, you also need to select the WINS server for which you want to view records from the list.

Configure the appropriate option, then click Find Now.

4. The database is displayed in the right pane of the WINS dialog box, as shown in Figure 16-13.

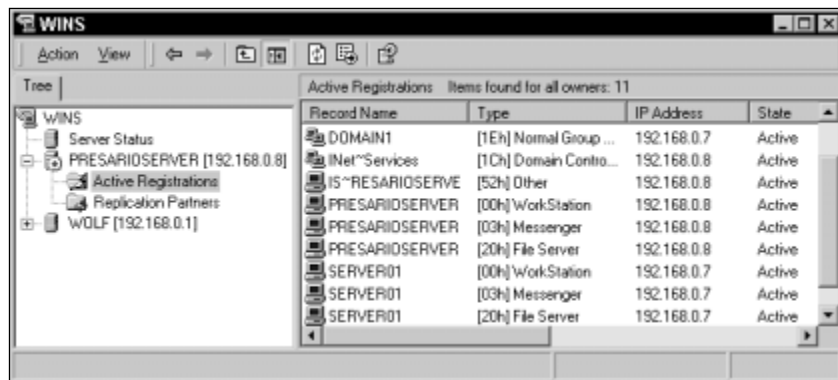


FIGURE 16-13 Viewing the WINS server database

When you finish viewing the database, close WINS.

You can also use System Monitor, a Performance tool, to monitor the WINS Server object and its many counters. The WINS Server object and its counters are available in System Monitor after WINS is installed on a Windows 2000 Server computer. You can also use System Monitor to determine if your WINS server has adequate memory, processor, and disk resources.



#### CROSS-REFERENCE

I cover how to use System Monitor in Chapter 21.

### Troubleshooting WINS

Like DHCP servers, WINS servers don't normally require much troubleshooting. Once your WINS server is installed and correctly configured, it normally just works.

That said, the most common WINS problem is the inability to resolve a NetBIOS name to its associated IP address. This problem typically shows up when a user tries to map a network drive to a server by using the server's name, and receives an error message stating "The network path \\server\_name\share\_name could not be found."

If you experience this problem, here are some tips that might help you:

- Use the Services tool in Computer Management to verify that the Windows Internet Name Service (WINS) is started. If it's not, start this service.
- Verify that the client computer (or computers) experiencing the problem are configured to use the WINS server.
- Verify that the server (or other resource) that the client is attempting to connect to is configured to use the WINS server.
- Use `ping.exe` to verify that the client computer experiencing the problem can communicate with the WINS server by using TCP/IP.
- If you have multiple WINS servers on the network, verify that WINS server replication is correctly configured on each WINS server, and that replication is occurring.

## Configuring NetBIOS Name Resolution Options on Client Computers

If you plan to use `lmhosts` files to provide NetBIOS name resolution services for your client computers, you don't have to configure NetBIOS name resolution options on these client computers, because Windows 2000 computers are automatically configured to use `lmhosts` files by default. You do, however, have to manually edit the `lmhosts` file on each computer.

If you plan to use one or more WINS servers to provide NetBIOS name resolution services for your client computers, you *do* need to configure the client computers on your network to use the WINS server(s) before NetBIOS name resolution will take place.



### TIP

When I say “client computer,” I’m referring to clients of the WINS server, which include *all* computers on the network, *including the WINS server itself*. You need to configure *all* of the computers on your network for NetBIOS name resolution.

You can configure client computers to use a WINS server in one of two ways. You can either manually configure each client computer to use the WINS server, or you can configure your DHCP server to supply each client computer with the IP addressing information it needs to use the WINS server. (In the section earlier in this chapter on “Configuring DHCP Options,” I discussed the two important options that should be configured if you want your DHCP server to supply client computers with the information they need to use a WINS server.)

In the following steps, I’ll show you how to configure a Windows 2000 client computer to use a WINS server for NetBIOS name resolution.

## STEP BY STEP

### MANUALLY CONFIGURING NETBIOS NAME RESOLUTION OPTIONS

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the **Network and Dial-up Connections** folder, right-click the computer’s Local Area Connection, and select Properties from the menu that appears.
3. In the Local Area Connection Properties dialog box, highlight the Internet Protocol (TCP/IP) and click Properties.

## STEP BY STEP

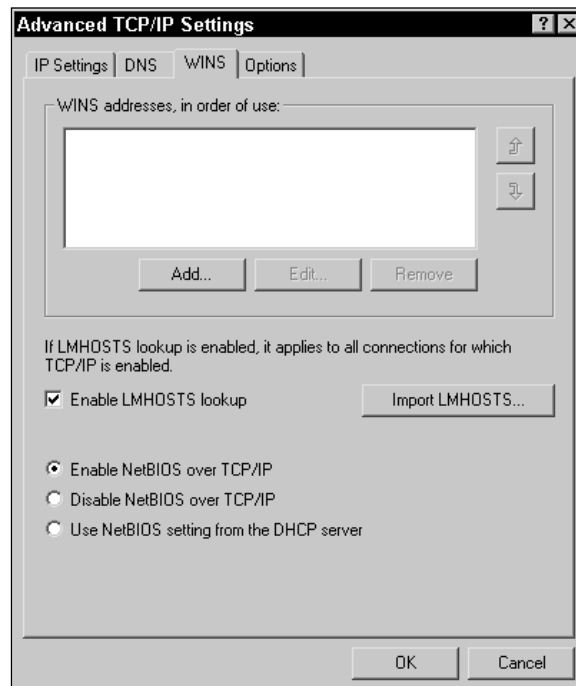
Continued



## TIP

If the computer has more than one Local Area Connection, you'll need to perform these steps on each of the connections.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click Advanced.
5. In the Advanced TCP/IP Settings dialog box, click the WINS tab.
6. The WINS tab appears, as shown in Figure 16-14.



**FIGURE 16-14** Configuring NetBIOS name resolution options on the WINS tab

**To configure the computer to use a WINS server**, click Add. In the TCP/IP WINS Server dialog box, enter the IP address of the WINS server, and click Add. If you want this computer to use more than one WINS server, repeat this process until IP addresses for all WINS servers have been added.

**If you want this computer to use both a WINS server and an `lmhosts` file**, accept the default selection in the check box next to “Enable LMHOSTS lookup.”

**If you want this computer to only use the WINS server, and to not use an `lmhosts` file**, clear the check box next to “Enable LMHOSTS lookup.”

## STEP BY STEP

Continued

7. In the bottom of this dialog box, select one of the following three options:
  - ▶ **Enable NetBIOS over TCP/IP:** If you have any non-Windows 2000 Windows-based computers on your network (such as Windows NT, Windows 95 or 98) select this option. This option is selected by default.
  - ▶ **Disable NetBIOS over TCP/IP:** If all of the computers on your network are Windows 2000 computers, *and* you don't use any programs or applications that require NetBIOS, select this option.
  - ▶ **Use NetBIOS setting from the DHCP server:** If you want to use your DHCP server to control whether NetBIOS is enabled on this computer (instead of enabling or disabling NetBIOS on the local computer), select this option.
- Click OK.
8. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
9. In the Local Area Connection Properties dialog box, click OK.
10. Close the **Network and Dial-up Connections** folder.

## Routing TCP/IP

IP routing is a function of the Internet Protocol (IP) that uses IP address information to send data packets from a source computer on one network segment across one or more routers to a destination computer on another network segment. Hardware devices that perform routing are called *routers*. Windows 2000 Server computers can function as routers, but Windows 2000 Professional computers can't.



### EXAM TIP

The Network exam has more objectives on routing than you can shake a stick at. This is an extremely complex subject. Make sure you know the features each of the Windows 2000 Server routing protocols has to offer, and when and how each protocol should be used.

Windows 2000 Server computers that have multiple network adapter cards can function as IP routers. These computers are sometimes called *multihomed* computers, because they have more than one network adapter card. In addition, even if a Windows 2000 Server computer only has one

network adapter card, it may still be able to function as an IP router if it has a modem or other communications device (such as an ISDN adapter, an X.25 adapter, and so on) installed.

Routing, like TCP/IP, is an immense topic. In the next several sections I'll explore several important routing topics, including: static routing; configuring a router; managing ports, interfaces, and demand-dial routing; and dynamic routing. Finally, I'll discuss monitoring and troubleshooting TCP/IP routing.

## Static Routing

*Static routing* is basic, no-frills IP routing. No additional software is necessary to implement static routing in Windows 2000 Server computers. In order to function as a router, the Windows 2000 Server computer must have at least one network adapter card installed. In addition, it must have either an additional network adapter card or a communications device, such as a modem, installed.

### Enabling Routing

When you enable routing on a Windows 2000 Server computer (without installing additional routing software or protocols), you are configuring your Windows 2000 Server computer to function as a static router.

You can use the Routing and Remote Access administrative tool to enable routing on a Windows 2000 Server computer, as the following steps explain.

#### STEP BY STEP

##### ENABLING ROUTING ON A WINDOWS 2000 SERVER COMPUTER

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 routing, 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. In the Common Configurations screen, select the "Network router" option, as shown in Figure 16-15. Click Next.



##### CROSS-REFERENCE

See Chapter 17 for information on how to configure a remote access server and a VPN server.

## STEP BY STEP

Continued

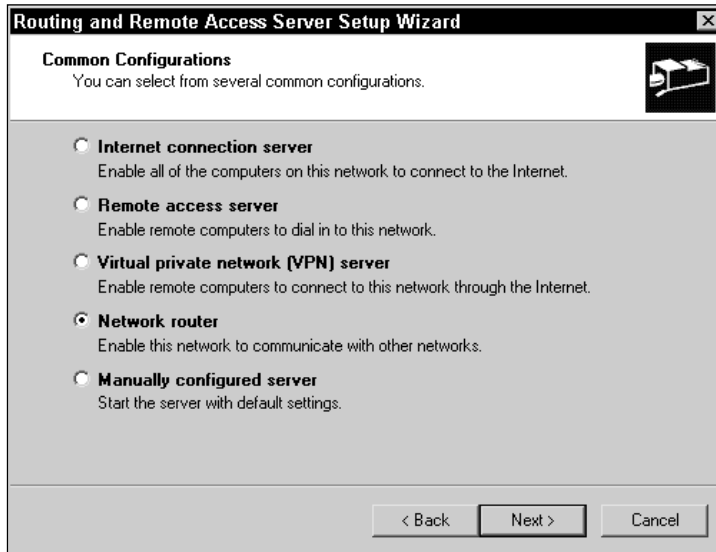


FIGURE 16-15 Configuring a Windows 2000 Server computer to be a router

5. In the Routed Protocols screen, verify that all network protocols required on the server are listed. Commonly listed protocols include IPX, TCP/IP, 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 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. In the Demand-Dial Connections screen, choose whether to use demand-dial connections on this server. A demand-dial connection is a type of dial-up (or VPN) connection that is used by a router only when it needs to transmit data to a remote network. Your two choices are Yes or No, and the default selection is No. You can change this option later if you change your mind. Make your selection, then click Next.
7. If you selected Yes in Step 6, the IP Address Assignment screen appears. Select the method you want to use for assigning IP addresses to remote routers when they connect to this computer using a demand-dial connection. Your choices are “Automatically” (this is the default setting), or “From a specified range of addresses.” Click Next.
8. In the Completing the Routing and Remote Access Server Setup Wizard screen, click Finish.

## STEP BY STEP

Continued

9. Windows 2000 starts the Routing and Remote Access service. Your Windows 2000 Server computer is now configured as a static router. Close Routing and Remote Access.

## Updating a Routing Table by Adding Static Routes

Static routers are not capable of automatically building a routing table. A *routing table* contains a list of network IDs, each of which is associated with the IP address of the router on the network that can forward data packets over the shortest path to the specified destination network. These entries are called *static routes*. In a static routing environment, administrators must manually configure the routing table on each individual router. If the network layout changes, the administrator must manually update the routing tables by adding or removing static routes to reflect these changes.

There are two ways to manually configure the routing table on a Windows 2000 Server computer that is configured as a static router. You can perform this task by using Routing and Remote Access, or you can use the `route.exe` command-line utility.

## STEP BY STEP

### USING ROUTING AND REMOTE ACCESS TO ADD A STATIC ROUTE TO A ROUTING TABLE

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 routing table you want to configure. Then click the + next to IP Routing. Then right-click Static Routes, and select New Static Route from the menu that appears.
3. The Static Routes dialog box appears, as shown in Figure 16-16.

In the Interface drop-down list box, select the connection to which this route applies. Your choices will depend on the number and type of connections configured on your Windows 2000 Server computer.

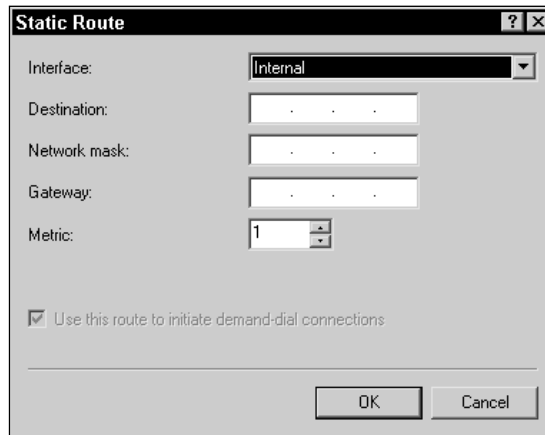
In the Destination text box, enter the IP address of the remote network segment for which you are configuring the static route.

In the Network mask text box, enter the subnet mask that is used on the remote network segment.



## STEP BY STEP

Continued

**FIGURE 16-16** Adding a static route

In the Gateway text box, enter the IP address of the router that can forward packets to this remote network segment.

In the Metric spin box, select the number of routers that packets must pass through in order to reach the remote network segment by using this static route.

Click OK.

4. The static route is created, and is displayed in the right pane. Close Routing and Remote Access.

---

For information on using the `route.exe` command-line utility to manually update a routing table, type **route /help** at the command prompt, and press Enter. I recommend that you use Routing and Remote Access to add static routes because the command line syntax for the `route.exe` command is very complex.

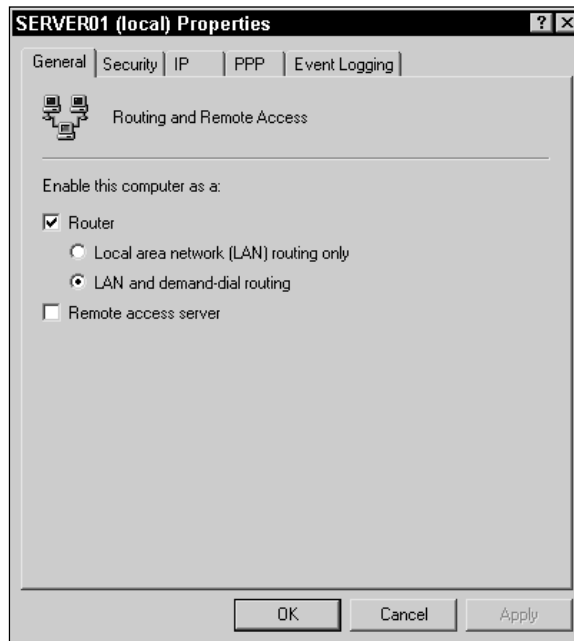
## Configuring a Router

Once you've configured your Windows 2000 Server computer to function as a router, you may need to configure the router's properties to meet your network's needs. You can use Routing and Remote access to configure several router properties, including security, protocol, and event logging options.

## STEP BY STEP

## CONFIGURING A ROUTER'S PROPERTIES

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 for which you want to configure routing properties, then select Properties from the menu that appears.
3. The server's Properties dialog box appears, with the General tab on top, as shown in Figure 16-17. If you have additional protocols installed (such as NWLink IPX/SPX/NetBIOS Compatible Transport Protocol or the AppleTalk Protocol), each protocol will have its own additional tab in this dialog box.



**FIGURE 16-17** Configuring the general properties of a router

On this tab, you can enable or disable routing. You can also configure whether this server will function as a remote access server (I cover remote access servers in great detail in Chapter 17).

Assuming you want this server to function as a router (and you have selected the check box next to Router), you should choose either to limit routing to the local area network only, or to enable both local area network and demand-dial routing to a remote network.

Make the appropriate configurations. To configure security options, click the Security tab.

## STEP BY STEP

Continued



## TIP

If you want this router to support demand-dial routing, but you didn't configure it to support demand-dial connections when you used the wizard to enable routing, you must select the "LAN and demand-dial routing" option on this tab.

4. On the Security tab, you can select an authentication provider that will be used for demand-dial and remote access connections. Your choices are Windows Authentication or RADIUS Authentication. The default selection is Windows Authentication, and is acceptable unless you're using a RADIUS server to authenticate remote access clients for multiple servers.

If you need to modify the authentication methods this server will use when it authenticates remote clients or routers, click Authentication Methods and make the necessary configurations. This option is normally only used by administrators with advanced knowledge of authentication protocols.

You can also select the accounting provider this server will use. The accounting provider logs all sessions with the router. You can select either Windows Accounting (this is the default), RADIUS Accounting, or None.

Make the appropriate configurations. To configure IP options, click the IP tab.

5. The IP tab appears, as shown in Figure 16-18.

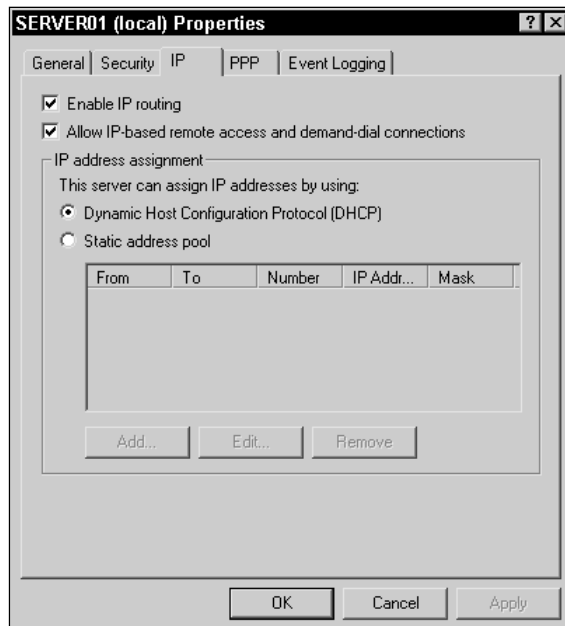


FIGURE 16-18 Configuring a router's IP options

**STEP BY STEP***Continued*

Notice that the “Enable IP routing” check box is selected. This is the default configuration. This check box must be selected in order for this computer to function as an IP router.

If you want this router to support IP on all of its connections, ensure that the “Allow IP-based remote access and demand-dial connections” check box is selected. If this check box is cleared (and the “Enable IP Routing” check box is selected), IP will only be used on local area connections.

**TIP**

If you want this router to support IP on demand-dial connections, make sure to select this check box.

Next, you can configure how this computer will assign IP addresses to computers and routers connecting to it. By default, the server is configured to use a DHCP server for IP address assignment. However, you can configure it to use a static IP address pool if you want to.

Make the appropriate configurations. To configure PPP options, click the PPP tab.

6. On the PPP tab, you can configure several Point-to-Point Protocol (PPP) options. In general, you only need to concern yourself with this tab if your computer is configured as a remote access server, or if your router supports demand-dial connections. By default, all PPP options are selected. The options are:
  - ▶ **Multilink connections**
  - ▶ **Dynamic bandwidth control using BAP or BACP**
  - ▶ **Link control protocol (LCP) extensions**
  - ▶ **Software compression**

Make any necessary changes. To configure Event Logging, click the Event Logging tab.

7. On the Event Logging tab, you can configure how Windows 2000 will handle event logging for routing and remote access events. You can select one of the following four levels of logging:
  - ▶ **Log errors only**
  - ▶ **Log errors and warnings** (this is the default setting)
  - ▶ **Log the maximum amount of information**
  - ▶ **Disable event logging**

In addition to selecting a logging level, you can enable or disable PPP logging in this dialog box. (It is disabled by default.)

When you finish configuring event logging options, click OK.

8. Close Routing and Remote Access.

## Managing Ports, Interfaces, and Demand-Dial Routing

Before I move on to the topic of dynamic routing, I need to explain a little about ports and routing interfaces. Routing ports may include all of the ports on your Windows 2000 Server computer, including VPN ports, modems, infrared ports, and parallel ports. A *routing interface* is a portal through which packets are routed. A routing interface can either be a hardware connection, such as a network adapter card or modem; or it can be a software connection, such as a VPN connection.

By default, when routing is enabled, all of the Windows 2000 Server computer's modems, infrared ports, and parallel ports are automatically enabled as routing ports. In addition to these ports, when either routing or remote access is enabled on a Windows 2000 Server computer, Windows 2000 creates and enables five PPTP ports and five L2TP ports.

By default, when you configure a Windows 2000 Server computer to function as a router, Windows 2000 automatically configures and enables all of the local area connections on the computer as routing interfaces. In addition, Windows 2000 creates and enables a loopback routing interface and an internal routing interface. A *loopback interface* is a routing interface that uses the TCP/IP loopback address of 127.0.0.1. This interface is primarily used by TCP/IP and is normally not used for actual routing. An *internal interface* is a virtual routing interface that is required and used only by the IPX protocol.

There's one more special kind of routing interface you need to know about. It's called a *demand-dial interface*, and it's used for demand-dial routing. In demand-dial routing, a routing connection is established from this server to a remote router only when data needs to be transmitted to or from the remote router. The routing connection is established by using a demand-dial interface. (The demand-dial interface is called a demand-dial connection in the Routing and Remote Access Server Setup wizard.) Demand-dial interfaces don't exist by default — they must be created by using Routing and Remote Access. A demand-dial interface requires the use of a modem, a VPN port, or any other port on the Windows 2000 Server computer.

So, there are a lot of tasks you need to perform to enable demand-dial routing on your Windows 2000 Server computer:

1. First, you must first configure your Windows 2000 Server computer to enable “LAN and demand-dial routing” and to “Allow IP-based remote access and demand-dial connections.” You may have chosen to use demand-dial connections when you used the wizard to enable routing on your computer, or you can manually configure these options in the server’s Properties dialog box in Routing and Remote Access. (I explained how to do this in the “Configuring a Router” section earlier in this chapter.)
2. Next, because a port is required by a demand-dial interface, you should ensure that the port you want this interface to use is configured to support demand-dial routing connections.
3. Finally, before demand-dial routing will occur, you need to create and configure a demand-dial interface.



#### TIP

Windows 2000 won’t permit you to configure a port or to create a demand-dial interface until you have enabled demand-dial routing on the server.

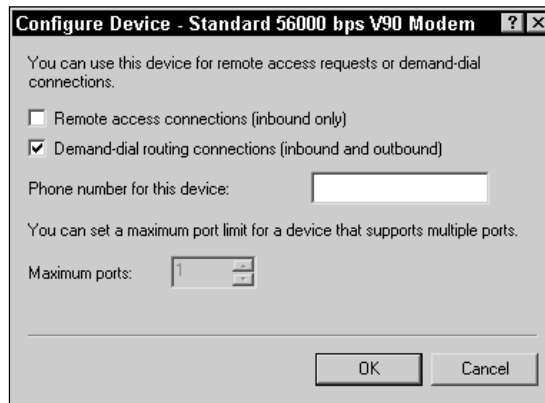
I’ll show you how to configure a port and how to create and configure a demand-dial interface in the steps that follow.

## STEP BY STEP

### CONFIGURING A 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 port you want to configure. Right-click Ports, and select Properties from the menu that appears.
3. In the Ports Properties dialog box, highlight the modem or port you want to configure, and click Configure.
4. The Configure Device dialog box for the port you selected appears, as shown in Figure 16-19.

## STEP BY STEP

*Continued***FIGURE 16-19** Configuring a port

Select the check box next to “Remote access connections (inbound only)” if this computer functions as a remote access server and you want to permit this port to be used for inbound connections from remote clients.

Select the check box next to “Demand-dial routing connections (inbound and outbound)” if this computer functions as a router and you want to permit this port to be used 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 or L2TP port, you can configure the maximum number of ports of this type that the Windows 2000 Server computer will support. The range can be between 0 and 30,000.

When you finish configuring the port, click OK.

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

## CREATING AND CONFIGURING A DEMAND-DIAL INTERFACE

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 on which you want to create a demand-dial interface. Right-click Routing Interfaces, and select New Demand-dial Interface from the menu that appears.
3. The Demand Dial Interface wizard starts. Click Next.
4. In the Interface Name screen, either accept the default name of Remote Router, or type in a new name for this interface. Click Next.

## STEP BY STEP

Continued

5. In the Connection Type screen, choose whether you want this interface to use a physical device (such as a modem, ISDN adapter, and so on) or a VPN port. Click Next.
6. **If you selected a physical device in Step 5**, the “Select a device” screen appears. Select the modem or other physical device you want this interface to use. Click Next.  
**If you selected a VPN port in Step 5**, the VPN Type screen appears. Select the type of VPN port you want to use. Your choices are: Automatic selection (this is the default), Point to Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP). Click Next.
7. **If you selected a physical device in Step 5**, the Phone Number screen appears. Enter the phone number of the dial-up server or router that this interface will connect to. Click Next.  
**If you selected a VPN port in Step 5**, the Destination Address screen appears. Enter the FQDN or IP address of the remote router that this interface will connect to. Click Next.
8. The Protocols and Security screen appears, as shown in Figure 16-20.

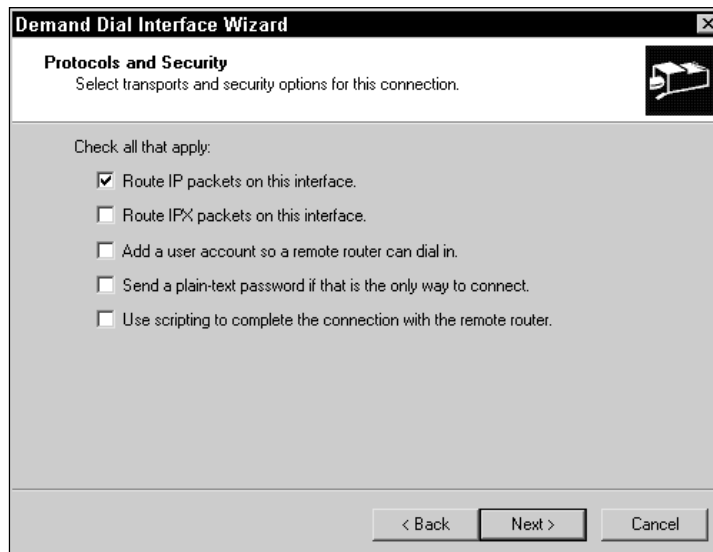


FIGURE 16-20 Selecting protocol and security options for the interface

Depending on whether you selected a physical device or a VPN port, some of these options may be grayed out and unavailable. Select the check box next to each of the protocol and security options you want to enable for this interface.



## STEP BY STEP

Continued



## TIP

If a remote router will use this interface to connect to this computer, select the check box next to “Add a user account so a remote router can dial in.” If you don’t select this check box, you’ll have to manually create a user account later for the remote router.

Click Next.

9. In the Dial Out Credentials screen, enter the user name, domain name, and password that this interface will use when it connects to a remote router. Click Next.
10. In the “Completing the demand-dial interface wizard” screen, click Finish.
11. If you need to change any of the settings you configured for this interface, you can do so by using Routing and Remote Access. In the left pane of the Routing and Remote Access dialog box, highlight Routing Interfaces. Then, in the right pane, right-click the demand-dial interface, and select Properties from the menu that appears. Make any necessary configuration changes, and click OK.
12. Close Routing and Remote Access.

---

## Dynamic Routing

*Dynamic routing* is intelligent IP routing. A dynamic router is capable of automatically building and updating a routing table. In a dynamic routing environment, administrators don’t have to configure the routing table on each router manually. As changes are made to the network, dynamic routers automatically adjust their routing tables to reflect these changes.

So, how does dynamic routing work? Periodically, each dynamic router on the network broadcasts packets containing the contents of its routing table. Dynamic routers that receive these packets add the routing table information received to their own routing tables. In this way, dynamic routers can recognize other routers as they are added to and removed from the network.

The process of updating routing tables on routers is not instantaneous. It may take from several seconds to several minutes before all routers on the network have accurate, up to date routing tables. The time it takes for a change to the network to be reflected in the routing tables of all routers on the network is called the convergence interval, or convergence time.

Dynamic routing requires the use of additional software in Windows 2000 Server computers. Until this software is installed, a Windows 2000 Server computer can only function as a static router.

In Windows 2000, this additional software comes in the form of three dynamic IP routing protocols:

- RIP Version 2 for Internet Protocol
- Open Shortest Path First (OSPF)
- IGMP Version 2, Router and Proxy

These routing protocols are included with Windows 2000 Server. By installing one of these protocols, a Windows 2000 Server computer can be transformed from a mere static router into a dynamic router. In addition, Windows 2000 includes two other routing protocols that, although not technically dynamic routing protocols, provide special functionality and may be used in conjunction with a dynamic routing protocol. These are the Network Address Translation Agent (NAT) and the DHCP Relay Agent.

I'll discuss how to install, configure, and manage all of these routing protocols in the sections that follow.

## Installing and Configuring RIP Version 2 for Internet Protocol

RIP Version 2 for Internet Protocol (RIP v2) is a dynamic IP routing protocol that is designed for small- to medium-sized networks. RIP v2 is a simple routing protocol that is relatively easy to install and maintain. However, this protocol uses a substantial amount of network bandwidth to maintain its routing tables. In addition, on large networks, it can take several minutes or more for the routing tables on all routers to converge when changes to the network occur.

RIP v2 can be installed on any Windows 2000 Server computer on which TCP/IP is installed and routing has been enabled.

### STEP BY STEP

#### INSTALLING RIP VERSION 2 FOR INTERNET PROTOCOL

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to install RIP Version 2 for Internet Protocol. Then click the + next to IP Routing. Right-click General, and select New Routing Protocol from the menu that appears.

## STEP BY STEP

*Continued*

3. In the New Routing Protocol dialog box, select RIP Version 2 for Internet Protocol from the list. Click OK.
4. The protocol is installed.

---

After RIP v2 is installed, you need to configure its properties. In addition, you need to configure this protocol to use one or more of the routing interfaces in your Windows 2000 Server computer. Until you configure RIP v2 to use at least one routing interface, RIP v2 won't be able to dynamically update your routing tables.

## STEP BY STEP

## CONFIGURING RIP VERSION 2 FOR INTERNET PROTOCOL

1. In the left pane of the Routing and Remote Access dialog box, right-click RIP, and select Properties from the menu that appears.
2. In the RIP Properties dialog box, you can configure the maximum number of seconds the router will wait before it sends triggered updates. (Triggered updates are high-priority updates that are generated when a router is added to or removed from the network. These updates are sent immediately instead of waiting until the next periodic update.) The default setting is 5 seconds.

You can also configure event logging in this dialog box. You can choose to: log errors only, log errors and warnings, log the maximum amount of information, or disable event logging. The default selection is "Log errors only."

To configure security options for the RIP v2, click the Security tab.

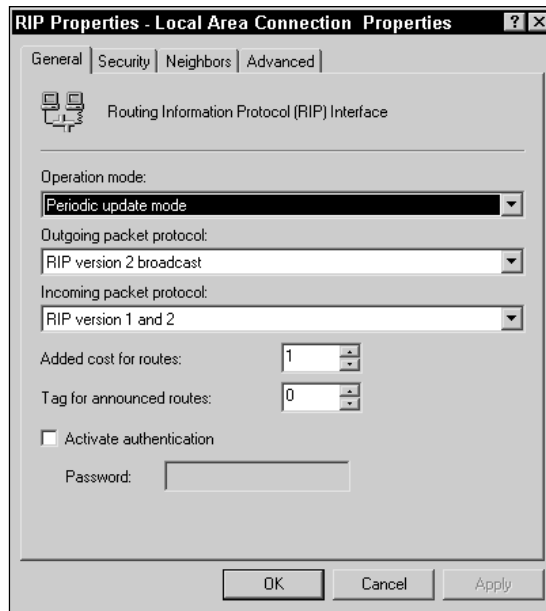
3. On the Security tab, select one of three options:
  - ▶ **Accept announcements from all routers:** Select this option if you don't want or need to use security. This is the default selection.
  - ▶ **Accept announcements from listed routers only:** Select this option if you want to prevent your routing tables from accepting updates from unknown routers. If you select this option, you must create a list of routers, by IP address, that this router will accept updates from.
  - ▶ **Ignore announcements from all listed routers:** Select this option if you want to prevent your routing table from accepting updates from specific, known routers on your network. If you select this option, you must create a list of routers, by IP address, that this router will not accept updates from.

When you finish configuring security options, click OK.

## STEP BY STEP

*Continued*

4. To configure RIP v2 to use a routing interface in the computer, right-click RIP, and select New Interface from the menu that appears.
5. In the New Interface for RIP Version 2 for Internet Protocol dialog box, highlight the interface you want to configure this protocol to use. Click OK.
6. The RIP Properties dialog box for the interface you selected appears, as shown in Figure 16-21.

**FIGURE 16-21** Configuring RIP v2 properties for an interface

In the “Operation mode” drop-down list box, select either the “Periodic update mode” or the “Auto-static update mode.” Periodic update is the default for LAN connections. If this mode is selected, RIP v2 sends out updates every 30 seconds. Auto-static update mode is the default for demand-dial connections. If this mode is selected, RIP v2 sends out updates only when the remote router requests them.

In the “Outgoing packet protocol” drop-down list box, select the protocol that will be used by this router to send updates to other routers. The four choices are: RIP version 1 broadcast, RIP version 2 broadcast, RIP version 2 multicast, and Silent RIP. The default protocol is RIP version 2 broadcast. If you select Silent RIP, this router will accept updates from other routers, but won’t send out any updates of its own.

## STEP BY STEP

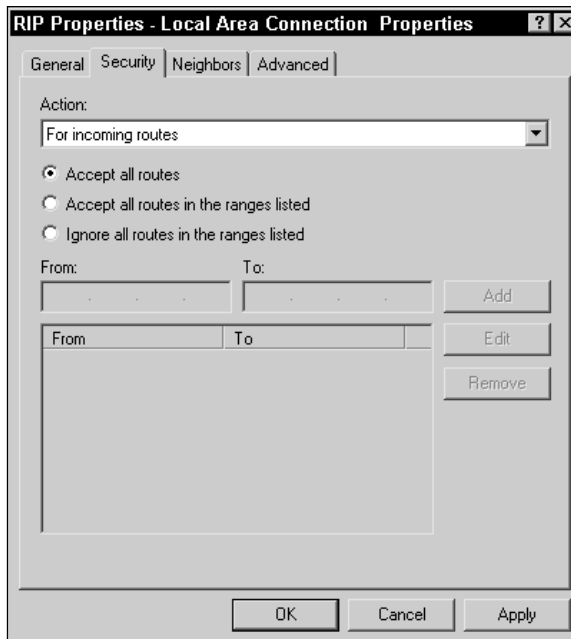
*Continued*

In the “Incoming packet protocol” drop-down list box, select the protocol that will be accepted by this router for incoming RIP packets. The four choices are: Ignore incoming packets, RIP version 1 and 2, RIP version 1 only, and RIP version 2 only. The default protocol is RIP version 1 and 2.

If you want this router to send a password when it communicates with other routers, and require that other routers send a password when they communicate with this router, select the check box next to “Activate authentication” and enter the password.

When you finish configuring options on this tab, click the Security tab.

7. The Security tab appears, as shown in Figure 16-22.



**FIGURE 16-22** Configuring RIP v2 security for an interface

On this tab you can configure security for incoming and outgoing routes. The default selection for both incoming routes and outgoing routes is “Accept all routes.” Selecting this option provides no security.

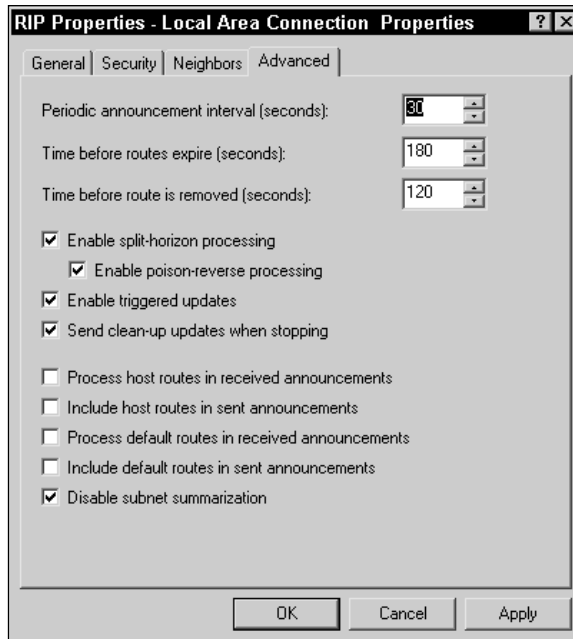
If security is needed, you can configure RIP v2 to either accept or ignore all routes in the ranges you specify. (If you select either of these two options, you must specify one or more ranges of IP addresses.)

When you finish configuring security options, click the Neighbors tab.

## STEP BY STEP

Continued

8. On this tab, you can specify how RIP v2 will communicate with neighbor routers. (A neighbor, in router-speak, is a router that is physically connected to any of the subnets that this router is physically connected to.) By default, RIP v2 uses broadcasts and multicasts when it sends out updates to its routing table. This means that the updates are not directed toward any specific router or computer. You can configure RIP v2 to send packets directly to neighbor routers (by specifying the router's IP address) *in addition to* using broadcasts or multicasts; or, you can configure RIP v2 to send packets directly to neighbor routers *instead of* using broadcasts or multicasts.
- When you finish making configurations on this tab, click the Advanced tab.
9. The Advanced tab appears, as shown in Figure 16-23. Notice the settings on this tab. This is the default configuration for RIP v2 on a local area connection.



**FIGURE 16-23** Configuring advanced RIP v2 properties for an interface

The options on this tab are seldom configured by administrators. For more information on any of the options, right-click the option's text, and select "What's This?" from the menu that appears. Windows 2000 displays a description of the option.

Make any necessary configuration changes, and click OK.

## STEP BY STEP

*Continued*

10. The interface you just configured RIP v2 to use is displayed in the right pane of the Routing and Remote Access dialog box. If you need to configure RIP v2 to use additional routing interfaces, repeat Steps 4 through 9 for each additional interface. Close Routing and Remote Access.

## Installing and Configuring Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic IP routing protocol that is designed for use in medium- to large-sized networks. OSPF is a link-state protocol that is relatively complex to configure and maintain. However, this protocol uses much less network bandwidth to maintain its routing table than RIP v2 uses, and its convergence time is much lower than RIP v2 on large networks — less than a minute. On the other hand, OSPF uses substantially more processor time than RIP v2 because it has to perform complex calculations to determine the shortest path to remote networks.

OSPF uses numerous difficult concepts and terms that you'll need to come to grips with. Here are some terms that you'll need to have under your belt before you can really understand OSPF and use it effectively on your network.

- **Routing area:** You can think of a routing area as a site — it's a group of IP subnets connected by high-speed links. In fact, if you're using Active Directory sites, it makes sense to configure a routing area for each site. Each routing area is identified by a number, called an area ID, that looks just like an IP address, only it has nothing to do with IP addressing — it simply identifies the area.
- **Backbone area (Area 0):** This is the area automatically created when OSPF is installed. This area is the core of OSPF routing. Normally, all other areas are connected to the backbone area. This area's ID is always 0.0.0.0 (hence the name, Area 0).
- **Internal routing:** This is routing that occurs within a single routing area.
- **Internal router:** This is a router that performs internal routing. All of this router's interfaces are connected to subnets in a single routing area.

- **Area border router:** This is a router that, unlike an internal router, has interfaces that are connected to subnets in more than one routing area. Normally, at least one interface of an area border router is connected to the backbone area, but this is not a requirement. Area border routers are used to route packets between routing areas.
- **Autonomous system:** All routing areas under the control of a single organization or company are referred to an autonomous system. You can think of an autonomous system as all of your company's networked routing areas.
- **Autonomous system boundary router:** This is a router that connects your autonomous system with either the Internet or another organization's autonomous system.

Now that your brain is overflowing with OSPF terminology, how about discussing something easier, like installing OSPF? OSPF can be installed on any Windows 2000 Server computer on which TCP/IP is installed and routing has been enabled.

## STEP BY STEP

### INSTALLING OPEN SHORTEST PATH FIRST (OSPF)

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to install OSPF. Then click the + next to IP Routing. Right-click General, and select New Routing Protocol from the menu that appears.
3. In the New Routing Protocol dialog box, select Open Shortest Path First (OSPF) from the list. Click OK.
4. The protocol is installed.

---

**Configuring OSPF to Use a Routing Interface** After you install OSPF, you need to configure it to use one or more of the routing interfaces in your Windows 2000 Server computer. Until you configure OSPF to use at least one routing interface, OSPF will be unable to dynamically update your routing tables.

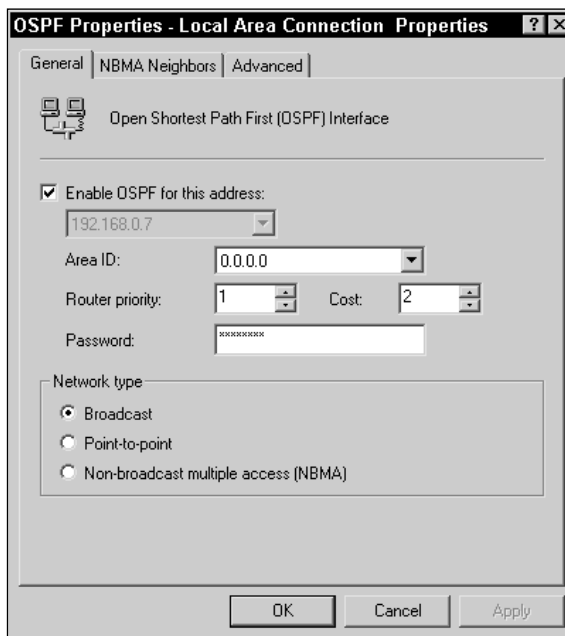


If you want to configure your OSPF router to perform internal routing only, ensure that all of the router's interfaces are connected to subnets within a single routing area.

## STEP BY STEP

### CONFIGURING OSPF TO USE AN INTERFACE

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which OSPF is installed. Then click the + next to IP Routing. Right-click OSPF, and select New Interface from the menu that appears.
3. In the New Interface for Open Shortest Path First (OSPF) dialog box, highlight the interface you want to configure OSPF to use. Click OK.
4. The OSPF Properties dialog box for the interface you selected appears, as shown in Figure 16-24. Notice the default settings for a local area connection.



**FIGURE 16-24** Configuring OSPF properties for an interface

Also notice that by default the check box next to “Enable OSPF for this address” is selected and that the IP address beneath it is grayed out. This is the default configuration for an interface that has only one IP address.

In the Area ID drop-down list box, select the routing area that this interface is physically connected to.

## STEP BY STEP

Continued

Either accept the default router priority and cost, or adjust them to meet your network's requirements.

In the Password text box, enter the password that will be used in the routing area you selected. If you don't configure a password, the default password is "12345678."

Finally, select the type of network this interface is connected to:

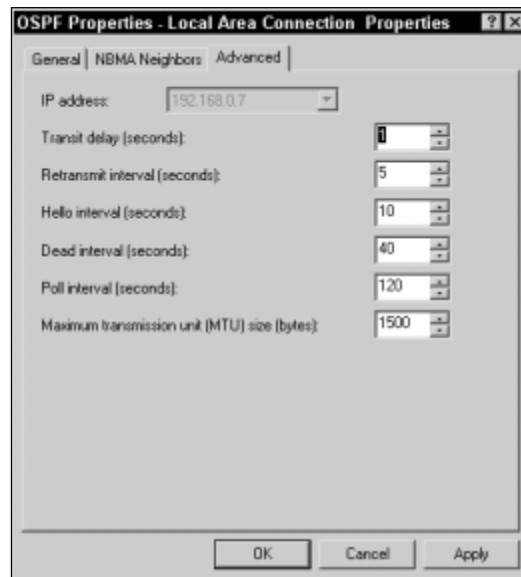
- ▶ **Broadcast:** Select this network type for all local area connections. If you are configuring a local area connection, this option is selected by default.
- ▶ **Point-to-point:** Select this network type for all demand-dial interfaces. If you're configuring a demand-dial interface, this option is selected by default.
- ▶ **Non-broadcast multiple access (NBMA):** Select this network type for all connections to X.25 or Frame Relay networks. If you're configuring an X.25 or Frame Relay interface, this option is selected by default.

When you finish configuring options on this tab, click the NBMA Neighbors tab.

5. On the NBMA Neighbors tab, specify a list of neighbor routers, by IP address, that this interface will use. The options on this tab are only available if you selected a network type of "Non-broadcast multiple access (NBMA)" on the General tab.

When you finish configuring this tab, click the Advanced tab.

6. The Advanced tab appears, as shown in Figure 16-25.



**FIGURE 16-25** Configuring advanced OSPF properties for an interface

## STEP BY STEP

*Continued*

The options on this tab are seldom configured by administrators. For more information on any of the options, right-click the option's text, and select "What's This?" from the menu that appears. Windows 2000 displays a description of the option.

Make any necessary configuration changes, and click OK.

7. The interface you just configured OSPF to use is displayed in the right pane of the Routing and Remote Access dialog box. If you need to configure OSPF to use additional interfaces, repeat Steps 2 through 6 for each additional interface. Close Routing and Remote Access.



## TIP

Remember, if you want this routing to perform internal routing only, make sure that all interfaces you configure this router to use are connected to subnets within the same routing area.

---

**Configuring Routing Areas** OSPF uses routing areas to break up its large, complex routing tables into manageable-sized chunks. Remember how I said that OSPF uses a lot of processor time to calculate the shortest path to each destination subnet? Well, if the routing table becomes too large, more demand may be placed on the router's hardware than it is capable of providing. So, the solution is to configure additional routing areas, which enable routers to maintain a portion of the company's routing table, instead of all of it.

Not all networks require multiple routing areas. If your network is small, you may only require a single routing area. In this case, Area 0 (the backbone area), which is automatically created when OSPF is installed, may be sufficient for your network's needs.

Routing areas are specified as one or more network number and subnet mask combinations. Each of these network number and subnet mask combinations specifies a subnet within the routing area. Because a subnet contains a range of IP addresses, these combinations are referred to as ranges.

## STEP BY STEP

## CONFIGURING OSPF AREAS

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which OSPF is installed. Then click the + next to IP Routing. Right-click OSPF, and select Properties from the menu that appears.

## STEP BY STEP

Continued

3. In the OSPF Properties dialog box, click the Areas tab.
4. The Areas tab appears, with the backbone area (0.0.0.0) displayed.

**To edit an area's configuration**, highlight the area, click Edit, and make any necessary configuration changes. Click OK.



## TIP

If you want to configure additional routing areas, you must edit Area 0 (the backbone area) and specify the network number and subnet mask combinations for the subnets you determine Area 0 should contain.

**To add an additional area**, click Add.

5. In the OSPF Area Configuration dialog box, enter the area ID for the new area. Click the Ranges tab.
6. On the Ranges tab, enter the network number and subnet mask combination for a subnet in the routing area. Click Add. Repeat this process until you've specified all subnets within the routing area. Click OK.
7. To define and configure additional routing areas, repeat Steps 4 through 6 until you've configured all desired routing areas. On the Areas tab, click OK.
8. Close Routing and Remote Access.

---

**Configuring Border Routing** *Border routing* is OSPF routing that spans more than one routing area. It requires the use of area border routers, which each have interfaces that are connected to subnets in more than one routing area.

Configuring border routing is much the same as configuring internal routing—the only difference is that in internal routing, all of the router's interfaces are connected to subnets within a single routing area; and in border routing, the router's interfaces are connected to subnets in more than one routing area. So, configuring border routing is simply a matter of configuring OSPF to use interfaces that are connected to subnets in different routing areas.

As I mentioned earlier, normally at least one interface of an area border router is connected to the backbone area, but this is not a requirement. In fact, sometimes, due to a company's network design, this is not possible. For example, suppose that you have a series of routing areas, and that Area 0 is connected to Area 10.0.0.0 by a router, and Area 10.0.0.0 is connected to Area 192.196.0.0 by a router, but Area 192.196.0.0 is *not* connected to Area 0 by a router. In this situation, the area border router that connects

Area 10.0.0.0 to Area 192.196.0.0 will not have a physical interface that is connected to Area 0. Instead, this border router will use an OSPF “virtual interface” to connect to Area 0 (the backbone area).

A virtual interface is simply a mapping that tells the border router which routing area is connected to Area 0 (and the IP address of a border router in the routing area that has an interface connecting it to Area 0) so that it has a way to forward packets to Area 0.

You can configure a virtual interface by configuring OSPF’s properties on the border router that does not have an interface connecting it to Area 0.

## STEP BY STEP

### CONFIGURING AN OSPF VIRTUAL INTERFACE

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to configure an OSPF virtual interface. Then click the + next to IP Routing. Right-click OSPF, and select Properties from the menu that appears.
3. In the OSPF Properties dialog box, click the Virtual Interfaces tab.
4. On the Virtual Interfaces tab, click Add.
5. The OSPF Virtual Interface Configuration dialog box appears, as shown in Figure 16-26.

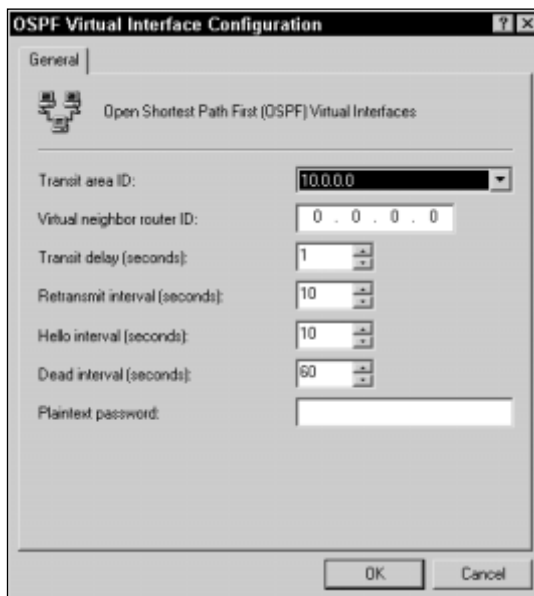


FIGURE 16-26 Configuring an OSPF virtual interface

**STEP BY STEP***Continued*

In the “Transit area ID” drop-down list box, select the area that is connected to Area 0.

In the “Virtual neighbor router ID” text box, enter the IP address of the border router in the transit area you specified that has an interface connected to Area 0.

The default selections for the remaining configurable options on this tab are acceptable for most situations. However, you must enter the password used by the virtual neighbor router in the “Plaintext password” text box.

Click OK.

6. In the OSPF Properties dialog box, click OK.
7. Close Routing and Remote Access.

---

## Installing and Configuring Network Address Translation (NAT)

Network Address Translation (*NAT*) is an IP routing protocol that enables computers (on a private network) that use private IP addresses to communicate with computers on the Internet that use registered IP addresses.

The cool thing about NAT is that a company only needs to have *one* registered IP address for its connection to the Internet, instead of having to pay for a registered IP address for *each* computer on its network. In addition, NAT prevents computers on the Internet from directly contacting computers on the private network, thus providing a measure of protection for corporate resources. I’m not saying that NAT is a full-blown firewall, but it’s certainly better than no protection at all.

Speaking of security, I recommend that you install NAT on a member server or a stand-alone server that doesn’t contain sensitive corporate information, not on a domain controller. The reason for this is that if NAT is installed on a domain controller, this computer, because it has a public IP address and has an interface that is connected to the Internet, is potentially vulnerable to hackers.

If you’re thinking that NAT sounds like Internet Connection Sharing, you’re right on the money. The main differences between the two are that NAT is configured on a router, and NAT doesn’t cause TCP/IP conflicts with existing IP routers, DHCP servers, or DNS servers on the network. In addition, NAT is more configurable than Internet Connection Sharing and is designed for larger networks. While Internet Connection Sharing is useful for home or very small office networks that don’t use a Windows

2000 domain, NAT is useful for small to medium-sized corporate networks that use Windows 2000 domains and Active Directory.

All computers on a network that uses NAT can use private IP addresses from the published private IP address ranges. Private IP addresses can't be used on the Internet, because Internet routers are configured not to forward packets addressed to these addresses. There are three ranges of private IP addresses:

10.0.0.1 – 10.255.255.254

172.16.0.1 – 172.31.255.254

192.168.0.1 – 192.168.255.254

For more information on private IP addresses, see RFC 1597, “Address Allocation for Private Internets.”

The interface on the Windows 2000 Server computer on which NAT is installed *does* need to have a registered IP address for the shared connection to the Internet.

NAT can be installed on any Windows 2000 Server computer on which TCP/IP is installed and routing has been enabled.

## STEP BY STEP

### INSTALLING NAT

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to install NAT. Then click the + next to IP Routing. Right-click General, and select New Routing Protocol from the menu that appears.
3. In the New Routing Protocol dialog box, select Network Address Translation (NAT) from the list. Click OK.
4. The protocol is installed.

---

**Configuring NAT Properties** NAT is a highly configurable IP routing protocol. You can configure event logging and TCP and UDP port translation. In addition, if another computer on your network runs a network application or service (such as a Web server or an FTP server) that needs to be accessed by users on the Internet, you can configure NAT to enable those users to access this application. Finally, you can choose whether to use

NAT as a DHCP server, a DNS proxy server, or both. A DNS proxy server receives name resolution requests from client computers, performs the name resolution by using DNS servers on the Internet, and then passes the results of the resolution back to the client computer.

## STEP BY STEP

### CONFIGURING NAT PROPERTIES

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which NAT is installed. Then click the + next to IP Routing. Right-click Network Address Translation (NAT), and select Properties from the menu that appears.
3. In the Network Address Translation (NAT) Properties dialog box, there are four tabs: General, Translation, Address Assignment, and Name Resolution.

On the General tab, configure how you want NAT to handle event logging. Select one of four logging levels: log errors only, log errors and warnings, log the maximum amount of information, or disable event logging.

When you finish event logging options, click the Translation tab.

4. On the Translation tab, you can set the number of minutes after which NAT will remove TCP and UDP port mappings. The default settings are 1440 minutes (24 hours) for TCP mappings, and 1 minute for UDP port mappings.

If you want to make a specific Internet application available to users on your network, click Applications and add the application in the dialog box provided. Click OK.

Click the Address Assignment tab.

5. The Address Assignment tab appears, as shown in Figure 16-27. Notice that by default, the check box next to “Automatically assign IP addresses by using DHCP” is not selected. NAT is not configured, by default, to function as a DHCP server for your network.

If you want to use NAT as a DHCP server, select the check box next to “Automatically assign IP addresses by using DHCP.” Then, either accept the default IP address and mask, or specify a different IP address range. If you’ve manually assigned some static IP addresses to computers or devices on your network, you can exclude these addresses by clicking Exclude and specifying the reserved addresses that NAT will not assign.



#### TIP

If you select this option, when NAT assigns IP addressing information to client computers, it will specify this Windows 2000 Server computer as the network’s default gateway and DNS server.



## STEP BY STEP

Continued

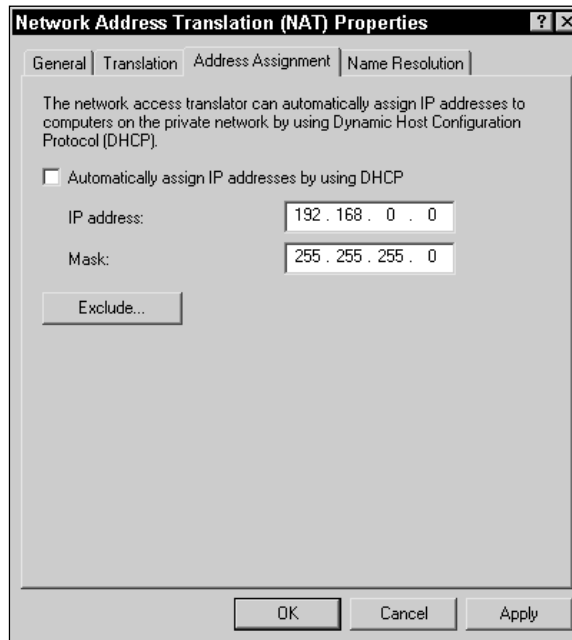


FIGURE 16-27 Configuring NAT to function as a DHCP server

If you *don't* select this option, you'll have to configure computers on your network to use this computer as their default gateway, and, if no DNS server is installed on the network, as their DNS server as well. Otherwise, computers on your network won't be able to access computers on the Internet.

After you finish making the appropriate configuration changes on this tab, click the Name Resolution tab.

6. On the Name Resolution tab, you can configure NAT to function as a DNS proxy server for the network. A DNS proxy server receives name resolution requests from client computers, performs the name resolution by using DNS servers on the Internet, and then passes the results of the resolution back to the client computer.



#### CAUTION

If the Windows 2000 Server computer on which NAT is installed is already functioning as a DNS server, this option should *not* be selected.

If this computer is *not* currently functioning as a DNS server, select the check box next to "Clients using Domain Name System (DNS)." In addition, if you are using another computer on your network as a DNS server, your existing DNS server *must* be configured to use the NAT server as a DNS forwarder.

**STEP BY STEP***Continued*

If you select the check box next to “Clients using Domain Name System (DNS),” and NAT is configured to use a demand-dial connection to the Internet, select the check box next to “Connect to the public network when a name needs to be resolved,” and select the appropriate demand-dial interface from the drop-down list box.

Make the appropriate configurations on this tab, and click OK.

7. Close Routing and Remote Access.

---

**Configuring NAT Interfaces** NAT must be configured to use two or more of the routing interfaces in your Windows 2000 Server computer. One of these interfaces must be the connection to the Internet. At least one other interface must be connected to your company’s private network — this is normally a local area connection.

Until you configure NAT to use these routing interfaces, users on your company’s private network won’t be able to use NAT to communicate with computers on the Internet. In the next section, I’ll show you how to configure NAT to use the routing interface connected to your company’s private network. It’s a very easy task to perform.

**STEP BY STEP****CONFIGURING NAT TO USE THE INTERFACE CONNECTED TO YOUR PRIVATE NETWORK**

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which NAT is installed. Then click the + next to IP Routing. Right-click Network Address Translation (NAT), and select New Interface from the menu that appears.
3. In the New Interface for Network Address Translation (NAT) dialog box, highlight the interface connected to your private network that you want NAT to use. (This is usually a Local Area Connection.) Click OK.
4. In the Network Address Translation Properties dialog box, ensure that the “Private interface connected to private network” option is selected. Click OK.

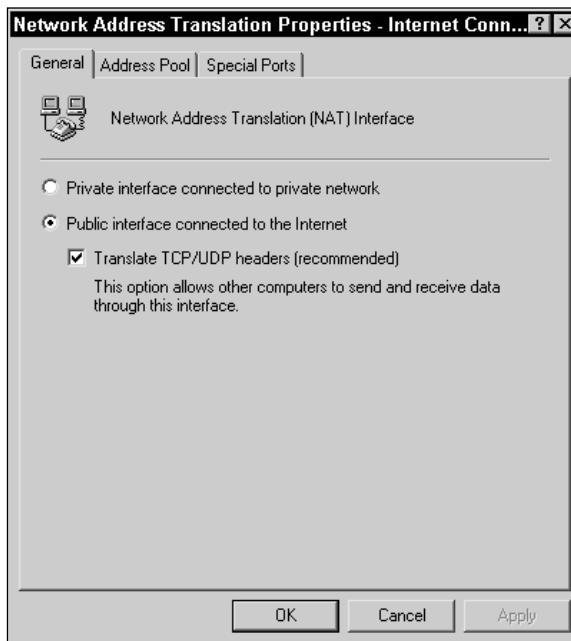
---

Unfortunately, configuring NAT to use a routing interface connected to the Internet is a more complex task.

## STEP BY STEP

**CONFIGURING NAT TO USE THE INTERFACE CONNECTED TO THE INTERNET**

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which NAT is installed. Then click the + next to IP Routing. Right-click Network Address Translation (NAT), and select New Interface from the menu that appears.
3. In the New Interface for Network Address Translation (NAT) dialog box, highlight the interface connected to the Internet that you want NAT to use. Click OK.
4. The Network Address Translation Properties dialog box for the interface you selected appears, shown in Figure 16-28.



**FIGURE 16-28** Configuring NAT to use an interface connected to the Internet

Ensure that the “Public interface connected to the Internet” option is selected. In addition, if you want users on your network to be able to access resources on the Internet, ensure that the check box next to “Translate TCP/UDP headers” check box is selected.

Click the Address Pool tab.

5. On the Address Pool tab, you can enter any public (registered) IP addresses assigned to you by your ISP that you want to associate with specific computers on your network.

**STEP BY STEP***Continued*

For example, if you have a Web server on your company's network (that runs on a computer other than the NAT server), you could associate one of the public IP addresses assigned to you with the private IP address of the Web server. Once this assignment is made, when the NAT server receives requests from users on the Internet that are addressed to the public IP address, the NAT server will forward these requests directly to the Web server's private IP address.

To make this assignment, first add the public IP addresses on this tab, then click Reservations, and associate the public IP address with the appropriate private IP address of the computer on your network.

When you finish making configurations on this tab, click the Special Ports tab.

6. The Special Ports tab enables you to redirect specific *types* of network traffic (such as http traffic) sent to a specific public IP address to the associated private IP address of a computer on your private network.

Configurations on this tab are not the same as making a reservation on the Address Pool tab. If you make an address reservation, all traffic sent to the specified public IP address is forwarded to the associated private IP address of the computer on your private network. If you use the Special Ports tab, only traffic that is sent to the specified public IP address *and that uses a specific TCP or UDP port* will be forwarded to the associated private IP address of the computer on your internal network.

The Special Ports feature gives you more granular control of what type of traffic is forwarded to the computers on your internal network, but requires substantial knowledge of TCP and UDP port numbers, including the applications associated with these port numbers. For more information on TCP and UDP port numbers, see RFC 1700, "Assigned Numbers."

Make any necessary configurations on this tab. Click OK.

7. Close Routing and Remote Access.

---

## Installing and Configuring the DHCP Relay Agent

The DHCP Relay Agent is a Windows 2000 routing protocol that forwards DHCP client configuration requests to a DHCP server on another network segment. The DHCP Relay Agent enables computers on one subnet to receive IP addresses from a DHCP server located on a different subnet.

The DHCP Relay Agent is typically installed on Windows 2000 Server computers that are functioning as static or dynamic IP routers, however any Windows 2000 Server computer on a network segment can function as the

DHCP Relay Agent. If you are not using Windows 2000 computers as routers, you may want to use the DHCP relay service that comes with your router (if there is one), instead of the Windows 2000 DHCP Relay Agent.

## STEP BY STEP

### INSTALLING AND CONFIGURING THE DHCP RELAY AGENT

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to install the DHCP Relay Agent. Then click the + next to IP Routing. Right-click General, and select New Routing Protocol from the menu that appears.
3. In the New Routing Protocol dialog box, select DHCP Relay Agent from the list. Click OK.
4. The protocol is installed. In the left pane of the Routing and Remote Access dialog box, right-click DHCP Relay Agent, and select Properties from the menu that appears.
5. In the DHCP Relay Agent Properties dialog box, enter the IP address of the DHCP server you want this router to forward DHCP client requests to, and click Add. Repeat this step if you want to specify more than one DHCP server. Click OK.
6. You must also bind the DHCP Relay Agent to all interfaces and connections on which you want it to be used. Until it is bound to an interface or connection, the DHCP Relay Agent won't function. To bind the DHCP Relay Agent to an interface or connection, in the left pane, right-click the DHCP Relay Agent, and select New Interface from the menu that appears.
7. In the New Interface for DHCP Relay Agent dialog box, select the interface you want to add. (The selections in this dialog box depend on the types of connections and routing interfaces you have configured on this computer.) Click OK.
8. The DHCP Relay Properties dialog box for the interface or connection you specified appears. Typically, the default selections in this dialog box are adequate and don't require modification. Make any necessary changes, and click OK.
9. Close Routing and Remote Access.

---

### Installing and Configuring IGMP

IGMP Version 2, Router and Proxy (which I'll call IGMP for short) is a dynamic IP routing protocol used to manage the propagation of multicast traffic throughout a routed TCP/IP network. IGMP stands for Internet Group Management Protocol.

When IGMP is installed and configured on a Windows 2000 Server computer, it maintains a table of multicast group members on the network (and the IP addresses of the subnets on which these members reside), and only forwards multicast traffic to the subnets on which multicast group members reside. In addition, like other dynamic routers, an IGMP router periodically forwards the contents of its IGMP tables to other IGMP routers on the network.

IGMP can be installed on any Windows 2000 Server computer on which TCP/IP is installed and routing has been enabled. After IGMP is installed, its properties can be configured, and IGMP must be configured to use one or more routing interfaces.

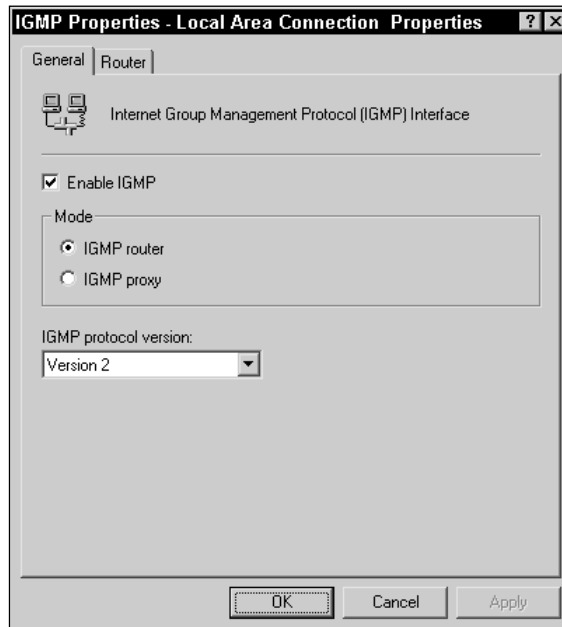
## STEP BY STEP

### INSTALLING AND CONFIGURING IGMP

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Routing and Remote Access.
2. In the Routing and Remote Access dialog box, click the + next to the server on which you want to install IGMP. Then click the + next to IP Routing. Right-click General, and select New Routing Protocol from the menu that appears.
3. In the New Routing Protocol dialog box, select "IGMP Version 2, Router and Proxy" from the list. Click OK.
4. The protocol is installed. To configure IGMP, in the left pane of the Routing and Remote Access dialog box, right-click IGMP, and select Properties from the menu that appears.
5. In the IGMP Properties dialog box, there is only one configuration to be made. Select the event logging level you want IGMP to use. You can choose from the following options: "Log errors only," "Log errors and warnings," "Log the maximum amount of information," or "Disable event logging." The default selection is "Log errors only." Click OK.
6. To configure IGMP to use an interface, in the left pane of the Routing and Remote Access dialog box, right-click IGMP, and select New Interface from the menu that appears.
7. In the New Interface for IGMP Version 2, Router and Proxy dialog box, select the interface you want IGMP to use, and click OK.
8. The IGMP Properties dialog box appears for the interface you selected, as shown in Figure 16-29. Notice that the check box next to "Enable IGMP" is selected. This is the default setting.

## STEP BY STEP

Continued

**FIGURE 16-29** Configuring IGMP to use a routing interface

Select one of two modes:

- ▶ **IGMP router:** Select this mode if you want IGMP to use information received by this interface to update the router's multicast group membership tables. Selecting this mode provides full IGMP functionality on this interface. This is the default selection.
- ▶ **IGMP proxy:** Select this mode if you want IGMP to use this interface only for forwarding multicast traffic. If the interface you are configuring is connected to a network that uses multicast routing protocols other than IGMP, select this mode. Only one interface in a router can be configured to use this mode.

When proxy mode is selected, all multicast packets received on router interfaces that are configured as IGMP routers are forwarded by the proxy mode interface. All multicast packets received by the proxy interface are forwarded by all interfaces that are configured as IGMP routers.

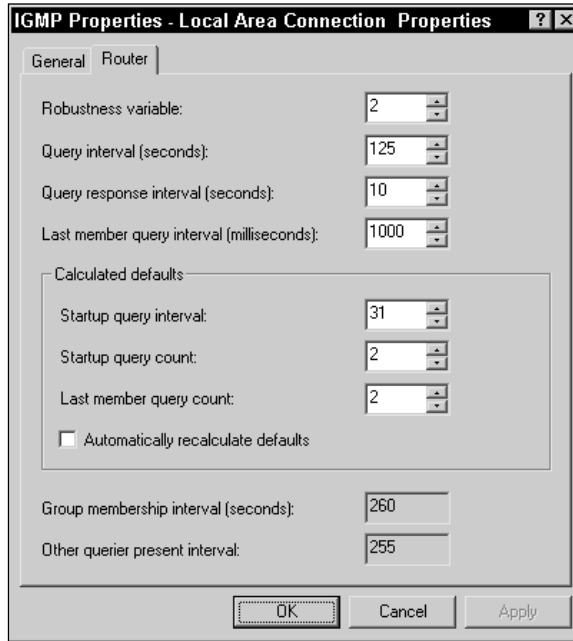
Then, select the IGMP protocol version you want IGMP to use on this interface. The version you select from the drop-down list box should match the version of IGMP in use by other IGMP routers on the network segment this interface is connected to. Your choices are either Version 1 or Version 2. Version 2 is the default selection and is supported by most implementations of IGMP.

Click the Router tab.

## STEP BY STEP

*Continued*

9. The Router tab appears, as shown in Figure 16-30. Notice the default settings on this tab.



**FIGURE 16-30** Configuring router options on an IGMP interface

The default configurations on this tab are acceptable for most situations. If you want more information about any of the options, right-click the text of an option and select "What's This?" from the menu that appears.

When you finish configuring router options, click OK.

10. Close Routing and Remote Access.

---

## Monitoring TCP/IP Routing

As an administrator, you should periodically monitor TCP/IP routing on the Windows 2000 Server computer you've configured to function as a router. In addition to monitoring the status of your server, interfaces, and ports and viewing various TCP/IP routing statistics, you'll want to ensure that routing tables are being constructed and maintained, and that the server has sufficient resources (such as memory, processor, and disk) to handle its routing tasks.



You can perform several monitoring tasks in Routing and Remote Access:

- By highlighting Server Status, you can view the status of this server and determine whether the Routing and Remote Access service is started.
- By highlighting Routing Interfaces, you can view a list of all routing interfaces configured for this server and the connection state (connected or disconnected) of each interface.
- By highlighting Ports, you can view a list of all ports in this computer and the port status (active or inactive) of each port.
- By right-clicking General (under IP Routing), you can view TCP/IP information (such as the number of IP routes, the number of IP datagrams forwarded, and so on). In addition, if IGMP is installed, you can view the multicast forwarding table and multicast statistics.
- By right-clicking Static Routes, you can view the IP routing table. This table includes any static entries you've configured, as well as dynamic entries generated by the routing protocols installed on this computer. Figure 16-31 shows a portion of an IP routing table.

Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	192.168.0.1	Local Area Connection	1	Network management
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.0.0	255.255.255.0	192.168.0.7	Local Area Connection	2	OSPF
192.168.0.0	255.255.255.0	192.168.0.7	Local Area Connection	1	Local
192.168.0.7	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	240.0.0.0	192.168.0.7	Local Area Connection	1	Local
255.255.255.255	255.255.255.255	192.168.0.7	Local Area Connection	1	Local

FIGURE 16-31 Viewing an IP routing table in Routing and Remote Access

- By highlighting any specific routing protocol, you can view the interfaces that protocol is configured to use and various statistics for those interfaces.
- By right-clicking a specific routing protocol, you can view various information pertaining to that protocol. Depending on the protocol, you may be able to view such items as: a list of neighbor routers (RIP and OSPF), a group table (IGMP), areas and the link-state database (OSPF), and DHCP allocator and DNS proxy information (NAT).

In addition to using Routing and Remote Access, you can use System Monitor, a Performance tool, to monitor the IP object and its many counters. In particular, the Datagrams Forwarded/sec counter is helpful for determining how many packets your router has forwarded. You can also use System Monitor to determine if your Windows 2000 Server computer that is functioning as a router has adequate memory, processor, and disk resources.



#### CROSS-REFERENCE

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

## Troubleshooting TCP/IP Routing

Most TCP/IP routing problems occur during the initial implementation of routing, and are the result of an incorrectly configured routing protocol, an incorrectly configured routing interface(s), or both, on your Windows 2000 Server computer.

The most common TCP/IP routing problem is the inability of a computer on one subnet to communicate with a computer located on another subnet. When this occurs, assuming that the hardware components of your network infrastructure (cables, hubs, and so on) are functioning properly, the most likely cause of the problem is an incorrect routing configuration or a failed router.

There are two primary tools you can use to help you diagnose and resolve TCP/IP routing problems: the `tracert.exe` command-line utility, and the Routing and Remote Access administrative tool.

`Tracert` is short for “trace route.” This command-line utility is useful for determining where routing communications have broken down. The `tracert.exe` command-line utility works by sending a test communication packet across the network to a remote computer. It then displays the path the packet takes on its journey from the source computer (the computer on which `tracert.exe` is run) to the destination computer, including all routers along the way. If `tracert.exe` is unable to contact the destination computer, you can easily view where the communications path between the two computers broke down, and specifically you can tell which router failed to correctly forward the message.

To use the `tracert.exe` command-line utility, start a command prompt on the source computer. At the command prompt, type **`tracert remote_computer_name`** (or **`remote_IP_address`**) and press Enter. `Tracert.exe`

will trace the communications path between the two computers, and then display the trace information.

The Routing and Remote Access administrative tool is also helpful for troubleshooting TCP/IP routing problems. By using this tool you can view the status of the server that's functioning as a router, determine whether the Routing and Remote Access service is started, and determine whether Routing and Remote Access is enabled on that server. If the service is not started, you can use the Services tool in Computer Management to start the Routing and Remote Access service. If Routing and Remote Access has been disabled for some reason, you can use the Routing and Remote Access tool to enable it.

You can also use Routing and Remote Access to verify that the routing protocols appropriate for your network are installed and configured correctly. In addition, you can verify that each routing protocol is configured to use the appropriate routing interface(s) on the computer.

## Configuring TCP/IP Packet Filters

Windows 2000 has a TCP/IP security feature called *TCP/IP packet filtering*. You can use TCP/IP packet filtering (often called TCP/IP filtering for short) to control the type of TCP/IP packets that a Windows 2000 computer on your network will receive. For example, you can prevent your Windows 2000 Server computer (that is functioning as a Web server) from receiving ping messages, which hackers sometimes use in an attempt to crash a server.

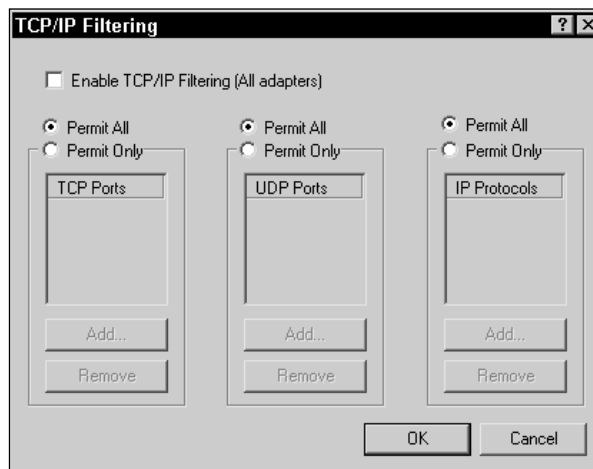
You can also use TCP/IP packet filtering to control the type of TCP/IP packets that each routing interface on your Windows 2000 Server computer (when it's functioning as a router) will receive, forward, or both. TCP/IP filtering was called TCP/IP Security in Windows NT 4.0.

TCP/IP packet filtering is not enabled by default. TCP/IP packet filtering for a computer is configured in the `Network and Dial-Up Connections` folder. TCP/IP packet filtering for a router is configured, on an interface-by-interface basis, by using the Routing and Remote Access administrative tool.

## STEP BY STEP

## CONFIGURING TCP/IP PACKET FILTERING FOR A COMPUTER

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the **Network and Dial-up Connections** folder, right-click any Local Area Connection, and select Properties from the menu that appears. (The settings you make on this connection will be applied to all Local Area Connections on the computer.)
3. In the Local Area Connection Properties dialog box, highlight the Internet Protocol (TCP/IP) and click Properties.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click Advanced.
5. In the Advanced TCP/IP Settings dialog box, click the Options tab.
6. On the Options tab, highlight “TCP/IP filtering” and click Properties.
7. The TCP/IP Filtering dialog box appears, as shown in Figure 16-32. Notice that, by default, the check box next to “Enable TCP/IP Filtering” is cleared.



**FIGURE 16-32** Configuring TCP/IP filtering for a Windows 2000 computer

To enable TCP/IP filtering on this computer, select the check box next to “Enable TCP/IP Filtering (All adapters).”

Then, to specify the types of traffic that will be permitted, select either the Permit All or Permit Only option for TCP Ports, UDP Port, and IP Protocols. If you select the Permit Only option, you must specify the types of traffic that will be accepted by this computer. If you select Permit Only and don’t specify the type of traffic that will be accepted, no traffic of that type will be accepted by the computer.

## STEP BY STEP

Continued

For example, if you select Permit Only for TCP Ports, you must specify the actual port numbers of all TCP ports that will be accepted by this computer.



## TIP

To configuring packet filtering for IP protocols, you must specify each allowed IP protocol by its associated protocol number. If you don't know what number is assigned to a protocol, you can use Notepad to view the *SystemRoot\system32\drivers\etc\protocol* file, or you can consult RFC 1700, "Assigned Numbers."

When you finish configuring packet filtering, click OK.

8. In the Advanced TCP/IP Settings dialog box, click OK. In the Internet Protocol (TCP/IP) Properties dialog box, click OK. In the Local Area Connection Properties dialog box, click OK.
9. Close the **Network and Dial-up Connections** folder.

## STEP BY STEP

## CONFIGURING TCP/IP PACKET FILTERING FOR A ROUTER

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 functions as a router) on which you want to configure TCP/IP packet filtering. Then click the + next to IP Routing. Highlight General. Then, in the right pane, right-click the interface for which you want to configure filtering, and select Properties from the menu that appears.
3. **If you want to limit the type of network traffic this interface will receive**, click Input Filters.  
**If you want to limit the type of network traffic this interface will send or forward**, click Output Filters.
4. The Input Filters (or Output Filters) dialog box appears. You'll come back to this dialog box in a minute, but for now you need to decide whether you want to add filters that will exclude specified types of traffic, or add filters that will permit only specified types of traffic. Click Add.
5. In the Add IP Filter dialog box, you can filter network traffic that comes from a specific source network (subnet) or that is addressed to a specific destination network (subnet). Or, you can filter network traffic by IP protocol type or by TCP or UDP port number. When you finish configuring the filter, click OK.

**STEP BY STEP***Continued*

6. Repeat Steps 4 and 5 until you've added all of the filters you need for this interface.
7. Then, if you're creating an input filter, choose one of the following options that specify how the filters you've created will be applied to this interface:
  - ▶ **Receive all packets except those that meet the criteria below**
  - ▶ **Drop all packets except those that meet the criteria below.**Or, if you're creating an output filter, choose one of the following options that specify how the filters you've created will be applied to this interface:
  - ▶ **Transmit all packets except those that meet the criteria below**
  - ▶ **Drop all packets except those that meet the criteria below.**Select the appropriate option and click OK.
8. In the Properties dialog box for the interface, click OK.
9. Close Routing and Remote Access.

## Configuring and Troubleshooting IPSec

IPSec is short for Internet Protocol security. *IPSec* is a collection of security protocols and cryptography services that encrypts TCP/IP traffic between two computers, thus preventing unauthorized users who capture network traffic from viewing or modifying sensitive data. Windows 2000 is the first Windows operating system that provides support for IPSec.

The most common use of IPSec is on corporate networks that transmit sensitive data over their internal networks. IPSec is also used for communications between two private networks via the Internet.

Some advantages of using IPSec are that IPSec is relatively easy to implement on a Windows 2000 network, it provides seamless functionality to users, and it can provide a high level of security. The only disadvantage is the increased processor utilization required to encrypt and decrypt TCP/IP traffic.

**EXAM TIP**

Expect to see several tough IPSec questions on the Network exam. Be sure you know how to create and configure IPSec policies, rules, and filters, and that you know when to use transport mode and tunnel mode. I recommend you practice configuring these elements before taking the exam.

There are a couple of IPSec terms you should be familiar with: *transport mode* and *tunnel mode*. IPSec is implemented in one of these two modes.

IPSec's default mode is transport mode. In this mode, IPSec encrypts the data portion of each IP packet, and then sends the IP packet to the destination computer. This mode is typically used on a company's internal network.

IPSec can be configured to use tunnel mode. Tunnel mode is typically used between two routers that are connected via a public network such as the Internet. Tunnel mode is very similar to a VPN, and is often used for the same reasons. In tunnel mode, IPSec first encrypts the entire IP packet. Then, IPSec uses the encrypted packet as the data portion of a new IP packet that it creates and sends, usually over the Internet, to the destination computer. The original IP packet is said to be "tunneled" within the new IP packet.

In the following sections I'll explain how to enable IPSec, how to create and customize IPSec policies, and how to configure IPSec for tunnel mode. Finally, I'll cover monitoring and troubleshooting IPSec.

## Enabling IPSec

IPSec is not enabled by default. IPSec is implemented in Windows 2000 as a security policy. Because of this, the tool you use to enable IPSec depends on which computer(s) on your network you want to enable IPSec for:

- To enable IPSec on an individual Windows 2000 computer, you can configure the advanced TCP/IP settings for any Local Area Connection in the **Network and Dial-up Connections** folder, or you can use the Local Security Policy tool in Administrative Tools. (Select Start ⇨ Settings ⇨ Control Panel, double-click Administrative Tools, then double-click Local Security Policy.) Or, you can use the local Group Policy editor (`gpedit.msc`).
- To enable IPSec on all Windows 2000 computers in a domain, you can use the Domain Security Policy tool in Administrative Tools. (Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Domain Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.

- To enable IPsec on all domain controllers in a domain, you can use the Domain Controller Security Policy tool in Administrative Tools. (Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Domain Controller Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.
- To enable IPsec on all Windows 2000 computers in a particular OU in a domain, you can use Active Directory Users and Computers to configure a Group Policy object (GPO) that enables IPsec on all of the computers in the OU.

The easiest way to enable IPsec for a large number of computers on a network is by using Group Policy. I'll show you how to do this in the steps that follow.

## STEP BY STEP

### ENABLING IPSEC BY USING GROUP POLICY

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, expand domains and OUs as necessary until the domain or OU associated with the GPO for which you want to enable IPsec is displayed in the left pane. Highlight the domain or OU, then select Action ⇨ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO you want to use to enable IPsec, and click Edit. (You can also double-click the GPO.)
5. The Group Policy dialog box appears. Click the + next to the **windows Settings** folder in the Computer Configuration section. Then click the + next to Security Settings. Highlight IP Security Policies on Active Directory. The three default IPsec policies are displayed in the right pane.
6. To enable IPsec, you must select *one* of these policies and assign it to the computers to which this GPO applies. The three default policies are:
  - ▶ **Client (Respond Only):** If you select this policy, the computers in the domain or OU (to which this GPO applies) won't use IPsec for regular communications – they will only use IPsec to communicate with a computer that requests the use of IPsec.



## STEP BY STEP

Continued

- ▶ **Secure Server (Require Security):** If you select this policy, the computers in the domain or OU (to which this GPO applies) will use IPSec for all communication with other computers. Other computers on the network that don't have IPSec enabled *won't* be able to communicate with the computers to which this GPO applies.
- ▶ **Server (Request Security):** If you select this policy, the computers in the domain or OU (to which this GPO applies) will use IPSec for all communication with other computers in the domain or OU. Other computers on the network that don't have IPSec enabled *will* be able to communicate with the computers to which this GPO applies.



## TIP

A Windows 2000 computer can have only *one* IPSec policy.

In the right pane, right-click the policy you want to assign, and select Assign from the menu that appears.

7. Close the Group Policy dialog box.
8. In the domain or OU's Properties dialog box, click OK.
9. Close Active Directory Users and Computers.

---

IPSec is now enabled on the computers to which the GPO applies.

## Creating and Customizing IPSec Policies

When you enabled IPSec, you were introduced to the three default IPSec policies. In most cases, these default policies will be adequate to implement IPSec on your network. However, it's conceivable that your network may have special needs that require you to create or customize an IPSec policy. But before I get into the nuts and bolts of creating and customizing policies, I want to explain a little about IPSec policies.

As I mentioned earlier, a Windows 2000 computer can have only one IPSec policy. An IPSec policy consists of one or more IPSec rules. IPSec rules specify how IPSec will be applied on the computer. When an IPSec policy has more than one rule, Windows 2000 applies the most specific rule (that is, the rule containing the most restrictive IP filter) first, and applies the most general rule last. An administrator can't specify the order

in which rules are applied — Windows 2000 determines this order. Each rule contains several IPsec configuration settings:

- **IP Filter:** When you configure a rule, you choose an IP filter that spells out what specific type of IP traffic this IPsec rule applies to.
- **IP Filter Action:** You also choose a filter action, which determines whether IPsec will either require encryption of the IP traffic specified by the filter, request encryption of this traffic, or permit unencrypted traffic.
- **Authentication Method:** This setting involves selecting how this computer will authenticate itself to the destination computer. There are three methods: the Windows 2000 default method (Kerberos V5 protocol), using a certificate from a specified certificate authority, and using a predetermined encryption key.
- **Tunnel Setting:** This option specifies whether IPsec will be used in transport mode or tunnel mode. By default, IPsec is used in transport mode. If tunnel mode is used, you must specify the IP address of the destination computer with which the tunnel will be established.
- **Connection Type:** This setting specifies whether this rule applies to all network connections, only to local area connections, or only to remote access connections.

Now that you have a better understanding of the contents of an IPsec policy, I'll show you how to create and customize one.

## STEP BY STEP

### CREATING AN IPSEC POLICY

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, expand domains and OUs as necessary until the domain or OU associated with the GPO for which you want to create an IPsec policy is displayed in the left pane. Highlight the domain or OU, then select Action ⇨ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to create an IPsec policy, and click Edit.

**STEP BY STEP***Continued*

5. The Group Policy dialog box appears. Click the + next to the **Windows Settings** folder in the Computer Configuration section. Then click the + next to Security Settings. Right-click IP Security Policies on Active Directory, and select Create IP Security Policy from the menu that appears.
6. The IP Security Policy Wizard starts. Follow the instructions presented on-screen to create the IPsec policy.

---

Once you've created the new IPsec policy, Windows 2000 prompts you to edit and customize this policy. The following steps explain how to customize any IPsec policy.

**STEP BY STEP****CUSTOMIZING AN IPSEC POLICY**

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, expand domains and OUs as necessary until the domain or OU associated with the GPO for which you want to customize an IPsec policy is displayed in the left pane. Highlight the domain or OU, then select Action ⇨ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO for which you want to customize an IPsec policy, and click Edit.
5. The Group Policy dialog box appears. Click the + next to the **Windows Settings** folder in the Computer Configuration section. Then click the + next to Security Settings. Highlight IP Security Policies on Active Directory. In the right-pane, right-click the policy you want to customize and select Properties from the menu that appears.
6. The IPsec policy's Properties dialog box appears, as shown in Figure 16-33. This happens to be a Properties dialog box for a newly created IPsec policy. Notice that, by default, a newly created policy only has the Default Response rule associated with it.  
  
On the Rules tab you can add, remove, and edit rules for this IPsec policy. To add a rule, click Add.
7. The Create IP Security Rule wizard starts. Click Next.

## STEP BY STEP

Continued

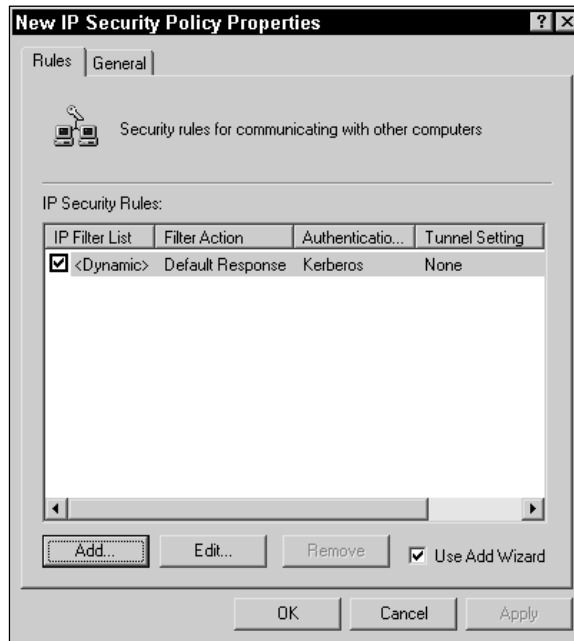


FIGURE 16-33 Configuring an IPSec policy

8. In the Tunnel Endpoint screen, select from one of two options:
  - ▶ **This rule does not specify a tunnel:** This is the default setting. If chosen, IPSec functions in transport mode.
  - ▶ **The tunnel endpoint is specified by this IP address:** Select this option if you want to configure IPSec for tunnel mode. If you select this option, specify the IP address of the destination computer with which the tunnel will be established. (This is usually the IP address of a router that connects a company's private network to the Internet.)

Click Next.

9. In the Network Type screen, select the type of network connections to which this rule will apply. Your options are:
  - ▶ **All network connections**
  - ▶ **Local area network (LAN)**
  - ▶ **Remote access**

Click Next.

10. The Authentication Method screen appears, as shown in Figure 16-34.

## STEP BY STEP

Continued

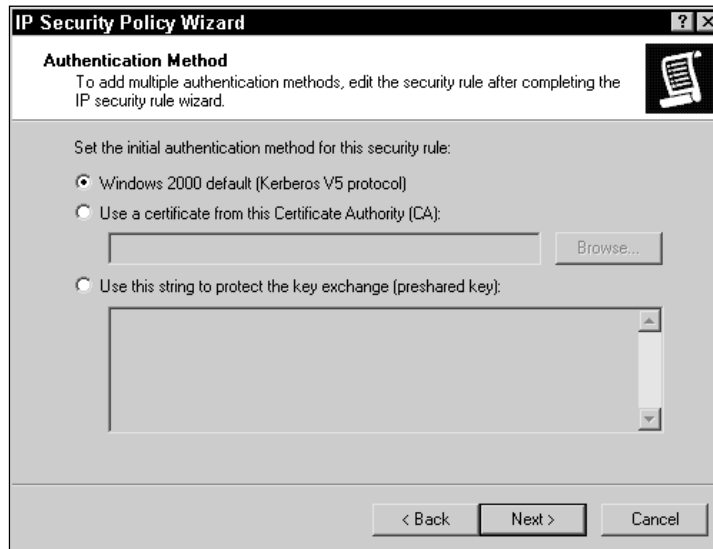


FIGURE 16-34 Selecting an authentication method for an IPSec rule

Select the appropriate method, make any additional configurations needed, and click Next.

11. The IP Filter List screen appears, as shown in Figure 16-35.

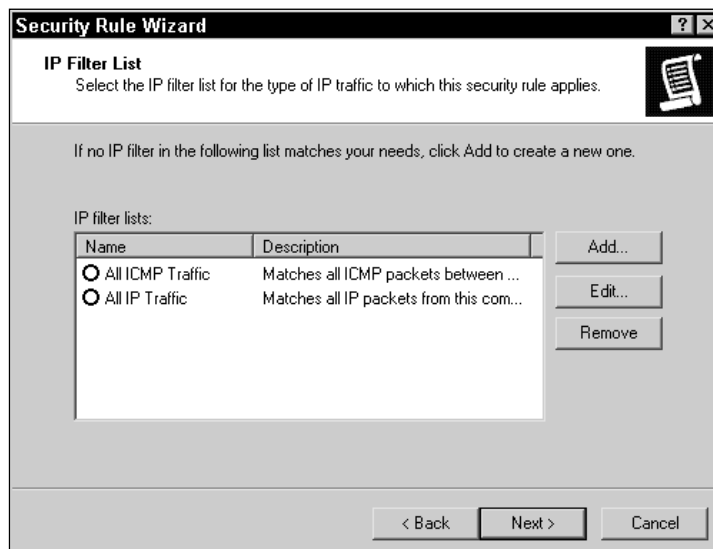


FIGURE 16-35 Selecting an IP filter for an IPSec rule

## STEP BY STEP

*Continued*

Either select the IP filter you want this rule to use, or click Add to create a new filter. You can create a filter that specifies an IP protocol, a TCP or UDP source or destination port, a source IP address (or IP address range), or a destination IP address (or IP address range). You can create a complex filter that combines one or more of these options. In addition, when you create a new IP filter, the filter will be available for all IPSec rules, not just this one. When you finish selecting or creating an IP filter, click Next.

12. The Filter Action screen appears, as shown in Figure 16-36. Notice the three default filter actions you can select from: Permit, Request Security (Optional), and Require Security.



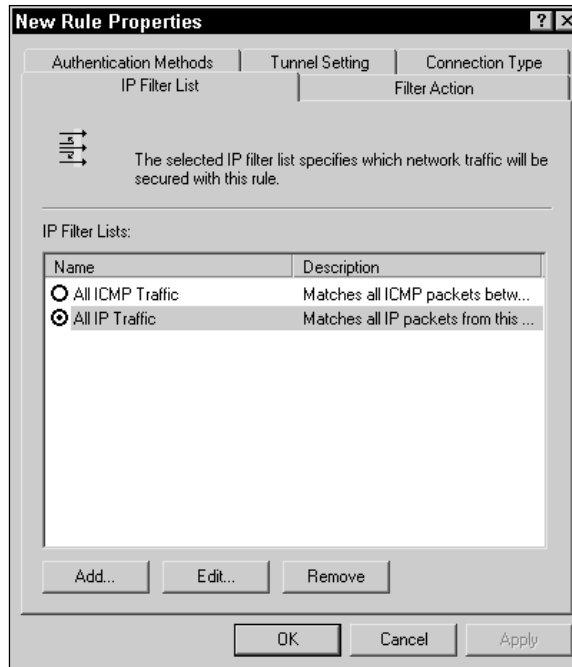
**FIGURE 16-36** Selecting an IP filter action for an IPSec rule

Either select the filter action you want this rule to use, or click Add to create a new filter action. When you finish selecting or creating a filter action, click Next.

13. The Completing the New Rule Wizard screen appears. If you need to edit the rule you've just created, accept the default selection in the check box next to "Edit properties." If you don't want to edit this rule, clear this check box. Click Finish.
14. If you accepted the default selection in the previous step, the rule's Properties dialog box appears, as shown in Figure 16-37.

Notice the five tabs in this dialog box: IP Filter List, Filter Action, Authentication Methods, Tunnel Setting, and Connection Type. Edit this rule as desired, and click OK.

## STEP BY STEP

*Continued*

**FIGURE 16-37** Configuring the properties of an IPSec rule

15. The IPSec policy's Properties dialog box reappears. Ensure that the check box next to each rule you want this policy to use is selected. These rules are displayed in the order they are created – not necessarily in the order that Windows 2000 will apply them. Click Close.
16. Close Group Policy. In the domain or OU's Properties dialog box, click OK. Close Active Directory Users and Computers.

## Monitoring IPSec

Windows 2000 includes a nice tool for monitoring IPSec — it's called IP Security Monitor. You can use IP Security Monitor to:

- Determine whether IPSec is enabled on the monitored Windows 2000 computer (this can either be the local computer on which you run IP Security Monitor, or a remote computer specified when you start IP Security Monitor).

- Determine if IPSec security is being used when the monitored Windows 2000 computer communicates with other computers.
- View various IPSec statistics.

IP Security Monitor is available on both Windows 2000 Professional and Windows 2000 Server computers.

## STEP BY STEP

### USING IP SECURITY MONITOR

1. From the desktop, select Start ⇨ Run.
2. In the Run dialog box, type **ipsecmon *computer\_name*** and press Enter. *Computer\_name* represents the name of the computer for which you want to monitor IPSec. If you don't specify a computer name, IP Security Monitor will monitor the local computer.
3. IP Security Monitor starts. Figure 16-38 shows the IP Security Monitor dialog box. Notice the box in the lower right portion of the screen that indicates whether IP Security (IPSec) is enabled on this computer.

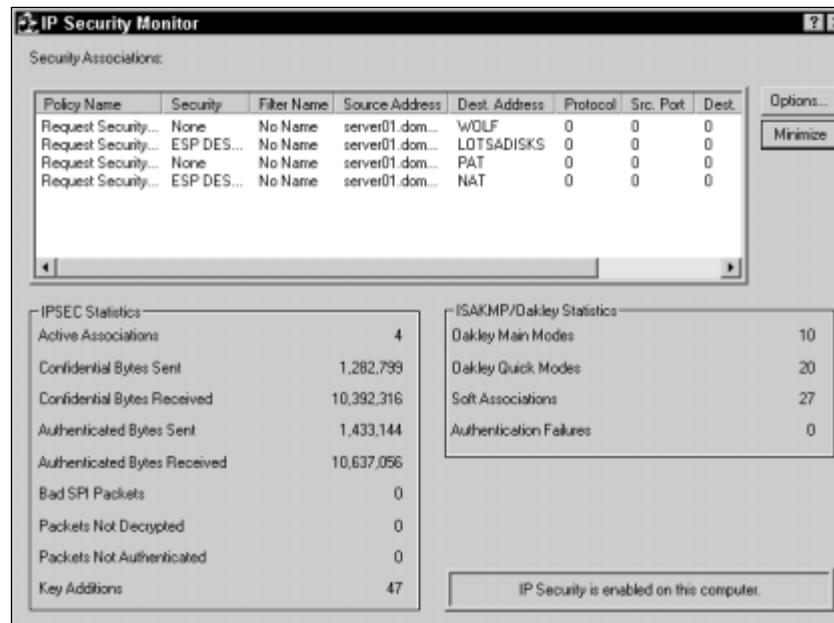


FIGURE 16-38 Using IP Security Monitor



## STEP BY STEP

*Continued*

By default, the statistics in this dialog box are updated every 15 seconds. To change this frequency, click Options and enter the number of seconds you want IP Security Monitor to wait between refreshes.

When you finish monitoring IPsec, close the IP Security Monitor dialog box.

## Troubleshooting IPsec

If you use the default policies and default rules when configuring IPsec, it's not likely that you'll run into too many problems. However, if you create custom rules, IP filters, filter actions, and so on, things can become pretty complex, and even confusing. If you're having problems getting IPsec up and running on your Windows 2000 network, here are a few tips that might help:

- Use IP Security Monitor to determine whether IPsec is enabled on a Windows 2000 computer, and whether IPsec security is being used for this computer's communications with other computers.
- If you've recently implemented an IPsec policy on a Windows 2000 computer, but IPsec is either not enabled or IPsec security is not being used by this computer, try rebooting the computer before performing more complex troubleshooting actions.
- If you enable IPsec by using Group Policy, but IPsec is not enabled on the intended computers, follow standard Group Policy troubleshooting methods to ensure that Group Policy (including IPsec policy) is being applied appropriately.
- If you've customized one or more of the three default IPsec policies, and you want to restore these policies to their original configurations, you can highlight IP Security Policies on Active Directory (in Group Policy editor) and select Action ⇨ All Tasks ⇨ Restore Default Policies.
- If multiple administrators can edit IPsec policies and you're concerned that the policies may be corrupt, you can check the integrity of these policies by highlighting IP Security Policies on Active Directory (in Group Policy editor) and select Action ⇨ All Tasks ⇨ Check Policy

**Integrity.** If the IPSec policies are not corrupt, Windows 2000 displays a dialog box indicating that the integrity of these policies has been verified.

- If you think that the system files used to implement IPSec may be damaged or missing, you can reinstall these files by removing, and then reinstalling, TCP/IP on the Windows 2000 computer.



## KEY POINT SUMMARY



This chapter introduced several important TCP/IP topics:

- The Transmission Control Protocol/Internet Protocol (TCP/IP) is a widely used transport protocol. It is a fast, routable enterprise protocol that is used on the Internet. In addition to being supported by Windows 2000, TCP/IP is supported by many other operating systems.
- IP addresses must be unique – no two computers or other network devices on an internetwork should have the same IP address.
- You can assign an IP address to a Windows 2000 computer either by manually specifying a computer's IP address configuration, or by configuring a computer to obtain IP addressing information automatically from a DHCP server.
- When the DHCP service is installed on a Windows 2000 Server computer that is a member of a domain, before the service can start, you must authorize the DHCP server in Active Directory.
- A DHCP server requires one or more scopes to assign IP addressing information to client computers. You can use the DHCP administrative tool to create scopes, superscopes, and multicast scopes.
- NetBIOS name resolution is normally accomplished in one of two ways. You can either manually configure an lmhosts file on each individual computer on the network, or install a WINS server and configure client computers on the network to use it.
- IP routing is a function of the Internet Protocol (IP) that uses IP address information to send data packets from a source computer on one network segment across one or more routers to a destination computer on another network segment.

- In order to function as a router, a Windows 2000 Server computer must have at least one network adapter card installed. In addition, it must have either an additional network adapter card or a communications device, such as a modem, installed.
- Routing is enabled on a Windows 2000 Server computer by using the Routing and Remote Access administrative tool. If no additional routing protocols are installed, the computer will function as a static router.
- The five routing protocols that ship with Windows 2000 Server are: RIP Version 2 for Internet Protocol, Open Shortest Path First (OSPF), Network Address Translation (NAT), the DHCP Relay Agent, and IGMP.
- When a routing protocol is installed, it must be configured to use at least one (and sometimes more) interfaces on the Windows 2000 Server computer.
- TCP/IP packet filtering is a TCP/IP security feature used to control the type of TCP/IP packets that a Windows 2000 computer will receive. It is also used to control the type of TCP/IP packets that each routing interface on a Windows 2000 Server computer (that's functioning as a router) will receive, forward, or both.
- IPsec is another security feature of TCP/IP in Windows 2000. IPsec is a collection of security protocols and cryptography services that encrypts TCP/IP traffic between two computers, thus preventing unauthorized users who capture network traffic from viewing or modifying sensitive data.

## STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about TCP/IP and to help you prepare for the Professional, Server, and Network exams:

- **Assessment questions:** These questions test your knowledge of the TCP/IP 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 analyze TCP/IP, DHCP, WINS, routing, and IPSec configurations or problems. 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 Exercises:** These exercises are hands-on practice activities that you perform on a computer. The two labs in this chapter give you an opportunity to practice configuring TCP/IP, installing and configuring DHCP and WINS, configuring routing, and enabling IPSec.

### Assessment Questions

1. You are manually configuring TCP/IP addressing information on a Windows 2000 Professional computer on your network. What should you enter in the "Default gateway" text box?
  - A. The IP address of a WINS server on the local network segment
  - B. The IP address of a router on the local network segment
  - C. The local network segment's subnet mask
  - D. The local network segment's network ID
2. You just finished installing the Dynamic Host Configuration Protocol (DHCP) service on a Windows 2000 Server computer that is a domain controller on your network. What must you do before the DHCP service can start?

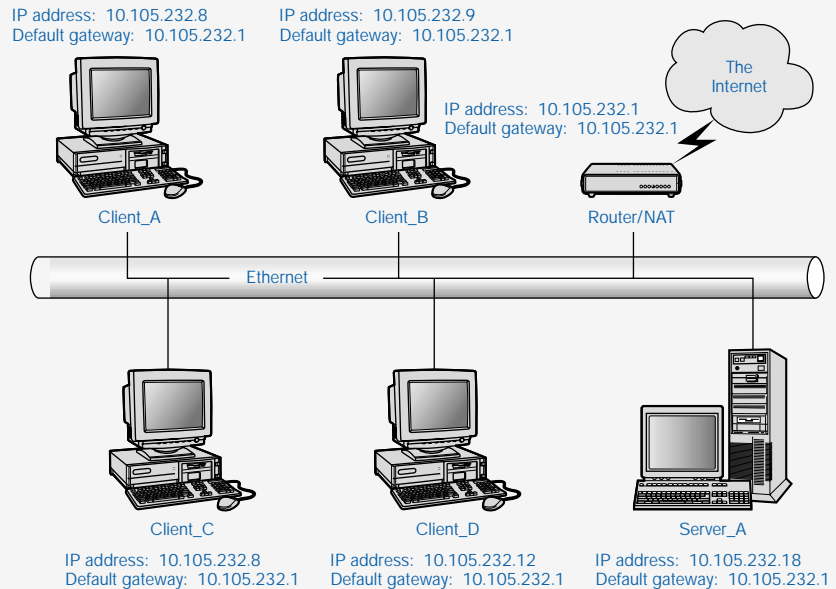
- A. Authorize the DHCP server in Active Directory
  - B. Configure a scope, a superscope, and a multicast scope
  - C. Configure a DHCP address reservation
  - D. Configure the DHCP server for DNS integration
3. You want to create a scope on your Windows 2000 Server DHCP server that will contain a range of Class D IP addresses so that the DHCP server can assign these addresses to client computers that request them. What kind of scope should you create?
- A. A scope
  - B. A superscope
  - C. A multicast scope
  - D. Any of the above scope types
4. You recently installed WINS on a Windows 2000 Server computer on your network. Prior to installing WINS, you configured the computer's local area connection with a static IP address. Because of your network's size, only a single WINS server will be needed. What else must you do in order for the WINS server to begin providing NetBIOS name resolution services on your network?
- A. Add IP address-to-NetBIOS name entries to the `lmhosts` file on each client computer
  - B. Configure WINS replication
  - C. Authorize the WINS server in Active Directory
  - D. Configure each client computer to use the WINS server
5. You are the administrator of a medium-sized private network. You have existing routers and DHCP servers on this network. You want to enable computers on your company's network that use private IP addresses to communicate with computers on the Internet that use registered IP addresses. Which Windows 2000 feature or protocol should you use to accomplish this?
- A. Internet Connection Sharing
  - B. OSPF
  - C. NAT
  - D. DHCP Relay Agent

6. You want to enable dynamic routing on a Windows 2000 Server computer on your TCP/IP network. You want this computer to manage the propagation of multicast traffic throughout your network. Which routing protocol should you use?
  - A. IGMP Version 2, Router and Proxy
  - B. Open Shortest Path First (OSPF)
  - C. RIP Version 2 for Internet Protocol
  - D. Network Address Translation (NAT)
7. You want to enable static routing on a Windows 2000 Server computer on your network. TCP/IP is installed and configured on this computer, and the computer has two network adapter cards installed. You use the Routing and Remote Access administrative tool to enable routing. What additional protocol must be installed before static routing can occur?
  - A. RIP Version 2 for Internet Protocol
  - B. NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
  - C. Open Shortest Path First (OSPF)
  - D. No additional protocols need to be installed
8. You want to provide security for TCP/IP communications on your company's routed Windows 2000 network. What features or protocols can you use to provide security? (Choose all that apply.)
  - A. TCP/IP packet filtering
  - B. IPSec
  - C. IP Security Monitor
  - D. Internet Connection Sharing

## Scenarios

In this chapter I introduced you to numerous TCP/IP and TCP/IP-related topics. Here's your chance to tackle a few situations you might encounter in real life. For each of the following problems, consider the given facts and answer the question or questions that follow.

1. Users of two computers on your Windows 2000 network report that they are unable to communicate with other computers on the network. Figure 16-39 shows the configuration of several components on this network subnet.



**FIGURE 16-39** Network configuration for problem 1

- a. What is causing the TCP/IP connectivity problem in this situation?
  - b. What should you do to resolve the problem?
2. You recently installed and configured the DHCP service on a Windows 2000 Server computer on your network. The computer is a member server of Domain4. You've created several scopes on the DHCP server, but client computers are not able to obtain their IP addressing information from this server.
    - a. What is the most likely cause of this problem?
    - b. What should you do to resolve the problem?
  3. You recently enabled IPSec for all computers in your Windows 2000 domain by using Group Policy. However, you discover, by using IP Security Monitor, that IPSec is not enabled on any of the computers in one of the OUs in the domain.
    - a. What is the most likely cause of this problem?
    - b. What should you do to resolve the problem?
  4. Your company's Windows 2000 network has two WINS servers, one in San Francisco and the other in Houston. The two locations are connected by a 56 Kbps WAN link. You are in the process of configuring WINS replication between these two servers.

- a. Which replication partner type should you select for each of these servers?
  - b. What additional replication configuration will you probably want to make?
5. A user of one of the Windows 98 client computers on your Windows 2000 network reports that she is unable to connect to servers on the network by using the servers' NetBIOS names. You use both WINS and DNS servers on your network.
- a. What is the most likely cause of this problem?
  - b. What should you do to resolve this problem?
6. You are the administrator for a large, routed TCP/IP network that spans multiple locations and uses numerous routers and WAN links. Your Windows 2000 computer is unable to connect to a Windows 2000 Server computer located on a remote subnet. What tool can you use to determine where the network communications are breaking down?

## Lab Exercises

### Lab 16-1 Configuring TCP/IP



- ▶ Professional
- ▶ Server
- ▶ Network

The purpose of this lab is to provide you with an opportunity to practice the TCP/IP configuration skills you learned in this chapter. Specifically, you'll manually configure TCP/IP on your Windows 2000 Professional computer, and configure a TCP/IP packet filter.

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

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the *Network and Dial-up Connections* folder, right-click the Local Area Connection, and select Properties from the menu that appears.



3. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
4. In the Internet Protocol (TCP/IP) Properties dialog box, ensure that the “Use the following IP address” option is selected. Then change the computer’s IP address by adding 100 to the number that represents the fourth octet. For example, if your IP address is currently 192.168.59.101, change it to 192.168.59.201.



#### CAUTION

---

If you’re on a live company network, changing your computer’s IP address could cause TCP/IP communications problems on the network, so you may not want to perform this step.

Click Advanced.

5. In the Advanced TCP/IP Settings dialog box, click the Options tab.
6. On the Options tab, highlight TCP/IP filtering and click Properties.
7. In the TCP/IP Filtering dialog box, select the check box next to “Enable TCP/IP Filtering (All adapters).” Then, in the IP Protocols section, select the Permit Only option, and click Add.
8. In the Add Filter dialog box, type **6** in the IP Protocol text box. Click OK.
9. In the TCP/IP Filtering dialog box, in the IP Protocols section, click Add again.
10. In the Add Filter dialog box, type **17** in the IP Protocol text box. Click OK.
11. In the TCP/IP Filtering dialog box, in the IP Protocols section, click Add again.
12. In the Add Filter dialog box, type **1** in the IP Protocol text box. Click OK.
13. In the TCP/IP Filtering dialog box, notice that three protocols are listed in the IP Protocols section. You have just configured a filter that permits only IP traffic that uses the ICMP (1), TCP (6), and UDP (17) protocols. Click OK.
14. In the Advanced TCP/IP Settings dialog box, click OK.
15. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.

16. In the Local Area Connection Properties dialog box, click OK.
17. In the Local Network dialog box, click Yes to restart your computer now. Boot your computer to Windows 2000 Server and log on as Administrator to perform the next lab.

## Lab 16-2 Managing TCP/IP on Your Network



- ▶ Professional
- ▶ Server
- ▶ Network

The purpose of this lab is to provide you with an opportunity to practice using many of the TCP/IP-related services, protocols, and features you learned about in this chapter.

There are five parts to this lab:

- Part 1: Installing Network Services (DHCP and WINS)
- Part 2: Configuring DHCP
- Part 3: Configuring NetBIOS Name Resolution and Monitoring WINS
- Part 4: Configuring and Monitoring Routing
- Part 5: Enabling, Configuring, and Monitoring IPsec

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

### Part 1: Installing Network Services (DHCP and WINS)

In this part, you install the DHCP and WINS services on your Windows 2000 Server computer.

1. Select Start ⇨ Settings ⇨ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, highlight Networking Services, and click Details.

5. In the Networking Services dialog box, select the check boxes next to Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS), and click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. When prompted, insert your Windows 2000 Server compact disc into your computer's CD-ROM drive and click OK. When the Microsoft Windows 2000 CD dialog box appears, close it. Windows 2000 configures components and installs DHCP and WINS. In the Completing the Windows Components Wizard screen, click Finish.
8. Close Add/Remove Programs. Then close Control Panel. Remove your Windows 2000 Server compact disc from your computer's CD-ROM drive.

## Part 2: Configuring DHCP

In this part, you configure the DHCP service. First, you authorize the DHCP server in Active Directory and configure DHCP for DNS integration. Next, you create a superscope and five scopes, and configure DHCP options for those scopes. Next, you create a multicast scope. Finally, you monitor DHCP by using the DHCP administrative tool.

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ DHCP.
2. In the left pane of the DHCP dialog box, highlight server01.domain1.mcse. Select Action ⇨ Authorize.
3. Wait a minute or two, then select Action ⇨ Refresh.
4. The DHCP Server is now authorized. Notice that the icon next to the DHCP server now contains a green, upward pointing arrow (instead of a red, downward pointing arrow).
5. In the DHCP dialog box, select Action ⇨ Properties.
6. In the server01.domain1.mcse Properties dialog box, click the DNS tab.
7. On the DNS tab, select the "Always update DNS" option. Then select the check box next to "Enable updates for DNS clients that do not support dynamic update." Click OK.
8. In the DHCP dialog box, select Action ⇨ New Scope.
9. The New Scope wizard starts. Click Next.

10. In the Scope Name screen, type in a name of **Superscope** and a description of **A superscope containing 6 scopes** in the text boxes provided. Click Next.
11. The IP Address Range screen appears. In the “Start IP address” text box, type **192.168.59.1**. In the “End IP address” text box, type **192.168.64.254**. Accept the default Length and Subnet mask settings. Click Next.
12. In the Create Superscope screen, select the Yes option and click Next.
13. In the Lease Duration screen, accept the default DHCP lease duration of 8 days, and click Next.
14. In the Configure DHCP Options screen, accept the default selection of “Yes, I want to configure these options now,” and click Next.
15. In the Router (Default Gateway) screen, enter an IP address of **192.168.59.1** and click Add. Click Next.
16. In the Domain Name and DNS Servers screen, in the “Parent domain” text box, type **domain1.mcse**. Then, in the IP address text box, type in the IP address of this computer, which should be **192.168.59.101** unless you have been instructed to use a different IP address. Click Add. Click Next.
17. In the WINS Servers screen, enter an IP address of **192.168.59.101**. Click Add. Click Next.
18. In the Activate Scope screen, accept the default selection of Yes. Click Next.
19. In the Completing the New Scope Wizard screen, click Finish.
20. Windows 2000 creates the scope. It is displayed in the right pane of the DHCP dialog box. Select Action ⇌ New Multicast Scope.
21. The New Multicast Scope wizard starts. Click Next.
22. In the Multicast Scope Name screen, type in a name of **Multicast** in the text box provided. Click Next.
23. The IP Address Range screen appears. In the “Start IP address” text box, type **239.0.0.1**. In the “End IP address” text box, type **239.0.5.254**. Accept the TTL of 32. Click Next.
24. In the Add Exclusions screen, click Next.
25. In the Lease Duration screen, accept the default DHCP multicast lease duration of 30 days, and click Next.

26. In the Activate Multicast Scope screen, select Yes. Click Next.
27. In the Completing the New Multicast Scope Wizard screen, click Finish.
28. Windows 2000 creates the multicast scope. It is displayed in the right pane of the DHCP dialog box. Click the + next to Superscope Superscope 0. Click the + next to Scope 192.168.59.0. Highlight Address Leases. The right pane is probably empty right now, but normally, after the DHCP server has been up and running for a while, and clients have been configured to obtain their IP addressing information from the DHCP server, there will be several leases listed.
29. In the left pane, right-click server01.domain1.mcse and select Display Statistics from the menu that appears.
30. Notice the DHCP server statistics that are displayed. Click Close.
31. Close DHCP.

### Part 3: Configuring NetBIOS Name Resolution and Monitoring WINS

In this part, you configure NetBIOS name resolution options on your Windows 2000 Server computer, and then you monitor your WINS server.

1. Select Start ⇨ Settings ⇨ Network and Dial-up Connections.
2. In the `Network and Dial-up Connections` folder, right-click the computer's Local Area Connection, and select Properties from the menu that appears.
3. In the Local Area Connection Properties dialog box, highlight the Internet Protocol (TCP/IP) and click Properties.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click Advanced.
5. In the Advanced TCP/IP Settings dialog box, click the WINS tab.
6. On the WINS tab, click Add.
7. In the TCP/IP WINS Server dialog box, type **192.168.59.101** (or the IP address of this computer, if you have been instructed to use a different IP address). Click Add.
8. On the WINS tab, click OK.
9. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
10. In the Local Area Connection Properties dialog box, click OK.

11. Close the **Network and Dial-up Connections** folder.
12. Shut down and restart your computer so that it will register its IP address with the WINS server. Reboot your computer to Windows 2000 Server, and log on as Administrator.
13. Select **Start** ⇨ **Programs** ⇨ **Administrative Tools** ⇨ **WINS**.
14. In the left pane of the WINS dialog box, click the + next to **SERVER01**. Then right-click **SERVER01**, and select **Display Server Statistics** from the menu that appears.
15. The WINS Server 'SERVER01' Statistics dialog box is displayed. View your WINS server's statistics, then click **Close**.
16. In the left pane of the WINS dialog box, highlight the **Active Registrations** folder. Then right-click this folder and select **Find by Owner** from the menu that appears.
17. In the **Find by Owner** dialog box, select the "All owners" option, and click **Find Now**.
18. The WINS database is displayed in the right pane of the WINS dialog box. When you finish viewing the database, close WINS.

#### Part 4: Configuring and Monitoring Routing

In this part, you enable routing on your Windows 2000 server computer. Next, you update a routing table by adding a static route. Then, you add two routing interfaces and implement demand-dial routing. Next, you install and configure routing protocols, including OSPF and NAT. Then you implement internal routing and border routing. Finally, you monitor IP routing statistics.

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**, 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. In the **Common Configurations** screen, select the "Network router" option. Click **Next**.
5. In the **Routed Protocols** screen, click **Next**.

6. In the Demand-Dial Connections screen, select the Yes option, and click Next.
7. In the IP Address Assignment dialog box, accept the default selection of Automatically, and click Next.
8. In the Completing the Routing and Remote Access Server Setup Wizard screen, click Finish.
9. Windows 2000 starts the Routing and Remote Access service. Your Windows 2000 Server computer is now configured as a static router.
10. In the left pane of the Routing and Remote Access dialog box, click the + next to SERVER01. Click the + next to IP Routing. Right-click Static Routes, and select New Static Route from the menu that appears.
11. In the Static Route dialog box, select Local Area Connection from the Interface drop-down list box. Then enter the following information in the appropriate text boxes:
  - Destination: **10.99.0.0**
  - Network mask: **255.255.0.0**
  - Gateway: **192.168.59.254**
  - Metric: **1**Click OK.
12. In the left pane of the Routing and Remote Access dialog box, right-click Routing Interfaces, and select New Demand-dial Interface from the menu that appears.
13. The Demand Dial Interface wizard starts. Click Next.
14. In the Interface Name screen, accept the default name of Remote Router. Click Next.
15. In the Connection Type screen, accept the default option of "Connect using a modem, ISDN adapter, or other physical device." Click Next.
16. In the "Select a device" screen, select "Standard 56000 bps V90 Modem" from the list. Click Next.
17. In the Phone Number screen, type in **5551212**. Click Next.
18. In the Protocols and Security screen, accept the default selection and click Next.

19. In the Dial Out Credentials screen, enter a user name of **Administrator**, a domain name of **domain1**, and a password of **password**. Confirm the password by retyping it. Click Next.
20. In the “Completing the demand-dial interface wizard” screen, click Finish.
21. In the left pane of the Routing and Remote Access dialog box, right-click Routing Interfaces, and select New Demand-dial Interface from the menu that appears.
22. The Demand Dial Interface wizard starts. Click Next.
23. In the Interface Name screen, type in a name of **Internet**. Click Next.
24. In the Connection Type screen, accept the default option of “Connect using a modem, ISDN adapter, or other physical device.” Click Next.
25. In the “Select a device” screen, select “Standard 56000 bps V90 Modem” from the list. Click Next.
26. In the Phone Number screen, type in **5559998**. Click Next.
27. In the Protocols and Security screen, accept the default selection and click Next.
28. In the Dial Out Credentials screen, enter a user name of **Administrator**, a domain name of **ISP**, and a password of **password**. Confirm the password by retyping it. Click Next.
29. In the “Completing the demand-dial interface wizard” screen, click Finish.
30. In the left pane of the Routing and Remote Access dialog box, right-click General (under IP Routing), and select New Routing Protocol from the menu that appears.
31. In the New Routing Protocol dialog box, highlight Open Shortest Path First (OSPF) and click OK.
32. In the left pane of the Routing and Remote Access dialog box, right-click General (under IP Routing), and select New Routing Protocol from the menu that appears.
33. In the New Routing Protocol dialog box, highlight Network Address Translation (NAT) and click OK.



34. In the left pane of the Routing and Remote Access dialog box, right-click Network Address Translation (NAT), and select Properties from the menu that appears.
35. In the Network Address Translation (NAT) Properties dialog box, select the “Log the maximum amount of information” option and click OK.
36. In the left pane of the Routing and Remote Access dialog box, right-click Network Address Translation (NAT), and select New Interface from the menu that appears.
37. In the New Interface for Network Address Translation (NAT) dialog box, select Local Area Connection and click OK.
38. In the Network Address Translation Properties – Local Area Connection dialog box, ensure that the “Private interface connected to private network” option is selected. Click OK.
39. In the left pane of the Routing and Remote Access dialog box, right-click Network Address Translation (NAT), and select New Interface from the menu that appears.
40. In the New Interface for Network Address Translation (NAT) dialog box, select Internet and click OK.
41. In the Network Address Translation Properties – Internet dialog box, ensure that the “Public interface connected to the Internet” option is selected, and that the check box next to “Translate TCP/UDP headers” is also selected. Click OK.
42. In the left pane of the Routing and Remote Access dialog box, right-click OSPF, and select Properties from the menu that appears.
43. In the OSPF Properties dialog box, click the Areas tab.
44. On the Areas tab, click Edit.
45. In the OSPF Area Configuration dialog box, click the Ranges tab.
46. On the Ranges tab, enter a Destination of **192.168.0.0** and a Network mask of **255.255.0.0** and click Add. Click OK.
47. On the Areas tab, click Add.
48. In the OSPF Area Configuration dialog box, enter an Area ID of **10.200.0.0** and click the Ranges tab.
49. On the Ranges tab, enter a Destination of **10.200.0.0** and a Network mask of **255.255.0.0** and click Add. Click OK.

50. On the Areas tab, click OK.
51. In the left pane of the Routing and Remote Access dialog box, right-click OSPF, and select New Interface from the menu that appears.
52. In the New Interface for Open Shortest Path First (OSPF), select Local Area Connection and click OK.
53. In the OSPF Properties – Local Area Connection Properties dialog box, ensure that the Area ID is 0.0.0.0. Click OK.
54. In the left pane of the Routing and Remote Access dialog box, right-click OSPF, and select New Interface from the menu that appears.
55. In the New Interface for Open Shortest Path First (OSPF), select Remote Router and click OK.
56. In the OSPF Properties – Remote Router Properties dialog box, select an Area ID of 10.200.0.0 from the drop-down list box. Click OK.
57. In the left pane of the Routing and Remote Access dialog box, highlight Server Status. Then, in the right pane, view the status of your router.
58. Highlight Routing Interfaces. Then, in the right pane, view all of the local area and demand-dial interfaces on your router.
59. Right-click General (under IP Routing), and select Show TCP/IP Information from the menu that appears.
60. The SERVER01 – TCP/IP Information dialog box is displayed. View the statistics in this dialog box, then close the dialog box.
61. Right-click OSPF, and select Show Link-state Database from the menu that appears.
62. The SERVER01 – OSPF Link State Database dialog box appears. View this database. Close the dialog box.
63. Close Routing and Remote Access.

## Part 5: Enabling, Configuring, and Monitoring IPSec

In this part, you enable IPSec on your Windows 2000 Server computer, and configure and customize IPSec policies and rules for domain1.mcse and for server01. You also configure IPSec for transport mode and tunnel mode. Finally, you use IP Security Monitor to view and monitor IPSec.

1. Select Start ⇨ Programs ⇨ Administrative Tools ⇨ Domain Security Policy.

2. In the left pane of the Domain Security Policy dialog box, highlight IP Security Policies on Active Directory. In the right pane, right-click Server (Request Security) and select Properties from the menu that appears.
3. In the Server (Request Security) Properties dialog box, click Add.
4. The Create IP Security Rule wizard starts. Click Next.
5. In the Tunnel Endpoint screen, select the “The tunnel endpoint is specified by this IP address” option. Then enter an IP address of **192.168.200.1** and click Next.
6. In the Network Type screen, accept the default option of “All network connections” and click Next.
7. In the Authentication Method screen, click Next.
8. In the IP Filter List screen, click Add.
9. In the IP Filter List dialog box, type in a name of **Tunnel Mode** and a description of **All IP traffic for remote network** and click Add.
10. The IP Filter wizard starts. Click Next.
11. In the IP Traffic Source screen, select a source address of “Any IP address” from the drop-down list box. Click Next.
12. In the IP Traffic Destination screen, select a destination address of “A specific IP subnet” from the drop-down list box. Then enter an IP address of **192.168.240.0** and a subnet mask of **255.255.255.0** and click Next.
13. In the IP Protocol Type screen, select a protocol type of Any from the drop-down list box. Click Next.
14. In the Completing the IP Filter Wizard screen, ensure that the “Edit properties” check box is cleared, and click Finish.
15. In the IP Filter List dialog box, click Close.
16. In the IP Filter List screen in the Security Rule Wizard, select the Tunnel Mode filter from the IP filter lists box. Click Next.
17. In the Filter Action screen, select Require Security. Click Next.
18. In the Completing the New Rule Wizard screen, ensure that the “Edit properties” check box is cleared and click Finish.
19. In the Server (Request Security) Properties dialog box, notice the new Tunnel Mode rule that you created is displayed and selected. Click Close.

20. In the right pane of the Domain Security Policy dialog box, right-click Server (Request Security) and select Assign from the menu that appears.
21. Close Domain Security Policy.
22. Select Start ⇨ Run.
23. In the Run dialog box, type **secedit /refreshpolicy machine\_policy** and click OK.
24. Select Start ⇨ Run.
25. In the Run dialog box, type **ipsecmon server01** and click OK
26. The IP Security Monitor on server01 dialog box appears. Notice in the lower right corner of this dialog box that IP Security is enabled on this computer. View the various IPSec statistics displayed in this dialog box. Close IP Security Monitor.

## Answers to Chapter Questions

### Chapter Pre-Test

1. The Transmission Control Protocol/Internet Protocol (TCP/IP) is a widely used transport protocol. It is a fast, routable, enterprise protocol that is used on the Internet. In addition to being supported by Windows 2000, TCP/IP is supported by many other operating systems. TCP/IP is typically the recommended protocol for large, heterogeneous networks.
2. True
3. A default gateway address specifies the IP address of a router on the local network segment.
4. You can assign an IP address to a Windows 2000 computer in one of two ways: by manually specifying a computer's IP address configuration, or by configuring a computer to obtain IP addressing information automatically from a DHCP server.
5. A DHCP scope is a range of IP addresses on a DHCP server that can be assigned to DHCP clients that reside on a single subnet.

6. Windows Internet Name Service (WINS) is a Windows 2000 Server service that provides NetBIOS name resolution services to client computers.
7. You can use the Routing and Remote Access administrative tool to enable routing on a Windows 2000 Server computer.
8. The five routing protocols that ship with Windows 2000 are: RIP Version 2 for Internet Protocol, Open Shortest Path First (OSPF), Network Address Translation (NAT), the DHCP Relay Agent, and IGMP.
9. TCP/IP packet filtering and IPSec

## Assessment Questions

1. **B.** The default gateway address must specify the IP address of a router on the local network segment.
2. **A.** Before the DHCP service can start, the DHCP server must be authorized in Active Directory.
3. **C.** A superscope is the only type of scope that can contain other scopes.
4. **D.** When WINS is used, `lmhosts` files are not needed. If only one WINS server will be used, WINS replication does not need to be configured. A WINS server doesn't need to be authorized in Active Directory.
5. **C.** Network Address Translation (NAT) is the best answer. Internet Connection Sharing won't work because there are already existing routers and DHCP servers on the network.
6. **A.** IGMP is the only routing protocol that manages multicast traffic.
7. **D.** Dynamic routing requires the installation of additional protocols, but static routing does not.
8. **A, B.** Neither IP Security Monitor nor Internet Connection Sharing provide any security.

## Scenarios

1. The problem in this situation is that Client\_A has the same IP address as Client\_C. Duplicate IP addresses are not permitted. To resolve the problem, you should change either Client\_A's or Client\_C's IP address so that it is a unique IP address.
2. The most likely cause of this problem is that the DHCP server has not been authorized in Active Directory. Until the DHCP server is authorized, the DHCP service won't start on the server. You should use the DHCP administrative tool to authorize the DHCP server in Active Directory.
3. The most likely cause of this problem is that the OU is configured to block policy inheritance, or has a conflicting GPO. You should reconfigure Group Policy on the OU so that inheritance is no longer blocked, or that the conflicting GPO for the OU is removed, reordered, or reconfigured.
4. You should select a replication type of Pull for both servers. In addition, you might want to schedule WINS replication to occur during nonbusiness hours.
5. The most likely cause of this problem is that the Windows 98 computer is not configured to use the WINS server for NetBIOS name resolution. You should configure the Windows 98 computer to use the WINS server by specifying the IP address of your WINS server.
6. You should use the `tracert.exe` command-line utility to view the path through the network that attempted communication from your computer is taking, and to determine where network communication stops. Then you'll know which router is failing to correctly forward TCP/IP packets to the remote server.