CHAPTER

Networking Using TCP/IP

16

About Chapter 16

This chapter is a concise, practical primer on TCP/IP and related subjects.

After a brief overview of TCP/IP, this chapter discusses IP addressing, including how IP addresses are assigned, and explains the different types of IP routing.

Next, the chapter explains how to install and configure WINS, an NT Server service that provides NetBIOS name resolution to client computers. Then, installing and configuring Microsoft DNS Server, which provides host name resolution to client computers, is covered.

Then the chapter turns its attention to publishing on the Internet. Two Microsoft products, Internet Information Server and Peer Web Services, are featured. Complete steps to install these products are included.

Finally, Chapter 16 presents tips on troubleshooting common TCP/IP connectivity problems.

This chapter boasts four hands-on labs. In these labs, you'll implement WINS and Microsoft DNS Server, configure Internet Information Server, and install and configure Peer Web Services. You'll also install and configure an Internet (TCP/IP) router, and try to identify and resolve some common TCP/IP connectivity problems.

Chapter 16 is a "must read," no matter which of the three Windows NT 4.0 Microsoft Certified Professional exams you're preparing for. This chapter covers numerous exam objectives, including objectives concerning TCP/IP, protocols, network components, multiprotocol routing, Internet Information Server, Internet services, Peer Web Services, and troubleshooting objectives on resolving connectivity problems.

OVERVIEW OF TCP/IP

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

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

Microsoft includes several TCP/IP-based services with Windows NT that enhance networking, including Microsoft DHCP Server, RIP for Internet Protocol, Windows Internet Name Service (WINS), Microsoft DNS Server, Microsoft Internet Information Server, and Peer Web Services. Each of these services is discussed in this chapter.

concept link **This chapter covers only the basics of TCP/IP that are required for the Workstation, Server, and Enterprise exams. Volumes have been written on this subject! For more information on TCP/IP, see the TCP/IP topics in Books Online, and *TCP/IP MCSE Study Guide,* by Greg Bulette (IDG Books Worldwide, 1997).**

A good place to begin a basic discussion of TCP/IP is with IP addressing—including subnet masks and default gateway 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'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 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 have the same network ID.* The length of the network ID within an IP address is variable and is specified by

the subnet mask used in conjunction with the IP address. (Subnet masks are discussed 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 assure that unique IP addresses are used, if you plan to connect your network to the Internet, you should contact your Internet Service Provider or InterNIC to obtain a range of valid IP addresses for your network.

web links **InterNIC, which manages domain names as well as IP addresses, can be reached by e-mail at** `info@internic.net`.

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.

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 use the last two octets as the host ID. (Without getting into too much binary math, an octet number of 255 specifies the *entire* octet is part of the network ID; and an octet number of 0 specifies 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.)

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 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.

IP address: 192.168.75.122
Default gateway: 192.168.75.1

Computer_A

── Subnet_A ──

IP address: 192.168.75.1

Router

IP address: 192.168.70.1

── Subnet_B ──

IP address: 192.168.70.31
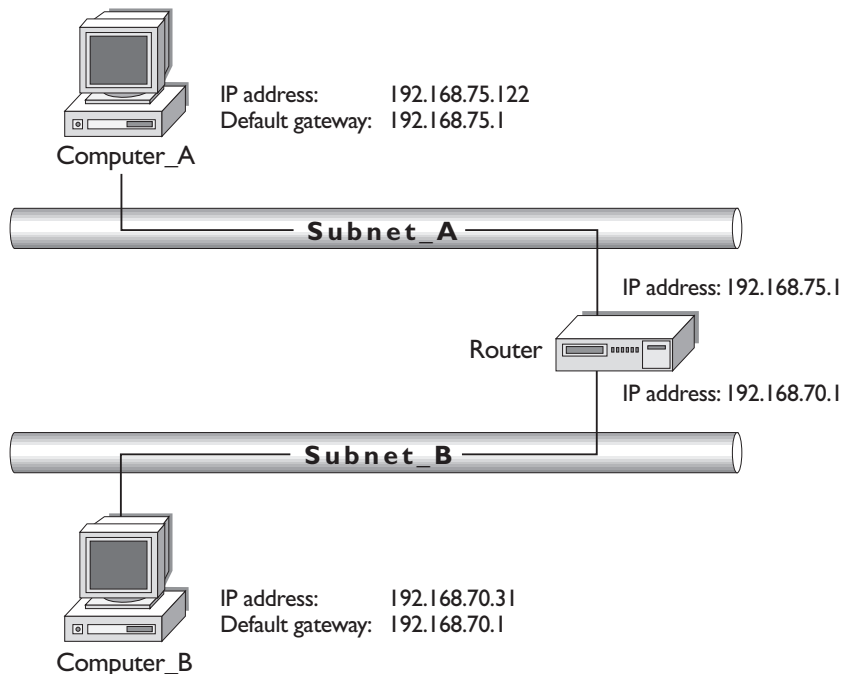Default gateway: 192.168.70.1

Computer_B

FIGURE 16-1   Default gateway addresses specify local router

Notice in Figure 16-1, 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.

ASSIGNING IP ADDRESSES

IP addresses must be configured on each computer when TCP/IP is installed. You can assign an IP address to a Windows NT computer in one of two ways: by configuring a computer to obtain an IP address automatically from a DHCP server, or by manually specifying a computer's IP address configuration.

IP addresses are assigned to Windows NT computers in the Microsoft TCP/IP Properties dialog box. Instructions for accessing and configuring this dialog box are covered later in this chapter.

Assigning IP Addresses 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.

This section discusses the advantages of using a DHCP server, the process of installing and configuring Microsoft DHCP Server, and configuring a client computer to obtain its IP address from a DHCP server.

Advantages of using a DHCP server

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 assuring 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 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 on every individual 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 Windows NT computer by using a DHCP server, you must first install and configure a DHCP server on your network.

Installing and configuring Microsoft DHCP Server

Microsoft includes a DHCP server product with Windows NT Server. *Microsoft DHCP Server* is an NT Server service that provides centralized management of IP address assignment. Microsoft DHCP Server can be installed on any Windows NT Server computer that has a manually configured IP address for each network adapter installed in it. The next sections explain how to install and configure Microsoft DHCP Server.

**TO INSTALL MICROSOFT DHCP SERVER ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:**

1. Select Start ≻ Settings ≻ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Services tab, click the Add command button.

5. In the Select Network Service dialog box, highlight Microsoft DHCP Server. Click OK.

6. A Windows NT Setup dialog box appears. Ensure the correct path to the Windows NT Server source files (normally the I386 folder on your Windows NT Server compact disc) is displayed in the text box. Edit the text box as necessary. Click the Continue command button.

7. Windows NT copies and installs the appropriate files. An informational dialog box appears, indicating all network adapters in this computer must have manually configured IP addresses. (At the end of the DHCP Server installation process, Windows NT prompts you to assign IP addresses manually to the computer's network adapters if you have not already done so.) Click OK.

8. The Network dialog box reappears. Click the Close command button. (Manually configure IP addresses only if prompted to do so.)

9. Windows NT performs various bindings operations.

10. The Network Settings Change dialog box is displayed, indicating you must shut down and restart the computer for the new settings to take effect. Click the Yes command button to restart the computer. You are now ready to configure Microsoft DHCP Server.

TO CONFIGURE MICROSOFT DHCP SERVER ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Log on as Administrator.

2. Select Start ≽ Programs ≽ Administrative Tools (Common) ≽ DHCP Manager.

3. The DHCP Manager dialog box appears. Select Server ≽ Add.

4. In the Add DHCP Server to Server List, type the IP address of the computer you installed Microsoft DHCP Server on. Click OK.

5. Highlight the IP address you entered in Step 4 in the DHCP Servers list box. Select Scope ≽ Create.

6. In the Create Scope dialog box, enter a starting and ending IP address (in the Start Address and End Address text boxes) to create a scope—a range of IP addresses also called an IP address pool. All IP addresses in the pool must have the same network ID. Enter a subnet mask in the Subnet Mask text box. This subnet mask will be used for all IP addresses assigned from this IP address pool. Figure 16-2 shows a configured Create Scope dialog box. Notice the IP Address Pool configurations. Click OK.
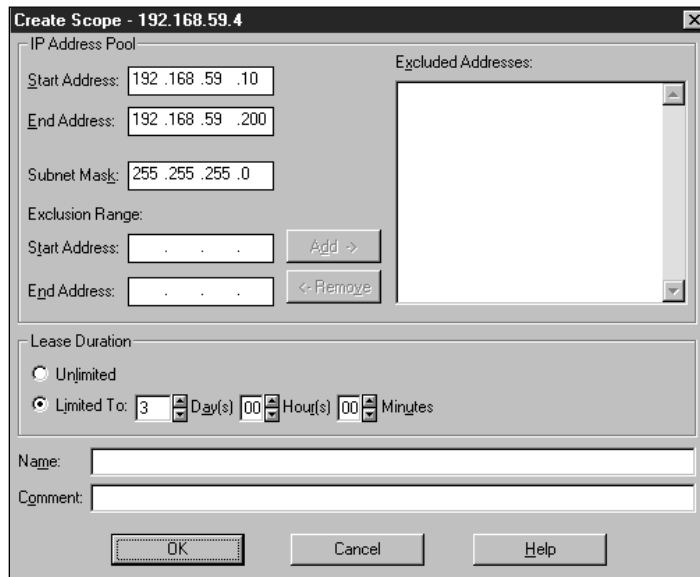
FIGURE 16-2   **Creating a DHCP scope**

7. The DHCP Manager dialog box appears, indicating the scope has been created, but not yet activated. Click the Yes command button. If a dialog box is displayed indicating no more information is available, click OK to clear it.

8. If you want the DHCP Server to assign a predefined default gateway address along with every IP address it assigns from this scope, select DHCP Options➢Scope in the DHCP Manager dialog box. Continue on to Steps 9, 10, and 11.

If you *don't* want the DHCP server to assign a default gateway address when it assigns IP addresses, skip to Step 12.

9. The DHCP Options: Scope dialog box appears. In the Unused Options list box, highlight 003 Router.
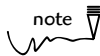
> note **You can configure several other options in the DHCP Options: Scope dialog box. A detailed discussion of these options is beyond the scope of this book and the objectives for the three Windows NT 4.0 Microsoft Certified Professional exams. For more information on the configurable options in this dialog box, see the various Help screens in DHCP Manager, the *Microsoft Windows NT Server Resource Kit for version 4.0* (Microsoft Press, 1996), and *TCP/IP MCSE Study Guide* (IDG Books Worldwide, 1997).**

Click the Add command button. Click the Value command button. Then click the Edit Array command button.

10. The IP Address Array Editor dialog box appears. Type in the IP address of the router you want assigned as the default gateway address in the New IP Address text box. Click the Add command button. Click OK.

11. In the DHCP Options: Scope dialog box, click OK.

12. Exit DHCP Manager.

## *Configuring a computer to obtain an IP address from a DHCP server*

Now that you've installed and configured a DHCP server, you're ready to configure a client computer to obtain its IP address from a DHCP server.

TO CONFIGURE A WINDOWS NT CLIENT COMPUTER TO OBTAIN AN IP ADDRESS FROM A DHCP SERVER, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Protocols tab.

4. On the Protocols tab, double-click the TCP/IP Protocol in the Network Protocols list box. (Or, if you prefer, highlight the TCP/IP Protocol in the Network Protocols list box and click the Properties command button.)

5. The Microsoft TCP/IP Properties dialog box appears. Ensure the radio button next to "Obtain an IP address from a DHCP server" is selected.

Figure 16-3 shows the Microsoft TCP/IP Properties dialog box.
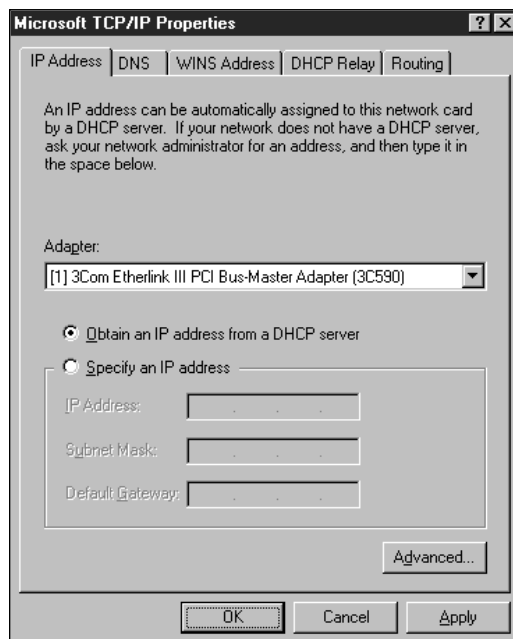
FIGURE 16-3 **Using a DHCP server to assign an IP address**

6. If the radio button next to "Obtain an IP address from a DHCP server" was *not* selected by default and you selected it, Windows NT displays a Microsoft TCP/IP warning dialog box, asking if you want to enable DHCP. Click the Yes command button to continue.

7. If only one network adapter is installed in the computer, click OK.

If additional network adapters are installed in the computer you are configuring to obtain IP addresses from a DHCP server, select each adapter (one at a time) from the Adapter drop-down list box, and select the radio button next to "Obtain an IP address from a DHCP server." When you have configured all network adapters, click OK.

8. The Network dialog box reappears. Click the Close command button.

9. A Network Settings Change dialog box is displayed, indicating you must shut down and restart the computer for the new settings to take effect. Click the Yes command button to restart the computer.
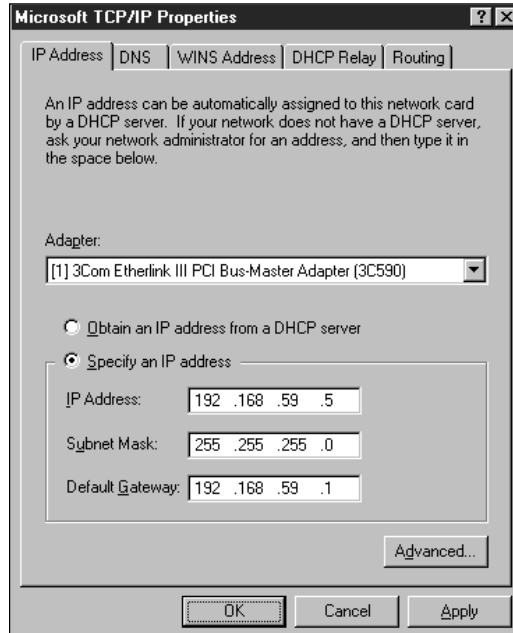
Assigning IP Addresses Manually

If you don't have a DHCP server, you must assign IP addresses manually. This method is both more time-consuming than using a DHCP server and more prone to error, because an IP address must be manually typed on each individual computer. The following section explains the steps involved in assigning an IP address manually.

TO ASSIGN AN IP ADDRESS MANUALLY TO A WINDOWS NT COMPUTER, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Protocols tab.

4. On the Protocols tab, double-click the TCP/IP Protocol in the Network Protocols list box. (Or, if you prefer, highlight the TCP/IP Protocol in the Network Protocols list box and click the Properties command button.)

5. The Microsoft TCP/IP Properties dialog box appears. Select the radio button next to "Specify an IP address." Then complete the following text boxes:

- **IP Address:** Enter the IP address you want to assign in the IP Address text box. (The IP address is a mandatory setting.) Press Tab.

- **Subnet Mask:** Either accept the default subnet mask displayed or type in the subnet mask you want to assign in the Subnet Mask text box. (The subnet mask is a mandatory setting.) Press Tab.

- **Default Gateway:** Type in a default gateway address in the Default Gateway text box. (The default gateway setting is optional.)

Figure 16-4 shows a manually configured IP address for a Windows NT Server computer.

FIGURE 16-4　**Assigning an IP address manually**

If only one network adapter is installed in the computer, click OK.

If additional network adapters are installed in the computer to which you want to manually assign IP addresses at this time, select each adapter (one at a time) from the Adapter drop-down list box and select the radio button next to "Specify an IP address." Type in an IP address, subnet mask, and default gateway (if desired) for each network adapter. When you have configured IP addresses for all network adapters, click OK.

6. The Network dialog box reappears. Click the Close command button.

7. A Network Settings Change dialog box is displayed, indicating you must shut down and restart the computer for the new settings to take effect. Click the Yes command button to restart the computer.

IP Routing

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 NT computers that have multiple network adapters (sometimes called *multihomed computers*) can function as IP routers. IP routers are occasionally referred to as *Internet routers*.

Two primary types of routing exist: static and dynamic. These topics are discussed in the next sections.

Static Routing

Static routing is basic, no-frills IP routing. No additional software is necessary to implement static routing in multihomed Windows NT computers.

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 computer. In a static routing environment, administrators must manually configure the routing table on each individual router. If the network layout changes, the network administrator must manually update the routing tables to reflect the changes.

Both Windows NT Workstation and Windows NT Server multihomed computers can be configured to function as static routers.

TO CONFIGURE A MULTIHOMED WINDOWS NT COMPUTER TO FUNCTION AS A STATIC ROUTER, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Protocols tab.

4. On the Protocols tab, double-click TCP/IP Protocol in the Network Protocols list box.

5. The Microsoft TCP/IP Properties dialog box appears. Click the Routing tab.

6. On the Routing tab, select the check box next to Enable IP Forwarding.
Figure 16-5 shows the Routing tab in the Microsoft TCP/IP Properties
dialog box. Notice the Enable IP Forwarding check box is selected. Click OK.
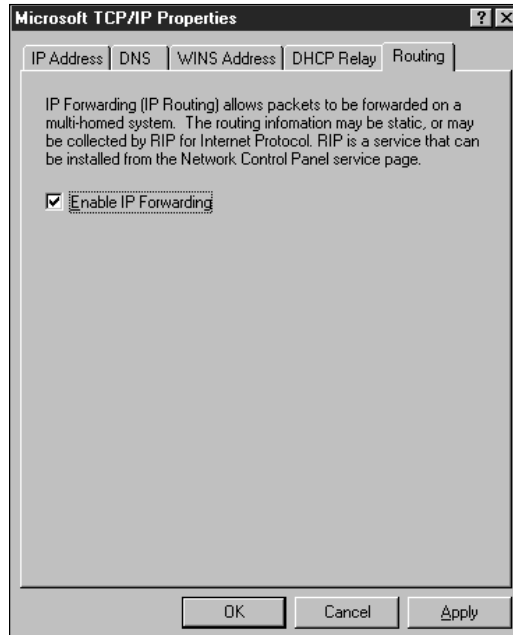
FIGURE 16-5 **Implementing static routing**

7. In the Network dialog box, click the Close command button.

8. A Network Settings Change dialog box appears. Click Yes to restart the
computer and implement the changes you made. After the computer
restarts, static routing will be enabled.

To configure the routing table manually on a Windows NT computer that is
configured as a static router, use the `Route.exe` command-line utility. For more
information on the `Route.exe` utility, type **route /help** at the command prompt.

Dynamic Routing

Dynamic routing is intelligent IP routing. Dynamic routing requires the use of
additional software in multihomed Windows NT Server computers.

A dynamic router is capable of automatically building and updating a routing
table. In a dynamic routing environment, administrators needn't configure the

routing table on each individual router manually. As changes are made to the network, dynamic routers automatically adjust their routing tables to reflect these changes.

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. By installing RIP for Internet Protocol, multihomed Windows NT Server computers can be configured to function as dynamic routers. *Routing Information Protocol* (RIP) is the software that allows Windows NT Server computers to share their routing tables dynamically. Dynamic routers that use RIP to share their routing tables are sometimes called *RIP routers.* The next section explains how to install RIP for Internet Protocol.

TO INSTALL RIP FOR INTERNET PROTOCOL ON A WINDOWS NT SERVER COMPUTER TO ENABLE DYNAMIC ROUTING, FOLLOW THESE STEPS:

1. Select Start ➤ Settings ➤ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Services tab, click the Add command button.

5. In the Select Network Service dialog box, highlight RIP for Internet Protocol.

Figure 16-6 shows the Select Network Service dialog box. Notice RIP for Internet Protocol is highlighted. Click OK.
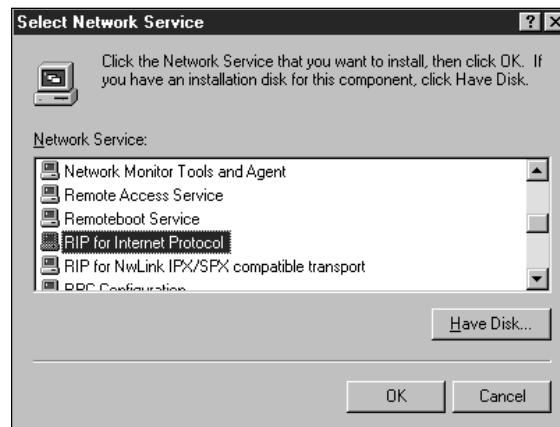
FIGURE 16-6   Installing RIP for Internet Protocol

6. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the I386 folder on your Windows NT Server compact disc) is listed in the text box. Edit the text box as necessary. Click the Continue command button.

7. The Network dialog box reappears.

   Windows NT, in the process of installing RIP for Internet Protocol, has automatically enabled IP forwarding.

   Click the Close command button.

8. Windows NT performs various bindings operations.

9. A Network Settings Change dialog box appears. Click Yes to restart the computer and implement the changes you made. After the computer restarts, dynamic (RIP) routing will be enabled.

The DHCP Relay Agent

The *DHCP Relay Agent* is a Windows NT Server service that forwards client DHCP configuration requests to a DHCP server on another network segment. The DHCP Relay Agent allows computers on one subnet to receive IP addresses from a DHCP server located on a different subnet.

The DHCP Relay Agent can be installed only on multihomed Windows NT Server computers. The DHCP Relay Agent is normally installed on Windows NT Server computers configured to function as static or dynamic routers. The next section explains how to install the DHCP Relay Agent.

TO INSTALL THE DHCP RELAY AGENT ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Services tab, click the Add command button.

5. In the Select Network Service dialog box, highlight DHCP Relay Agent. Click OK.

6. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the `I386` folder on your Windows NT Server compact disc) is listed in the text box. Edit the text box as necessary. Click the Continue command button.

7. The Network dialog box reappears. Click the Close command button.

8. Windows NT performs various bindings operations.

9. An Error-Unattended Setup dialog box appears, indicating you must configure the DHCP Relay Agent. Click the Yes command button.

10. The Microsoft TCP/IP Properties dialog box appears. Click the DHCP Relay tab.

11. The DHCP Relay tab appears, as shown in Figure 16-7. Notice no servers are shown in the DHCP Servers list box. Click the Add command button.
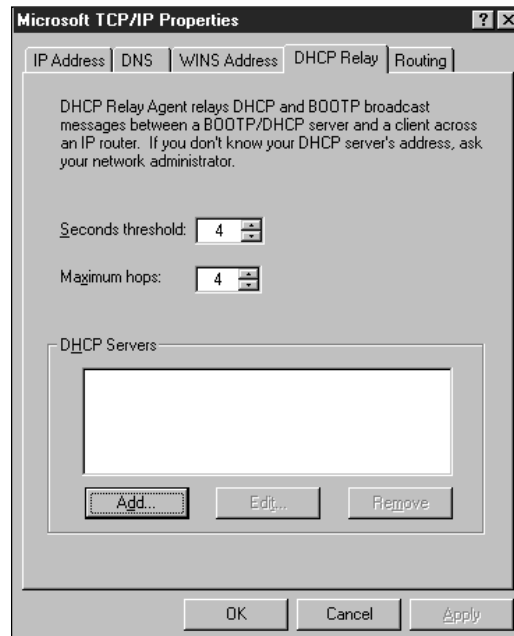
FIGURE 16-7   Configuring the DHCP Relay Agent

12. The DHCP Relay Agent dialog box appears, as shown in Figure 16-8.

FIGURE 16-8   Adding a server to the DHCP Servers list

Type in the IP address of the DHCP server to which you want the DHCP Relay Agent to forward requests. Click the Add command button.

13. The Microsoft TCP/IP Properties dialog box reappears, as shown in Figure 16-9. Notice an IP address is now listed in the DHCP Servers list box. Click OK.
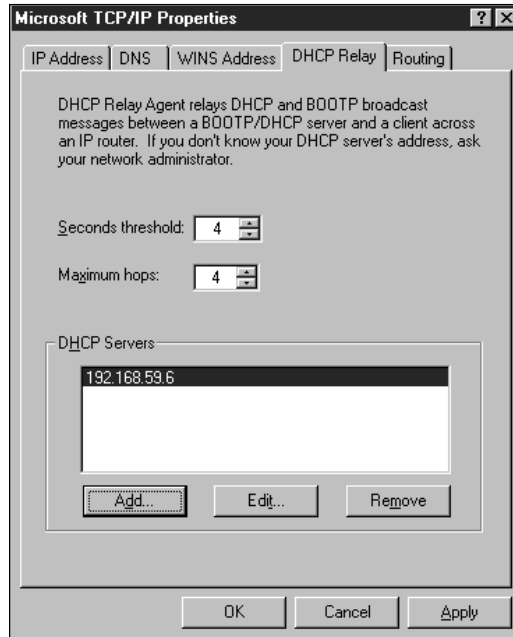
FIGURE 16-9 **DHCP Relay Agent successfully configured**

14. Windows NT performs various bindings operations.

15. A Network Settings Change dialog box appears. Click Yes to restart the computer and implement the changes you made.

WINDOWS INTERNET NAME SERVICE (WINS)

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

A *NetBIOS name* is the computer name assigned during the installation of Windows NT. A NetBIOS name can be up to 15 characters in length. 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.

You can perform NetBIOS name resolution 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 client computers to use it.

If you use an `LMHOSTS` file (a text file that contains a list of NetBIOS names and their associated IP addresses) 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.

Installing a WINS server and configuring client computers to use it is the preferred method of handling NetBIOS name resolution on Windows NT 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.

WINS can only be installed on Windows NT Server computers. On small networks, WINS is often installed on the primary domain controller (PDC). On larger networks, WINS is installed on multiple Windows NT Server computers.

The following section discusses how to install a WINS server and how to configure Windows NT computers to use the WINS server for NetBIOS name resolution.

Installing and Configuring WINS

Installing and configuring WINS is a two-step process: You must first install WINS on a Windows NT Server computer, and then you must configure each client computer on the network to use the WINS server for NetBIOS name resolution. The next two sections explain how to accomplish these tasks.

TO INSTALL WINS ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Select Start ➤ Settings ➤ Control Panel.
2. In the Control Panel dialog box, double-click Network.
3. In the Network dialog box, click the Services tab.
4. On the Services tab, click the Add command button.
5. The Select Network Service dialog box appears. Scroll down and highlight Windows Internet Name Service. Click OK.
6. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the `I386` folder on your Windows NT Server compact disc) is listed in the text box. Edit the text box as necessary. Click the Continue command button.
7. Windows NT copies and installs WINS. The Network dialog box reappears. Click the Close command button.
8. Windows NT performs various bindings operations.
9. A Network Settings Change warning dialog box appears, indicating you need to restart the computer now for the new settings to take effect. Click the Yes command button.

TO CONFIGURE A WINDOWS NT CLIENT COMPUTER TO USE A WINS SERVER FOR NETBIOS NAME RESOLUTION, FOLLOW THESE STEPS:

1. Select Start ➤ Settings ➤ Control Panel.
2. In the Control Panel dialog box, double-click Network.
3. In the Network dialog box, click the Protocols tab.
4. On the Protocols tab, double-click the TCP/IP Protocol in the Network Protocols list box.
5. The Microsoft TCP/IP Properties dialog box appears. Click the WINS Address tab.
6. The WINS Address tab appears, as shown in Figure 16-10. Notice you can enter IP addresses for a primary and a secondary WINS server.

    Type in the IP address for the primary WINS server. If you have multiple WINS servers on your network, you can type in the IP address for a secondary WINS server in case the primary WINS server becomes unavailable. Click OK.
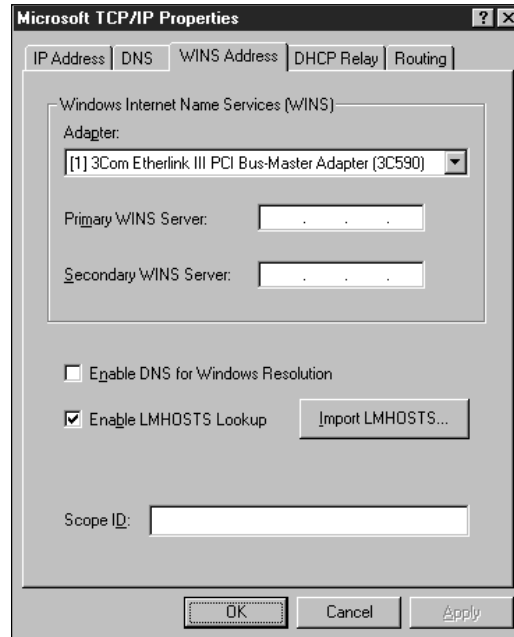
FIGURE 16-10 **Configuring primary and secondary WINS server addresses**

7. The Network dialog box reappears. Click the Close command button.

8. A Network Settings Change warning dialog box appears, indicating you need to restart the computer now for the new settings to take effect. Click the Yes command button.

If you don't want to configure WINS server addresses on each individual computer manually, you can use DHCP Manager to configure a DHCP server to supply the IP address of a primary and a secondary WINS server automatically to computers that obtain their IP address configurations from a DHCP server.

MICROSOFT DNS SERVER

Microsoft DNS Server is a Windows NT Server service that provides host name resolution services to client computers. *DNS* stands for *Domain Name System*. A

Windows NT Server computer that has Microsoft DNS Server installed on it is referred to as a *DNS server.*

A Windows NT computer's host name, by default, is the same as the computer's NetBIOS name (which is the computer name assigned during the installation of NT). Host names are used to access other computers on the network by using TCP/IP-based utilities, such as `FTP.exe` and Internet Explorer.

When a user attempts to access a World Wide Web server (such as `www.microsoft.com`) by using Internet Explorer, the user's computer must first obtain the IP address associated with the Fully Qualified Domain Name of the World Wide Web (WWW) server (in this case, `www.microsoft.com`). This process is called *host name resolution.* Once the user's computer has resolved the Fully Qualified Domain Name of the WWW server to its IP address, it can then establish TCP/IP network communications with the WWW server.

On the Internet, host names are stored in various domains and subdomains that form a hierarchical tree structure called the *Domain Name System* (DNS). (Please note that Internet domains are *not* the same as Windows NT Server domains.) The root of the DNS structure contains several domains with which you may be familiar. These domains are shown in Table 16-1.

TABLE 16-1 DNS ROOT DOMAINS	
DOMAIN	**DESCRIPTION**
com	Commercial organizations, such as `pepsi.com`
gov	Government organizations, such as `whitehouse.gov`
mil	Military organizations, such as `army.mil`
edu	Educational organizations, such as `stanford.edu`
net	Internet Service Providers, such as `nsf.net`
org	Nonprofit organizations, such as `metmuseum.org`

Many commercial companies store their host names in a subdomain of the `com` domain. Examples of subdomains within the `com` domain include `microsoft.com`, `chevrolet.com`, and so forth. Each subdomain is called a *zone.*

When a DNS server is initially installed, you must create a zone in which the DNS server will maintain its host names. A DNS server can have multiple zones. A DNS server stores all zone information, including host names and their associated IP addresses, in a database called a DNS database.

A DNS database is not dynamically created—the network administrator must manually enter host names and their associated IP addresses for each computer on the network.

An alternative to entering every host name and associated IP address manually into a DNS database on a Windows NT Server computer is to configure Microsoft DNS Server to access a WINS server to resolve host names. Because host names on Windows NT networks are usually the same as NetBIOS names, and because the WINS server dynamically updates its NetBIOS name to IP address resolution tables, configuring Microsoft DNS Server to use a WINS server is an efficient way for a network administrator to manage host name resolution without having to enter every host name and associated IP address manually.

The following section covers the steps involved in installing Microsoft DNS Server on a Windows NT Server computer, configuring a zone on Microsoft DNS Server, configuring a Microsoft DNS Server to use WINS Lookup for host name resolution, and configuring client computers to use a DNS server for host name resolution.

Installing and Configuring Microsoft DNS Server

Installing and configuring Microsoft DNS Server is a three-step process:

- First, you must install Microsoft DNS Server on a Windows NT Server computer.

- Second, you configure a zone on the Microsoft DNS Server. (Optionally, on networks that use DHCP and WINS, you can also configure Microsoft DNS Server to use WINS Lookup for host name resolution.)

- Third, you configure each client computer on the network to use a DNS server for host name resolution.

  Each of these installation and configuration tasks is described in the following sections.

TO INSTALL MICROSOFT DNS SERVER ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Services tab, click the Add command button.

5. In the Select Network Service dialog box, highlight Microsoft DNS Server. Click OK.

6. A Windows NT Setup dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the I386 folder on your Windows NT Server compact disc) is listed in the text box. Edit the text box as necessary. Click the Continue command button.

7. Windows NT copies and installs Microsoft DNS Server. The Network dialog box reappears. Click the Close command button.

8 Windows NT performs various bindings operations.

9. A Network Settings Change warning dialog box appears, asking if you want to restart your computer now for the new settings to take effect. Click the Yes command button.

TO CONFIGURE A ZONE ON A MICROSOFT DNS SERVER, FOLLOW THESE STEPS:

1. From the desktop, select Start ➢ Programs ➢ Administrative Tools (Common) ➢ DNS Manager.

2. In the Domain Name Service Manager dialog box, select DNS ➢ New Server.

3. The Add DNS Server dialog box appears. Type the IP address of the Windows NT Server computer you installed Microsoft DNS Server on in the DNS Server text box. Click OK.

4. A server appears (indicated by its IP address) in the Server List on the left side of the Domain Name Service Manager dialog box, as shown in Figure 16-11. Notice the Server Statistics.

Right-click the server's IP address. Select Refresh from the menu that appears. Right-click again on the server's IP address. Select New Zone from the menu that appears.

5. The Creating new zone for *ip_address* dialog box appears. Select the radio button next to Primary. Click the Next command button.
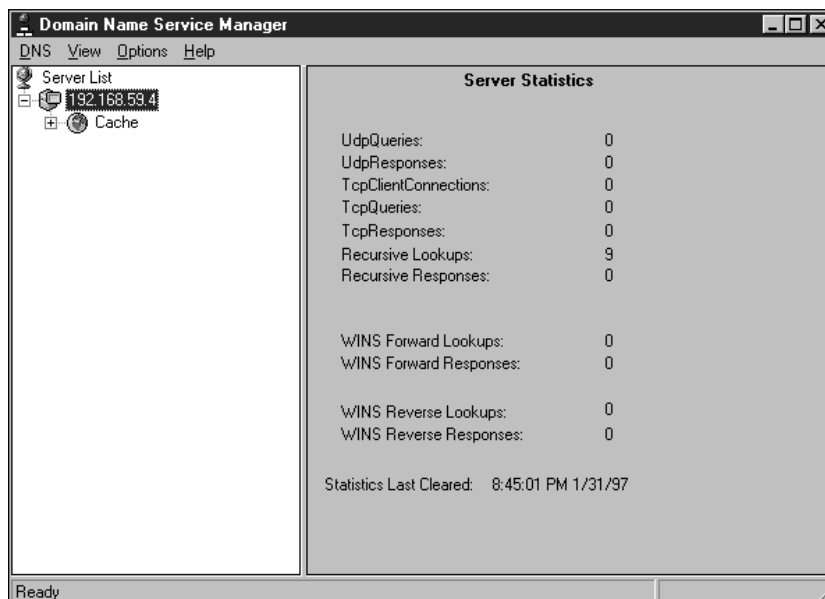
FIGURE 16-11   DNS server added to Server List

6. Type the Internet domain name this DNS server will manage in the Zone Name text box—for example, **lab.com**. Type a filename for the file the DNS server will use to store host name and IP address information for the domain in the Zone File text box—for example, **lab.com.dns**. (Don't include the final period.)

Figure 16-12 shows a configured "Creating new zone for 192.168.59.4" dialog box. Notice the zone information that has been entered. Click the Next command button.
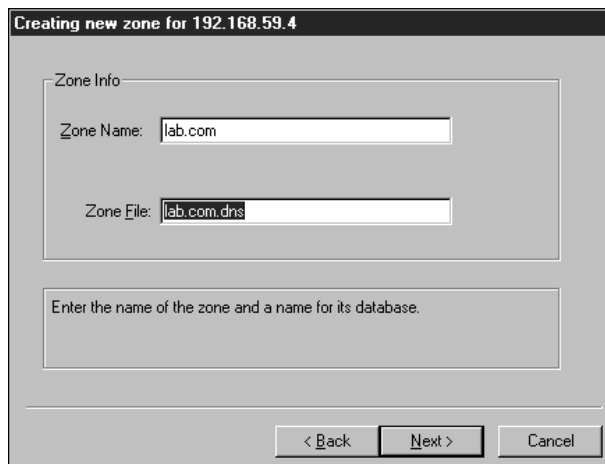
FIGURE 16-12   Creating a DNS zone

7. Click the Finish command button in the "Creating new zone for
ip_address" dialog box. The new zone appears in the Domain Name
Service Manager dialog box under the Server List for the Windows NT
Server computer, as shown in Figure 16-13. Notice the zone information
displayed in the dialog box.
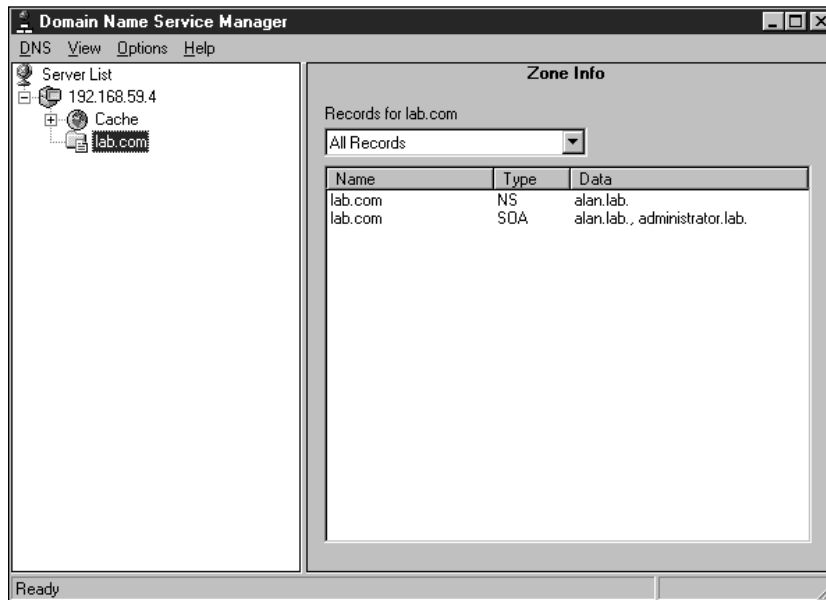
FIGURE 16-13   DNS zone created

8. This completes the creation of a zone.

If you are *not* using WINS, or if you have computers on your network that
don't use WINS, you can manually configure name resolution for those
computers now. The following steps explain how to enter computer (host)
names and their associated IP addresses manually into the DNS server's
database.

9. Right-click the new zone. Select New Host from the menu that appears.

10. The New Host dialog box appears, as shown in Figure 16-14. Note that you
must enter a host name and a host IP address in this dialog box.
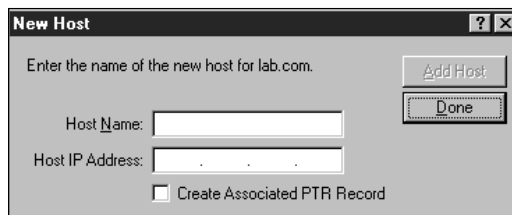
**FIGURE 16-14   Adding a
computer
to the DNS
server's
database**

Type in a host name (computer name) and its associated IP address in the Host Name and Host IP Address text boxes. Click the Add Host command button.

11. Repeat Step 10 for every additional computer you want to add to the DNS server's database. When you are finished, click the Done command button.

12. Exit DNS Manager.

TO CONFIGURE MICROSOFT DNS SERVER TO USE WINS LOOKUP FOR HOST NAME RESOLUTION, FOLLOW THESE STEPS:

1. From the desktop, select Start ➢ Programs ➢ Administrative Tools (Common) ➢ DNS Manager.

2. In the Domain Name Service Manager dialog box, double-click the IP address of the Microsoft DNS Server you want to configure.

3. Right-click the zone for which you want to configure WINS Lookup, and then select Properties from the menu that appears.

4. The "Zone Properties–*zone_name*" dialog box appears. Click the WINS Lookup tab.

5. On the WINS Lookup tab, select the check box next to Use WINS Resolution. In the uppermost WINS Servers text box, type the IP address of the WINS server you want to use for WINS Lookup, and click the Add command button.

A configured WINS Lookup tab is shown in Figure 16-15. Notice the check box next to Use WINS Resolution is selected and an IP address of a WINS server is listed. Click OK.

6. The Microsoft DNS Server is now configured to use WINS for host name resolution. Exit DNS Manager.

TO CONFIGURE A WINDOWS NT CLIENT COMPUTER TO USE A DNS SERVER FOR HOST NAME RESOLUTION, FOLLOW THESE STEPS:

1. Select Start ➢ Settings ➢ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Protocols tab.

4. On the Protocols tab, double-click the TCP/IP Protocol in the Network Protocols list box.

5. The Microsoft TCP/IP Properties dialog box appears. Click the DNS tab.

6. The DNS tab appears, as shown in Figure 16-16. Notice, by default, the computer's NetBIOS name is listed in the Host Name text box. Click the Add command button.
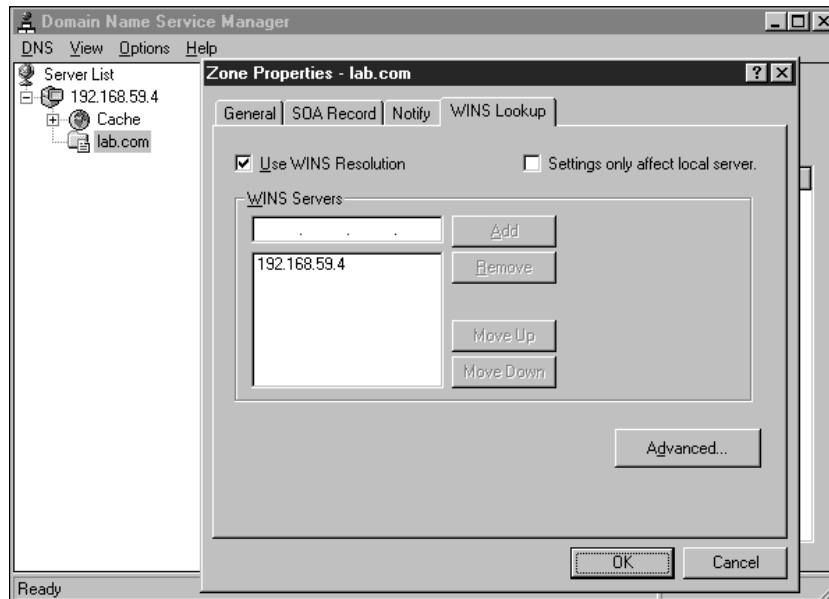
FIGURE 16-15   Configuring WINS Lookup
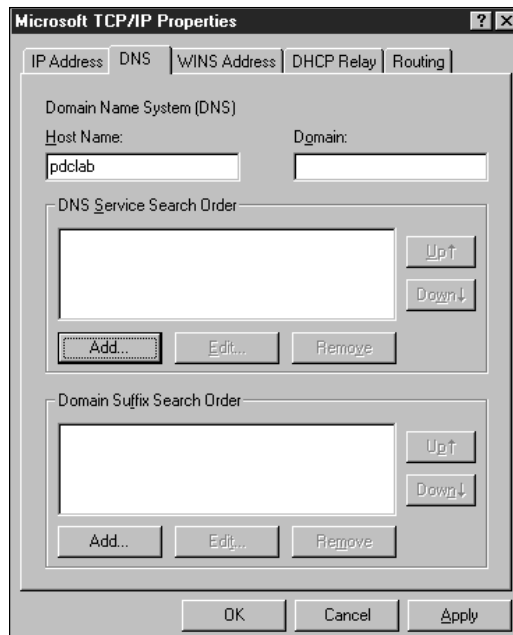
FIGURE 16-16   Configuring a client computer to use a Microsoft DNS Server for host name resolution

7. The TCP/IP DNS Server dialog box appears, as shown in Figure 16-17.

TCP/IP DNS Server   [? | X]

DNS Server: Add

[. . .]   Cancel
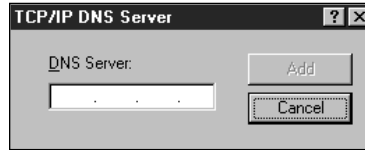
FIGURE 16-17   Adding a DNS server address

Type the IP address of the Microsoft DNS Server. Click the Add command button.

8. The Microsoft TCP/IP Properties dialog box reappears. Click OK.

9. The Network dialog box reappears. Click the Close command button.

10. A Network Settings Change warning dialog box appears, indicating you need to restart the computer now for the new settings to take effect. Click the Yes command button.

If you don't want to configure DNS server addresses manually on each individual client computer, you can use DHCP Manager to configure a DHCP server to automatically supply the IP address of a DNS server to computers that obtain their IP address configurations from the DHCP server.

PUBLISHING ON THE INTERNET

Publishing World Wide Web pages on the Internet is becoming more popular every day. Many companies and organizations, from small, home-based businesses to multimillion-dollar concerns, use the Web to advertise their products and services. Web pages can be made available to anyone who has an Internet connection and a Web browser, such as Internet Explorer or Netscape Navigator.

Microsoft has two primary tools for publishing on the Internet: Internet Information Server (for Windows NT Server computers) and Peer Web Services (for Windows NT Workstation computers). The following sections discuss these products in detail.

Microsoft Internet Information Server

Microsoft Internet Information Server (IIS) is a Windows NT Server service that provides World Wide Web (WWW), File Transfer Protocol (FTP), and Gopher publishing services.

Internet Information Server uses *Hypertext Transfer Protocol* (HTTP) to publish WWW documents on the Internet. FTP enables users to transfer files between computers on the Internet. The FTP service included with IIS replaces the FTP service included in previous versions of Windows NT Server. Gopher is a complicated publishing service that is not used extensively anymore and is not included in the objectives for the Windows NT 4.0 Microsoft Certified Professional exams.

Internet Information Server (IIS) requires the use of TCP/IP. You *must* have TCP/IP installed in your Windows NT Server computer to install and use IIS. No additional hardware is required to install and use IIS on an internal intranet.

The following sections discuss the basics of IIS, including: connecting your Internet Information Server to the Internet, installing IIS, using Internet Service Manager, configuring the WWW service, and configuring a virtual server.

Connecting your Internet Information Server to the Internet

If you want to connect your Internet Information Server to the Internet instead of just using it on your company's internal network (intranet), additional hardware is required.

Different hardware is required for different types of Internet connections. When determining the type of Internet connection to use, you should consider how many people will access your Internet Information Server, the frequency and duration of those accesses, and the size of documents and files being accessed.

Table 16-2 shows some of the Internet connection types, their speeds, and the additional hardware each requires.

You may want to consult with your Internet service provider (ISP) when determining the type of connection you need and when configuring the hardware and software used to establish your Internet connection.

TABLE 16-2 INTERNET CONNECTION TYPES		
CONNECTION TYPE	*SPEED*	*ADDITIONAL HARDWARE REQUIRED*
Modem	28.8–56Kbps	A modem and standard telephone line
ISDN	64–128Kbps	An ISDN adapter card with either an internal or external network terminating unit (NT1), and an ISDN line
Digital Leased Line	56Kbps–44.7Mbps	A router, a DSU/CSU, a network adapter, and a digital leased line—56Kbps, fractional T1, T1, or T3

Installing Microsoft Internet Information Server

Before installing Microsoft Internet Information Server (IIS), you should install Windows NT Server and TCP/IP. Additionally, you may want to install and configure the computer's Internet connection, including the additional hardware required, before you install IIS.

You can install IIS either during the Windows NT Server installation process or at a later time. The following steps explain how to install IIS on a computer after Windows NT Server and TCP/IP have been installed.

TO INSTALL MICROSOFT INTERNET INFORMATION SERVER (IIS) ON A WINDOWS NT SERVER COMPUTER, FOLLOW THESE STEPS:

1. Select Start ≽ Settings ≽ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Services tab, click the Add command button.

5. The Select Network Service dialog box appears. Highlight Microsoft Internet Information Server.

Figure 16-18 shows the Select Network Service dialog box. Notice Microsoft Internet Information Server is highlighted. Click OK.

6. An Internet Information Server Installation dialog box appears. Ensure the correct path to your Windows NT Server source files (usually the I386 folder on your Windows NT Server compact disc) is listed in the text box. Edit the text box as necessary. Click OK.
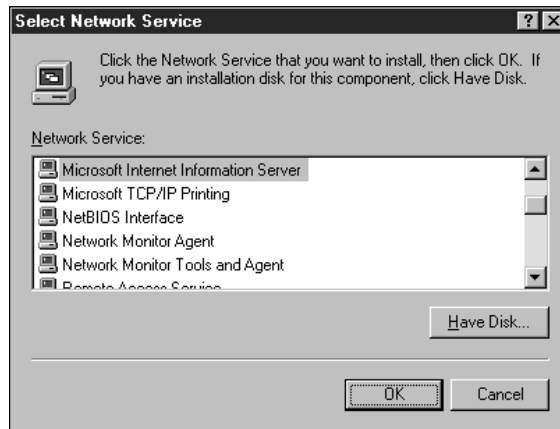
FIGURE 16-18   **Installing Microsoft Internet Information Server**

7. A Microsoft Internet Information Server 2.0 Setup dialog box appears. Click OK.

8. The Microsoft Internet Information Server 2.0 Setup dialog box appears, as shown in Figure 16-19. Notice the options that can be installed with IIS.
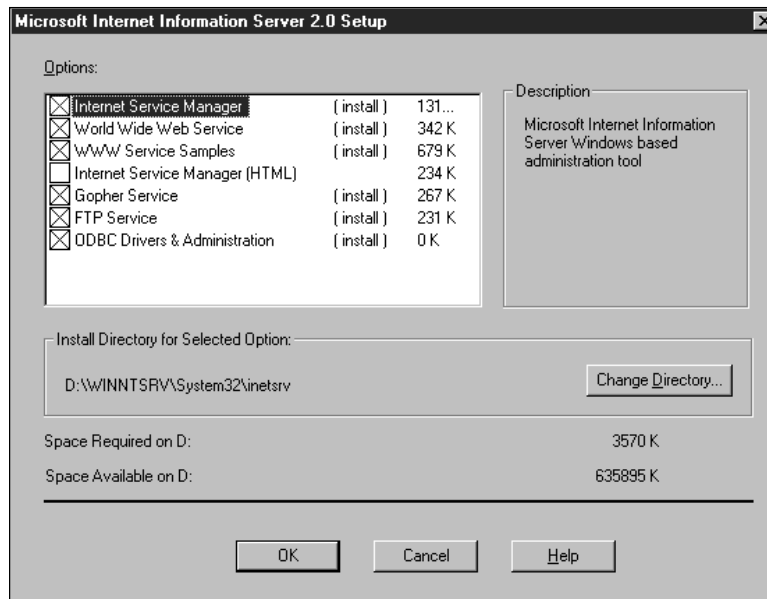
FIGURE 16-19   **Selecting IIS options**

Select all the options you want installed with IIS. Deselect any undesired options. Click OK.

9. If a Microsoft Internet Information Server 2.0 Setup dialog box appears prompting you to confirm the creation of the `inetsrv` folder, click the Yes command button.

10. The Publishing Directories dialog box appears, as shown in Figure 16-20. Note the default publishing directories.
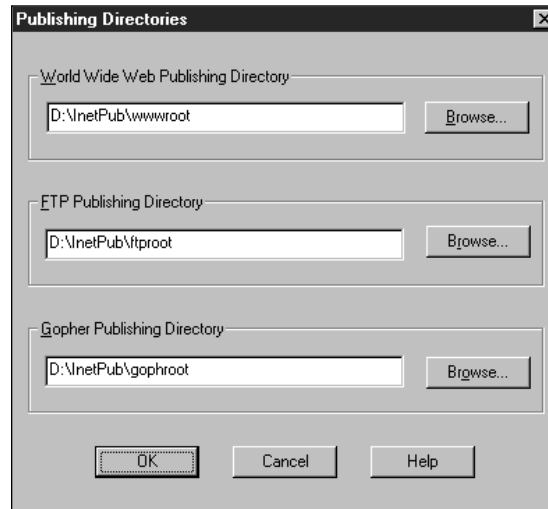
FIGURE 16-20   Configuring publishing directories for the WWW, FTP, and Gopher services

Configure the publishing directories as desired, or accept the default publishing directories presented. Click OK.

11. If a Microsoft Internet Information Server 2.0 Setup dialog box appears prompting you to create the publishing directories, click the Yes command button.

12. Windows NT installs Microsoft Internet Information Server and the options you selected. (This process takes a few minutes.)

13. If you installed the Gopher service and you have not yet assigned an Internet domain name to the computer, a dialog box appears, indicating you should assign an Internet domain name to your computer. Click OK.

14. If you installed ODBC drivers and administration, a dialog box may appear indicating you need to close Control Panel to continue the ODBC installation. Click OK to close Control Panel.

15. The Install Drivers dialog box appears. Highlight the ODBC drivers you want to install, and click OK.

16. The Microsoft Internet Information Server 2.0 Setup dialog box appears, indicating IIS was successfully installed. Click OK.

17. The Network dialog box reappears. Click the Close command button.

Microsoft Internet Information Server is now installed, and all its services have been started. You needn't restart your computer at this time.

Using Internet Service Manager

Once you have installed Microsoft Internet Information Server, you can use Internet Service Manager to manage IIS.

Internet Service Manager can be used to configure the IIS services, to configure IIS security, and to start and stop the individual IIS services.

Internet Service Manager can be accessed by selecting Start ➢ Programs ➢ Microsoft Internet Server (Common) ➢ Internet Service Manager.

The next section discusses configuring the WWW service.
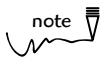
note **Because configuring the FTP and Gopher services is substantially similar to configuring the WWW service, detailed configuration instructions for the FTP and Gopher services are not included. For more information on the FTP and Gopher services, see the Help screens in Microsoft Internet Service Manager.**

TO CONFIGURE THE WWW SERVICE, FOLLOW THESE STEPS:

1. Start Internet Service Manager by selecting Start ➢ Programs ➢ Microsoft Internet Server (Common) ➢ Internet Service Manager. Figure 16-21 shows the Microsoft Internet Service Manager dialog box. Notice the WWW service is listed in the Service column and is running.

2. To access the Properties dialog box for the WWW service, highlight the computer on the same line as the WWW service, and select Properties ➢ Service Properties. The WWW Service Properties dialog box appears, as shown in Figure 16-22. Note the configurable options on the Service tab.
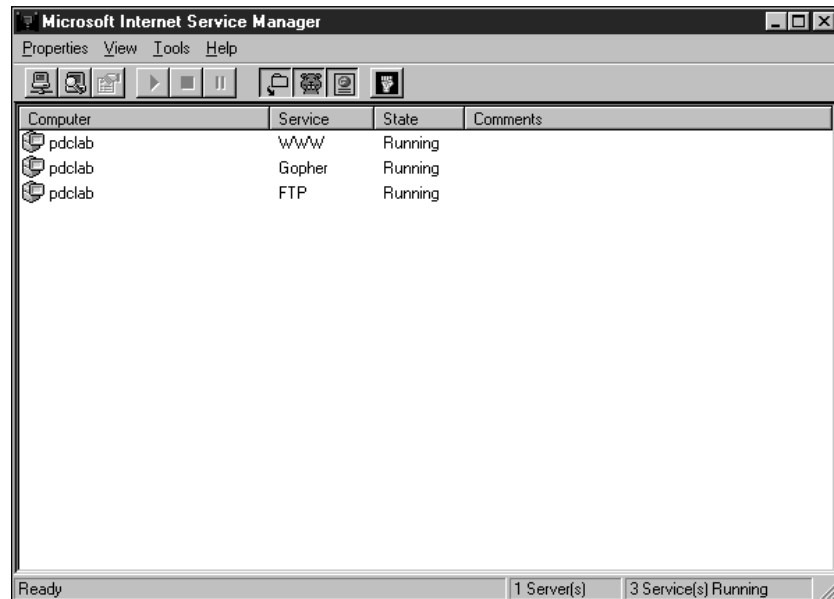
FIGURE 16-21   Using Internet Service Manager to configure IIS services
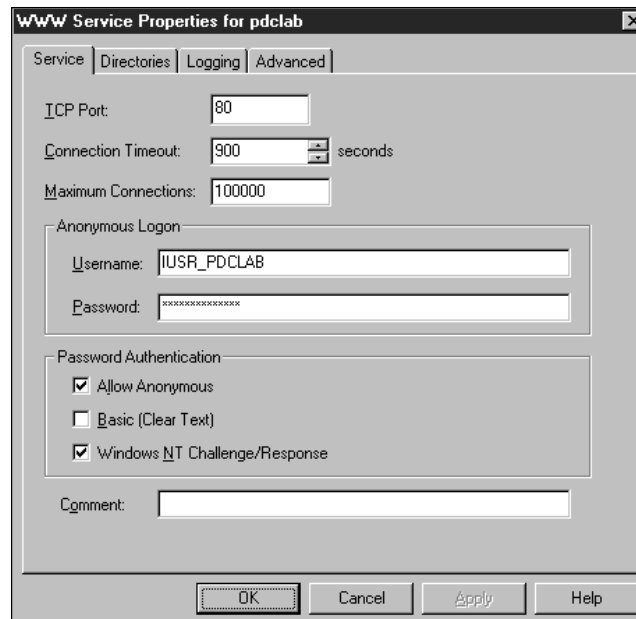
**FIGURE 16-22   Configuration options on the WWW Service
Properties Service tab**

3. Configure options for the WWW service on the Service tab. Many of the options on this tab are security features. The most commonly configured options are:

   - **Anonymous Logon:** This section should be configured if the check box next to Allow Anonymous is selected in the Password Authentication section. When a user name and password are entered in the Anonymous Logon section, the user rights and permissions assigned to this user name are applied to all anonymous users of the WWW service. In this way, IIS security is integrated with Windows NT security. The default user name listed is `IUSR_Computer_name`.

   - **Password Authentication:** The three options in this section are Allow Anonymous, Basic (Clear Text), and Windows NT Challenge/Response.

     - **Allow Anonymous:** If you select the check box next to Allow Anonymous, anyone with Internet access can access the WWW service on your server anonymously. These users will not be required to supply a user name and password. If you clear the check box next to Allow Anonymous, all users will be required to supply a user name and a password to access the WWW service. The Allow Anonymous option is selected by default.

     - **Basic (Clear Text):** If you select the check box next to Basic (Clear Text), user names and passwords can be sent over the Internet in an unencrypted format. Selecting this option is not normally desirable because it compromises the security of your server. If this check box is cleared, unencrypted user names and passwords will not be accepted by the WWW service. The Basic (Clear Text) option is not selected by default.

     - **Windows NT Challenge/Response:** If you select the check box next to Windows NT Challenge/Response, user names and passwords can be sent over the Internet in an encrypted format. If this check box is cleared, encrypted user names and passwords will not be accepted by the WWW service. This security feature is selected by default and should be used in high-security environments.

4. Configure advanced options for the WWW service as desired on the Advanced tab in the WWW Service Properties dialog box, as shown in Figure 16-23. Note: most of the options on the Advanced tab are used to manage access security for the WWW service.
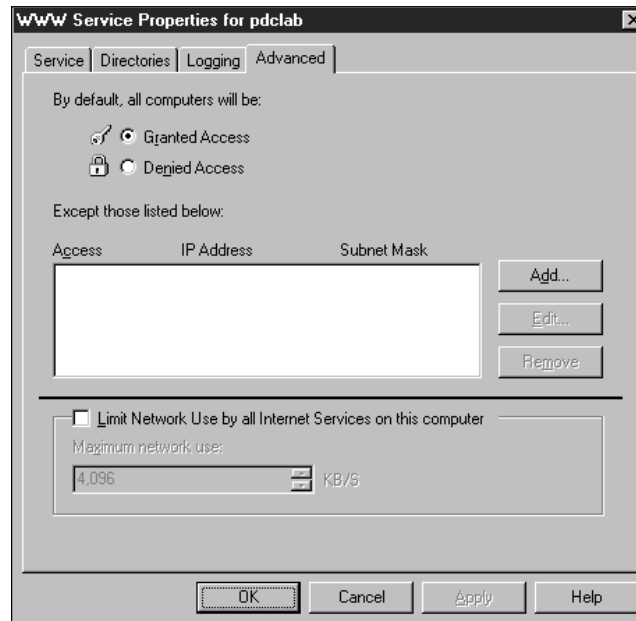
FIGURE 16-23   **Configuration options on the WWW Service Properties Advanced tab**

The Advanced tab is primarily used to control access to the WWW service by the IP address of the computer attempting to access the service. The most commonly configured options on the Advanced tab are:

o **Granted Access:** If you select the radio button next to this option, all computers on the Internet will be allowed to access the WWW service *except* those explicitly listed, by IP address, in the following list box. To add computers to the list box, click the Add command button.

o **Denied Access:** If you select the radio button next to this option, all computers on the Internet will be denied access to the WWW service *except* those explicitly listed, by IP address, in the following list box. To add computers to the list box, click the Add command button.

This completes the configuration of the WWW service

Configuring a virtual server   A *virtual server* is a pseudo WWW server with its own unique domain name and IP address. To the Internet user accessing the virtual server, a virtual server appears to be a separate server; but in reality, a virtual server

is *not* a separate server, but more like an extra shared folder on an Internet Information Server accessed by specifying a different domain name and IP address. A single Internet Information Server can be configured to accommodate multiple virtual servers. Each virtual server is assigned a separate publishing directory.

For example, an Internet service provider could use one Internet Information Server to host virtual servers for several customers. Each customer could have its own domain name, such as `www.company_a.com,` `www.company_b.com,` and `www.company_c.com,` and so forth. To Internet users accessing these companies' WWW services, each domain name appears to be on a separate server.

Configuring a virtual server consists of two parts: first, you must configure an additional IP address for your network adapter; second, you use Internet Service Manager to configure the virtual server. The following sections describe how to accomplish these tasks.

TO CONFIGURE AN ADDITIONAL IP ADDRESS FOR A NETWORK ADAPTER, FOLLOW THESE STEPS:

1. Select Start ≫ Settings ≫ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Protocols tab.

4. On the Protocols tab, double-click TCP/IP Protocol in the Network Protocols list box.

5. The Microsoft TCP/IP Properties dialog box appears. Click the Advanced command button.

6. The Advanced IP Addressing dialog box appears. In the Adapter drop-down list box, select the network adapter to which you want to assign an additional IP address. Click the Add command button in the IP Addresses section.

7. The TCP/IP Address dialog box appears. Type in the additional IP address and subnet mask you want to assign to the network adapter. Click the Add command button.

8. The Advanced IP Addressing dialog box reappears.

Figure 16-24 shows the Advanced IP Addressing dialog box with two IP addresses configured for a single network adapter. Click OK.

9. In the Microsoft TCP/IP Properties dialog box, click OK.

10. In the Network dialog box, click the Close command button.
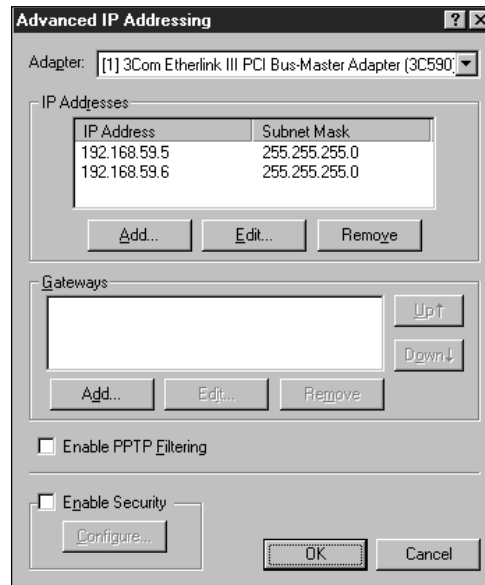
FIGURE 16-24 **Multiple IP addresses assigned to a single network adapter**

11. A Network Settings Change warning dialog box appears, asking if you want to restart your computer now for the new settings to take effect. Click the Yes command button.

TO USE INTERNET SERVICE MANAGER TO CONFIGURE THE VIRTUAL SERVER, FOLLOW THESE STEPS:

1. Select Start ➢ Programs ➢ Microsoft Internet Server (Common) ➢ Internet Service Manager.

2. In the Microsoft Internet Service Manager dialog box, highlight the computer on the same line as the WWW service, and select Properties ➢ Service Properties.

3. The WWW Service Properties dialog box appears. Click the Directories tab.

4. The Directories tab appears, as shown in Figure 16-25. Note the check box next to Directory Browsing Allowed. When selected, this option permits users to browse all files and folders published by the WWW service. For security reasons, this option is not normally selected. Click the Add command button.
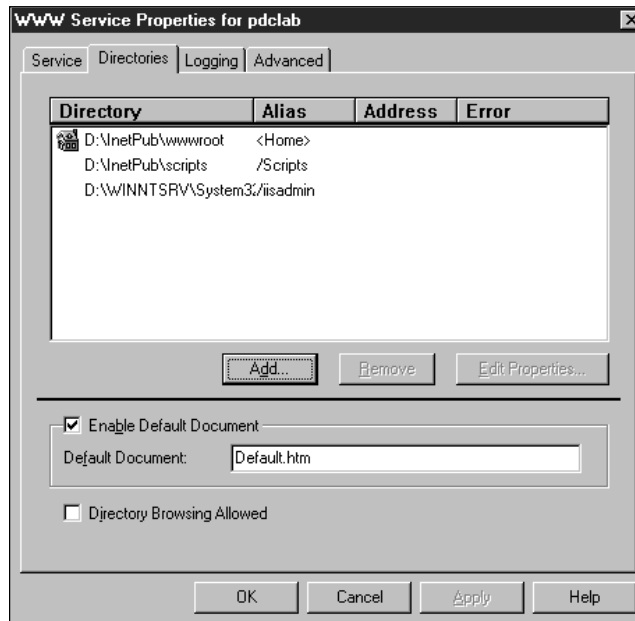
FIGURE 16-25   **Configuration options on the WWW Service Properties Directories tab**

5. In the Directory Properties dialog box, select the radio button next to Home Directory. In the Directory text box, type the full path to the home directory that will be used by the virtual server, for example: `c:\inetpub\wwwroot_2`. (This directory need *not* be an existing directory—entering a new directory in this text box will cause NT to create it when you click OK.) Then select the check box next to Virtual Server. Type in the additional IP address you assigned to your network adapter in the Virtual Server IP Address text box. Click OK.

Figure 16-26 shows the Directory Properties dialog box configured to implement a virtual server.

6. The WWW Service Properties dialog box reappears. The virtual server's home directory and IP address now appear in the list box. Click OK.

7. Exit Microsoft Internet Service Manager.
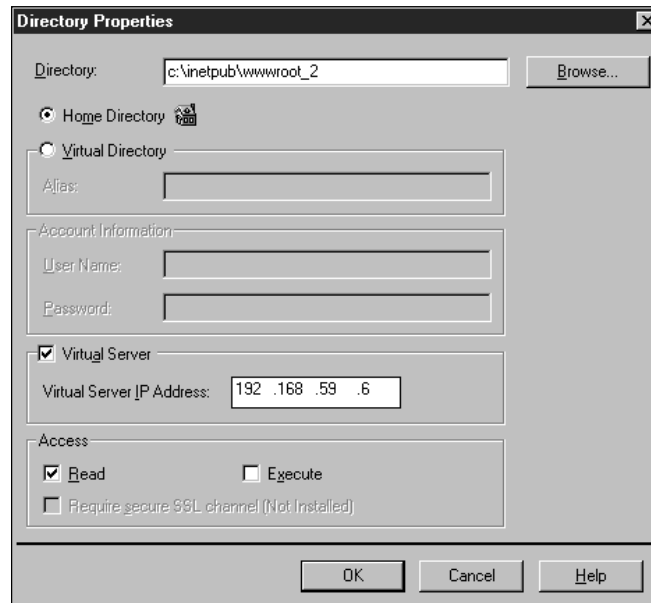
FIGURE 16-26   Configuring a virtual server

Peer Web Services Versus Internet Information Server

Peer Web Services is a Windows NT Workstation Internet publishing service. Peer Web Services is substantially the same as Internet Information Server, except Peer Web Services is optimized as a small-scale intranet publishing service for a limited number of users. Additionally, Peer Web Services lacks some of the functionality of IIS — most notably, Peer Web Services cannot accommodate virtual servers and cannot be configured to control access to the WWW service by an IP address.

Peer Web Services can be installed on any Windows NT Workstation computer with TCP/IP installed on it.

Internet Service Manager can be used to configure Peer Web Services in the same way it is used to configure IIS. On a Windows NT Workstation computer, Internet Service Manager is accessed by selecting Start ≥ Programs ≥ Microsoft Peer Web Services (Common) ≥ Internet Service Manager.

Installing Peer Web Services

Before installing Peer Web Services, you should install Windows NT Workstation and TCP/IP.

TO INSTALL PEER WEB SERVICES ON A WINDOWS NT WORKSTATION COMPUTER, FOLLOW THESE STEPS:

1. Select Start ≫ Settings ≫ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Service tab, click the Add command button.

5. In the Select Network Service dialog box, highlight Microsoft Peer Web Services. Click OK.

6. The Internet Information Server Installation—Files Needed dialog box appears. Ensure the correct source file location is displayed in the text box. (This is normally the I386 folder on the Windows NT Workstation compact disc.) Edit this text box if necessary. Click OK.

7. The Microsoft Peer Web Services Setup dialog box appears. Click OK.

8. In the Microsoft Peer Web Services Setup dialog box, select all the options you want installed with Peer Web Services. Deselect any undesired options. Click OK.

9. When a Microsoft Peer Web Services Setup dialog box appears prompting you to do so, click the Yes command button to create the installation directory.

10. The Publishing Directories dialog box appears. Modify the directories if desired, or accept the default publishing directories. Click OK.

11. A Microsoft Peer Web Services Setup dialog box appears. Click the Yes command button to create the publishing directories.

12. Windows NT copies and installs Peer Web Services. This process takes a few minutes.

13. If you installed the Gopher service and have not yet assigned an Internet domain name to the computer, a dialog box appears, indicating you should assign an Internet domain name to your computer. Click OK.

14. If you installed ODBC drivers and administration, a Microsoft Peer Web Services Setup dialog box appears, indicating you must close Control Panel before you can install the ODBC drivers. Click OK to close Control Panel.

15. If you installed ODBC drivers and administration, the Install Drivers dialog box appears. Highlight the ODBC drivers you want to install, and click OK.

16. A dialog box appears, indicating Microsoft Peer Web Services has been installed and set up. Click OK.

17. The Network dialog box reappears. Click the Close command button.

Troubleshooting Common TCP/IP Connectivity 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 has 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: IP address, subnet mask, and default gateway:

- **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 (the network ID portion of the IP address must be the same for all computers on the local subnet).

- **Subnet mask:** Ensure the computer's subnet mask is the same subnet mask used by all computers and routers located on that subnet.

- **Default gateway:** Ensure the computer's default gateway address matches the IP address of a router on the local subnet.

Two command-line utilities exist that can help you when you're troubleshooting TCP/IP connectivity problems: `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 ≻ Command Prompt. At the command prompt, type **ipconfig /all** 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 ≻ Command Prompt. At the command prompt, type **ping *ip_address*** and press Enter. (The IP address entered is the IP address of the computer with which you are attempting to communicate.) If your computer is able to communicate with the remote computer specified, ping.exe will display four replies from the remote computer's IP address. 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 your local computer. If TCP/IP is correctly configured on your local computer, ping.exe will display four replies from your local computer's IP address.

KEY POINT SUMMARY

This chapter explored how to network Windows NT using TCP/IP. The following points illuminate the major issues:

- The *Transmission Control Protocol/Internet Protocol* (TCP/IP) is a fast, routable, transport protocol that provides robust capabilities for Windows NT networking. TCP/IP is the protocol used on the Internet. TCP/IP is an enterprise protocol that is supported by many other operating systems. TCP/IP is typically the recommended protocol for large, heterogeneous networks.

- An *IP address* is a 32-bit binary number, broken into four 8-bit sections, which uniquely identifies a computer or other network device on a network that uses TCP/IP. *No two computers or other devices on an internetwork should have the same IP address.* An IP address contains two important identifiers: a *network ID* and a *host ID*. All computers located on the same network subnet have the same network ID. Each computer or other network device on a given network subnet must have a unique host ID.

- 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 on a given network segment.* If subnet masks are incorrectly configured, network communications problems due to routing errors may occur.

- A *default gateway address* specifies the IP address of a router on the local network segment. 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.

- IP addresses must be configured on each computer when TCP/IP is installed. You can assign an IP address to a Windows NT computer in one of two ways: by configuring a computer to obtain an IP address from a DHCP server, or by manually specifying a computer's IP address configuration.

- The advantages of using a DHCP server to assign IP addresses are as follows:

  - It allows central management of IP addresses, and assures addresses are valid and not duplicated.

  - It reduces the amount of administration time required to manage and maintain IP addresses for each computer on the network.

  - It reduces the likelihood of human error when IP addresses are assigned, because no need exists to enter an IP address manually on each individual computer.

- *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. Windows NT computers with multiple network adapters (called *multihomed* computers) can function as IP routers. The two primary types of routing are static and dynamic.

    - *Static routing* is basic IP routing. No additional software is necessary to implement static routing in multihomed Windows NT computers. Static routers are **not** capable of automatically building or updating a routing table, but must be manually configured by a network administrator.

    - *Dynamic routing* is intelligent IP routing. By installing *RIP for Internet Protocol*, a multihomed Windows NT Server computer can be configured to function as a dynamic router. A dynamic router is capable of automatically building and updating its routing table.

- The *DHCP Relay Agent* forwards client DHCP configuration requests to a DHCP server on another network segment, thus allowing computers on one subnet to receive IP addresses from a DHCP server located on another subnet.

- *Windows Internet Name Service* (WINS) provides NetBIOS name resolution services to client computers. *NetBIOS name resolution* is the process of resolving a NetBIOS name to an associated IP address. The two common methods used to perform NetBIOS name resolution include manually configuring an `LMHOSTS` file on each individual computer on the network, and installing a WINS server and configuring client computers to use it. The second method is the preferred method because the WINS server dynamically updates its NetBIOS name to IP address tables and, therefore, relieves the network administrator from having to enter and update this information on each computer manually.

- Installing and configuring WINS is a two-step process: first, you must install WINS on a Windows NT Server computer, and then you must configure each client computer on the network to use the WINS server for NetBIOS name resolution.

- Microsoft DNS Server provides host name resolution services to client computers. *Host name resolution* is the process of resolving a Fully Qualified Domain Name to an associated IP address. On the Internet, host names are stored in domains and subdomains that form a hierarchical tree structure called the *Domain Name System* (DNS). The root of the DNS structure contains several familiar domains, including: `com`, `gov`, `mil`, `edu`, `net`, and `org`. Each subdomain is called a *zone*.

- When you initially install a DNS server, you must create a zone in which the DNS server will maintain its host names. A DNS server can have multiple zones. A DNS server stores all zone information, including host names and their associated IP addresses, in a database called a *DNS database.* A DNS database is *not* dynamically created—the network administrator must *manually enter* host names and their associated IP addresses for each computer on the network. An alternative to entering every host name and associated IP address manually into a DNS database is to configure Microsoft DNS Server to use a WINS Server to resolve host names.

- Installing and configuring Microsoft DNS Server is a three-step process: First, you install Microsoft DNS Server on a Windows NT Server computer. Second, you configure a zone on the Microsoft DNS Server. (Optionally, on networks that use DHCP and WINS, you can also configure Microsoft DNS Server to use WINS Lookup for host name resolution.) Third, you configure each client computer on the network to use a DNS server for host name resolution.

- Microsoft has two primary tools for publishing on the Internet: *Internet Information Server* for Windows NT Server computers, and *Peer Web Services* for Windows NT Workstation computers. Both of these products require the use of TCP/IP.

- *Internet Information Server* (IIS) provides WWW, FTP, and Gopher publishing services. No additional hardware is required to install IIS on an internal intranet. If you want to connect your IIS to the Internet, however, you need additional hardware to support this connection.

- *Internet Service Manager* is a Windows NT tool you can use to manage IIS. You can use Internet Service Manager to configure the IIS services, configure IIS security, and start and stop the individual IIS services.

- Many of the configuration options on the WWW service enable you to manage security. When configuring password authentication, you can clear the check box next to Basic (Clear Text) and select the check box next to Windows NT Challenge/Response to prevent user names and passwords from being transmitted in an unencrypted format over the Internet. You can control access by IP address. You can ensure directory browsing is not selected, and you can require users to supply user names and passwords by not permitting anonymous users to access the WWW service.

- A *virtual server* is a pseudo WWW server with its own unique domain name and IP address. To the Internet user accessing the virtual server, a virtual server appears to be a separate server; but in reality, a virtual server is not a separate server, but more like an extra shared folder on an Internet Information Server. A single Internet Information Server can be configured to accommodate multiple virtual servers. Before you can configure a virtual server, you must configure an additional IP address for the network adapter in the Windows NT Server computer.

- *Peer Web Services* is a Windows NT Workstation Internet publishing service that is substantially the same as IIS, but is optimized as a small-scale intranet publishing service for a limited number of users. Before installing Peer Web Services, you should install Windows NT Workstation and TCP/IP.

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

  - 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. (The network ID portion of the IP address must be the same for all computers on the local subnet.)

  - Ensure the computer's subnet mask is the same subnet mask used by all computers and routers located on that subnet.

  - Ensure the computer's default gateway address matches the IP address of a router on the local subnet.

  - Also consider using the `Ipconfig.exe` and `ping.exe` command-line utilities when troubleshooting TCP/IP connectivity problems.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The questions in the following Instant Assessment section bring to mind key facts and concepts. In addition, some of the questions give you a chance to analyze situations and apply your knowledge of TCP/IP to that situation.

The hands-on lab exercises reinforce what you've learned and provide an opportunity for you to practice several tasks tested by the Microsoft Certified Professional Exams.

Instant Assessment

1. What does TCP/IP stand for?
2. Which transport protocol is typically recommended for use in large, heterogeneous networks?
3. What is an IP address?
4. What problem can occur if subnet masks are incorrectly configured?
5. What problem will occur if a computer's default gateway address does not specify a router on the local subnet?
6. What are the two methods you can use to assign IP addresses to Windows NT computers?
7. What is IP routing?
8. What are the two primary types of IP routing?
9. What Windows NT service must you install on a multihomed Windows NT Server computer for it to function as a dynamic router?
10. What is the DHCP Relay Agent, and what function does it perform?
11. What is WINS, and what function does it perform for client computers?
12. What service does Microsoft DNS Server provide to client computers?
13. Your company operates in a high-security environment. What steps can you take to secure access to the WWW service on your Microsoft Internet Information Server?
14. How must you configure the network adapter in your computer before you can configure a virtual server?

15. What are Microsoft's two primary tools for publishing on the Internet?

16. Your company plans to connect its Internet Information Server to the Internet over a fractional T1 leased line. What additional hardware is required to implement the connection?

17. You want to connect your Internet Information Server to the Internet using an ISDN line. What additional hardware is required to implement the connection?

18. What is a virtual server?

19. Which three TCP/IP settings should you check when troubleshooting a computer that has a TCP/IP connectivity problem?

20. You want to determine whether TCP/IP is correctly configured and initialized on a Windows NT computer. Which command-line utility can you use to help you determine this?

21. You want to verify TCP/IP network communications between two Windows NT Server computers. Which command-line utility can you use to help you determine this?

22. You want to display the TCP/IP configuration of a Windows NT computer. Which command-line utility can you use to accomplish this?

	T/F
23. All computers located on the same network segment have the same network ID.	_____
24. Each computer or other network device on a given network segment must have the same host ID.	_____
25. A subnet mask should be the same for all computers and other network devices on a given network segment.	_____
26. Static routers are *not* capable of automatically building and updating a routing table and must be manually configured.	_____
27. Dynamic routers are *not* capable of automatically building and updating a routing table and must be manually configured.	_____
28. A WINS server dynamically updates its NetBIOS name to IP address tables.	_____
29. A DNS database is dynamically created.	_____

concept link **For answers to the Instant Assessment questions see Appendix D.**

Hands-on Lab Exercises

The following hands-on lab exercises provide you with practical opportunities to apply the TCP/IP knowledge you've gained in this chapter.

Lab 16.25 *Implementing WINS and Microsoft DNS Server*

MCSE

Enterprise

The purpose of this lab exercise is to give you hands-on experience in installing WINS and DNS Server, and configuring DNS Server to interact with WINS.

This lab consists of two parts:

Part 1: Installing WINS and Microsoft DNS Server

Part 2: Configuring Microsoft DNS Server to interact with WINS

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator. Place your Windows NT Server compact disc in your CD-ROM drive.

Complete the following steps carefully.

Part 1: Installing WINS and Microsoft DNS Server

In this section, you install Windows Internet Name Service (WINS) and Microsoft Domain Name Service (DNS) Server on a Windows NT Server computer.

1. Select Start ➢ Settings ➢ Control Panel.
2. In the Control Panel dialog box, double-click Network.
3. In the Network dialog box, click the Services tab.
4. On the Services tab, click the Add command button.
5. In the Select Network Service dialog box, highlight Microsoft DNS Server. Click OK.
6. A Windows NT Setup dialog box appears. Ensure the correct source file location is displayed in the text box at the bottom of the dialog box. (This is probably the I386 folder on your Windows NT Server compact disc.) Edit this text box if necessary. Click the Continue command button.
7. Windows NT copies and installs Microsoft DNS Server. The Network dialog box reappears. Click the Add command button.
8. The Select Network Service dialog box appears. Scroll down and highlight Windows Internet Name Service. Click OK.

9. A Windows NT Setup dialog box appears. Ensure the correct source file location is displayed in the text box at the bottom of the dialog box. Click the Continue command button.

10. Windows NT copies and installs WINS. The Network dialog box reappears. Click the Close command button.

11. Windows NT performs various bindings operations. A Network Settings Change warning dialog box appears, asking if you want to restart your computer now for the new settings to take effect. Click the Yes command button.

12. Boot your computer to Windows NT Server and log on as Administrator. Continue on to Part 2.

Part 2: Configuring Microsoft DNS Server to interact with WINS

In this section, you configure Microsoft DNS Server to use WINS to resolve host names to IP addresses.

1. From the desktop, select Start ≫ Programs ≫ Administrative Tools (Common) ≫ DNS Manager.

2. In the Domain Name Service Manager dialog box, select DNS ≫ New Server.

3. The Add DNS Server dialog box appears. Type **192.168.59.5** in the DNS Server text box. Click OK.

4. Your server appears (indicated by its IP address) in the Server List on the left side of the Domain Name Service Manager dialog box. Right-click your server's IP address. Select Refresh from the menu that appears. Right-click again on your server's IP address. Select New Zone from the menu that appears.

5. The "Creating new zone for 192.168.59.5" dialog box appears. Select the radio button next to Primary. Click the Next command button.

6. Type **lab.com** in the Zone Name text box. Type **lab.com.dns** in the Zone File text box. Click the Next command button.

7. Click the Finish command button in the "Creating new zone for 192.168.59.5" dialog box. The `lab.com` zone appears in the Domain Name Service Manager dialog box under the Server List for your Windows NT Server computer. Right-click `lab.com`, and then select Properties from the menu that appears.

8. The "Zone Properties-lab.com" dialog box appears. Click the WINS Lookup tab.

9. On the WINS Lookup tab, select the check box next to Use WINS Resolution. In the uppermost WINS Servers text box, type **192.168.59.5** and click the Add command button. Click OK.

10. Your DNS Server is now configured to use WINS for host name resolution. Exit DNS Manager.

Lab 16.26 *Configuring Internet Information Server and installing and configuring Peer Web Services*

Workstation Enterprise

The purpose of this lab exercise is to give you hands-on experience in configuring Microsoft Internet Information Server and in installing and configuring Peer Web Services.

This lab consists of two parts:

Part 1: Configuring Microsoft Internet Information Server

Part 2: Installing and configuring Peer Web Services

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator.

Complete the following steps carefully.

Part 1: Configuring Microsoft Internet Information Server

In this section, you configure Microsoft Internet Information Server on your Windows NT Server computer.

1. Select Start ≻ Programs ≻ Microsoft Internet Server (Common) ≻ Internet Information Server Setup.

2. The Microsoft Internet Information Server 2.0 Setup dialog box appears. Click OK.

3. In the next Microsoft Internet Information Server 2.0 Setup dialog box that appears, click the Add/Remove command button.

4. Ensure the correct source file location is displayed in the text box. (This is probably the `C:\WINNTSRV\system32\inetsrv` folder on your Windows NT Server computer.) It should be unnecessary to edit this text box. Click OK.

5. In the Microsoft Internet Information Server 2.0 Setup dialog box, *deselect* the check box next to Gopher Service. (This will deinstall the Gopher Service, which is not used in most NT installations.) Click OK.

6. The Microsoft Internet Information Server 2.0 Setup dialog box appears. Click the Yes command button to stop the Gopher Publishing Service.

7. In the Microsoft Internet Information Server 2.0 Setup dialog box, click OK.

8. Select Start ≻ Programs ≻ Microsoft Internet Server (Common) ≻ Internet Service Manager.

9. In the Microsoft Internet Service Manager dialog box, double-click the first computer listed in the Computer list box.

10. The "WWW Service Properties for pdclab" dialog box appears. Notice the configuration options available on the Service tab. Click the Directories tab.

11. On the Directories tab, notice the configuration options available. Click the Logging tab.

12. On the Logging tab, notice the configuration options available. Click the Advanced tab.

13. Notice the configuration options available. Click OK.

14. In the Microsoft Internet Service Manager dialog box, highlight the first computer listed in the Computer list box. Select Properties ≻ Stop Service.

15. Notice the state of the WWW service has changed to Stopped. Select Properties ≻ Start Service.

16. Notice the state of the WWW service has changed to Running. Exit Microsoft Internet Service Manager.

17. Double-click Internet Explorer on your desktop.

18. The Microsoft Internet Explorer Home Page dialog box appears. Edit the Open text box so it reads **pdclab** and press Enter.

19. The Microsoft Internet Information Server home page is displayed. You have successfully configured and accessed the Microsoft Internet Information Server. Exit Internet Explorer.

20. Shut down your computer, reboot to Windows NT Workstation, and log on as Administrator. Place the Windows NT Workstation compact disc in your CD-ROM drive. Continue to Part 2.

Part 2: Installing and configuring Peer Web Services

In this section, you install and configure Peer Web Services on your Windows NT Workstation computer.

1. Select Start ≻ Settings ≻ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Services tab.

4. On the Service tab, click the Add command button.

5. In the Select Network Service dialog box, highlight Microsoft Peer Web Services. Click OK.

6. The Internet Information Server Installation—Files Needed dialog box appears. Ensure the correct source file location is displayed in the text box. (This is normally the I386 folder on your Windows NT Workstation compact disc.) Edit this text box if necessary. Click OK.

7. The Microsoft Peer Web Services Setup dialog box appears. Click OK.

8. In the Microsoft Peer Web Services Setup dialog box, *deselect* the check box next to Gopher Service. *Select* the check box next to Internet Service Manager (HTML). Click OK.

9. When a dialog box appears prompting you to do so, click the Yes command button to create the installation directory.

10. The Publishing Directories dialog box appears. Click OK to accept the default publishing directories.

11. Windows NT copies and installs Peer Web Services. This process takes a few minutes.

12. If a Microsoft Peer Web Services Setup dialog box appears, indicating you must close Control Panel before you can install the ODBC drivers, click OK to close Control Panel.

The Install Drivers dialog box appears. Highlight SQL Server, and then click OK.

13. A dialog box appears, indicating Microsoft Peer Web Services has been installed and set up. Click OK.

14. The Network dialog box reappears. Click the Close command button.

15. Exit Control Panel if it is still open.

16. Double-click Internet Explorer.

17. The Microsoft Internet Explorer Home Page appears. Edit the Address text box so it reads: **ntw40** and press Enter.

18. The Microsoft Peer Web Services home page is displayed. Scroll down to the Administrative Tools heading, and click the blue text that reads *click here* in the description under that heading.

19. Internet Service Manager for Peer Web Services appears. This is an HTML version of Internet Service Manager. Exit Internet Explorer.

Lab 16.27 *Installing and configuring an Internet (TCP/IP) router*

The purpose of this lab exercise is to give you hands-on experience in installing and configuring an Internet (TCP/IP) router on a Windows NT Server computer.

Begin this lab by booting your computer to Windows NT Server. Log on as Administrator. Place your Windows NT Server compact disc in your CD-ROM drive.

Complete the following steps carefully.

Server
Enterprise

1. Select Start ≻ Settings ≻ Control Panel.

2. In the Control Panel dialog box, double-click Network.

3. In the Network dialog box, click the Adapters tab.

4. On the Adapters tab, click the Add command button.

5. In the Select Network Adapter dialog box, highlight MS Loopback Adapter. Click OK. (You already installed a network adapter when you initially installed Windows NT Server. This step installs a second network adapter that will allow your computer to function as a TCP/IP router.)

6. The MS Loopback Adapter Card Setup dialog box appears. Click OK.

7. The Windows NT Setup dialog box appears. Ensure the correct source file location is displayed in the text box. (This is probably the I386 folder on your Windows NT Server compact disc.) Edit this text box if necessary. Click the Continue command button.

8. The Network dialog box reappears. Click the Services tab.

9. On the Services tab, click the Add command button.

10. In the Select Network Service dialog box, highlight RIP for Internet Protocol. Click OK.

11. The Windows NT Setup dialog box appears. Ensure the correct source file location is displayed in the text box. Click the Continue command button.

12. The Network dialog box reappears. Click the Close command button.

13. Windows NT performs various bindings operations, and then displays the Microsoft TCP/IP Properties dialog box. In the Adapter drop-down list box, select the MS Loopback adapter you installed in Steps 5–7 in this lab. (This is the second adapter in the list.) In the IP Address text box, type **192.168.60.1** and press Tab. In the Subnet Mask text box, type **255.255.255.0** and then click the Routing tab.

14. On the Routing tab, notice the check box next to Enable IP Forwarding is checked. Windows NT automatically selects this check box when RIP for Internet Protocol is installed. Click OK.

15. A Network Settings Change dialog box appears. Click the Yes command button to restart your computer so the new settings can take effect.

caution ▽ **If your computer is connected to a network that uses TCP/IP, you should remove RIP for Internet Protocol after the computer reboots. If you don't do this, it can cause routing problems on your network. (To remove RIP for Internet Protocol, use the Services tab in the Network application in Control Panel.) You will have to reboot your computer again after you remove RIP for Internet Protocol.**

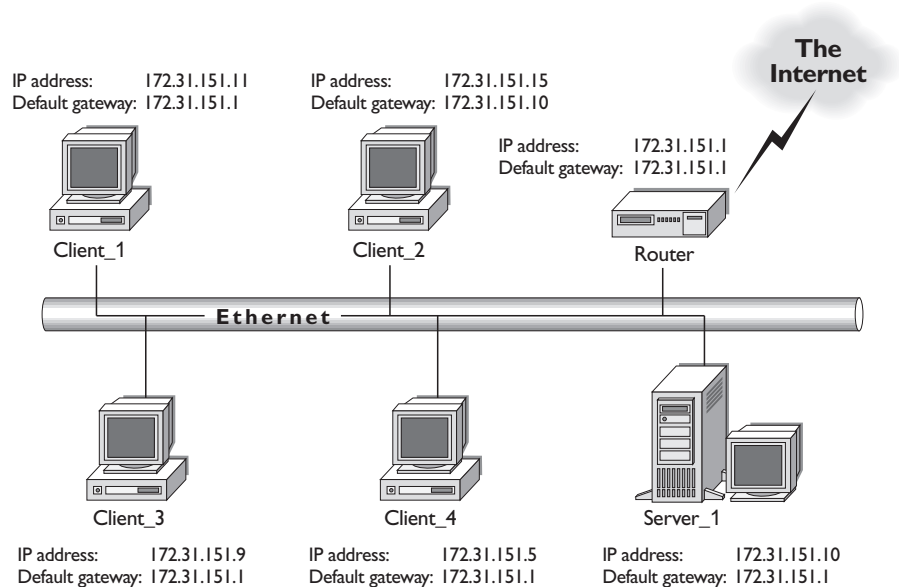## Lab 16.28 *Identifying and resolving TCP/IP connectivity problems*

The purpose of this lab exercise is to give you hands-on experience in identifying and resolving common TCP/IP connectivity problems.

Server
Enterprise

In each of the following situations:

1. Identify the TCP/IP connectivity problem (for example, an invalid or duplicate IP address).

2. Describe what you would do to resolve the problem.

**Situation 1**   Several components on a network subnet are configured as shown in Figure 16-27:

IP address: 172.31.151.11
Default gateway: 172.31.151.1

IP address: 172.31.151.15
Default gateway: 172.31.151.10

IP address: 172.31.151.1
Default gateway: 172.31.151.1

Client_1

Client_2

Router

The Internet

Ethernet

Client_3

Client_4

Server_1

IP address: 172.31.151.9
Default gateway: 172.31.151.1

IP address: 172.31.151.5
Default gateway: 172.31.151.1

IP address: 172.31.151.10
Default gateway: 172.31.151.1

FIGURE 16-27   Network subnet configuration for Situation 1

What is the TCP/IP connectivity problem in this situation?

What would you do to resolve the problem?

Situation 2   Several components on a network subnet are configured as shown
in Figure 16-28.
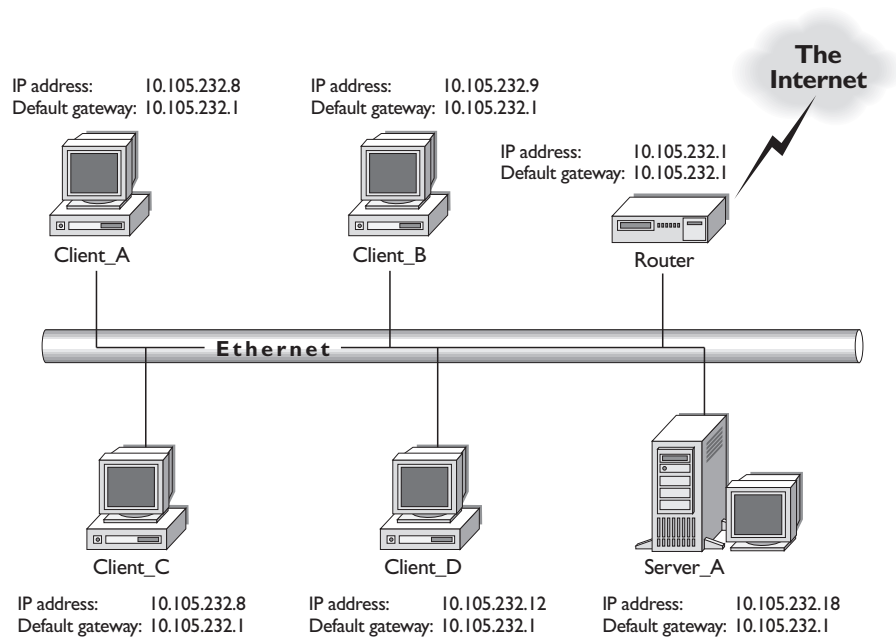
FIGURE 16-28   **Network subnet configuration for Situation 2**

What is the TCP/IP connectivity problem in this situation?

What would you do to resolve the problem?

concept link   **For answers to the hands–on lab exercise see Appendix D.**