EXAM OBJECTIVES

Network ▶

Exam 70-216

- Install, configure and troubleshoot DNS.
  - Install the DNS Server service.
  - Configure a root server.
  - Configure zones.
  - Configure a caching-only server.
  - Configure a DNS client.
  - Configure zones for dynamic updates.
  - Test the DNS Server service.
  - Implement a delegated zone for DNS.
  - Manually create DNS resource records.
- Manage and monitor DNS.

Directory Services ▶

Exam 70-217

- Install, configure and troubleshoot the components of Active Directory.
  - Install Active Directory.
  - Verify Active Directory installation.
- Install, configure and troubleshoot DNS for Active Directory.
  - Integrate an Active Directory DNS with a non-Active Directory DNS.
  - Configure zones for dynamic updates.
- Manage, monitor, and troubleshoot DNS.
  - Manage replication of DNS data.

CHAPTER

7

Installing and Configuring DNS and Active Directory

This chapter features important information on two tightly integrated Windows 2000 topics: DNS and Active Directory. You may be wondering what these two subjects are doing in the same chapter, but let me reassure you that they really do belong together. Because Active Directory is dependent on DNS, you've got to understand DNS (and in many cases you'll want to have your DNS server up and running) before you install Active Directory.

The bulk of this chapter, then, is all about DNS. I'll explain what DNS is, as well as how to install, configure, test, monitor, and troubleshoot DNS on a Windows 2000 Server/Advanced Server computer. I'll also show you how to configure client computers to use a DNS server. Finally, I'll discuss how to install Active Directory, including how to verify and troubleshoot the Active Directory installation.

Chapter Pre-Test

1. What does DNS stand for?
2. Define the term ***host name resolution***.
3. The DNS domain at the top of the DNS domain namespace is called the _____ domain. This domain is often represented by a _____.
4. List four types of DNS servers.
5. What does TTL stand for?
6. What two prerequisites must be met prior to installing Active Directory?

What Is DNS?

DNS stands for Domain Name System. The primary purpose of DNS, which consists of a set of specified naming rules and implementation standards, is to provide host name resolution.

Host name resolution is the process of resolving a computer's user-friendly host name (such as `www.idgbooks.com`) to the numerical IP address of that computer. The reason host name resolution is important is because TCP/IP-based applications and utilities, such as Web browsers, use IP addresses to communicate with other computers, while users prefer to use easily remembered host names to access other computers.

In the next several sections I'll explain what DNS has to do with Active Directory, talk a little about DNS domain names and naming conventions, explain in detail how host name resolution works using DNS, introduce you to zones and other basic DNS terminology, and finally, describe the many DNS server roles.

What Does DNS Have to Do with Active Directory?

You're probably wondering why I'm discussing DNS in the same chapter as Active Directory. (I know my editor did.) As I explained in Chapter 2, Active Directory uses the same hierarchical naming conventions as DNS. Because of this, client computers use DNS servers to locate Active Directory domain controllers and other Active Directory resources on the network. Without DNS, Active Directory couldn't function, because client computers wouldn't be able to locate these domain controllers and resources.

The bottom line, then, is that Active Directory is dependent on DNS. In fact, Active Directory can't be implemented until the DNS Server service (or its equivalent) is installed.

TIP

The actual installation of DNS can take place either prior to installing Active Directory, or as part of the Active Directory installation.

For large, established networks, it usually makes sense to install and configure a DNS server prior to installing Active Directory. However, for very small or brand new networks, it's easier to install DNS during the Active Directory installation.

DNS Domain Names and Naming Conventions

DNS is implemented as a hierarchical structure often called the *DNS domain namespace*. The trees and subtrees that make up the DNS domain namespace are called *DNS domains*. The DNS domain namespace is graphically represented as an inverted tree structure, with the root of the tree at the top.

The DNS domain at the top (or root) of the tree is called the *root domain*. It is often represented by a period (.).

The DNS domains directly under the root domain are called *top-level* domains. I've listed the most common top-level DNS domains for you in Table 7-1.

TABLE 7-1 Top-Level DNS domains

DNS Domain	Description of Subdomains of This Domain
`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`
`arpa`	Domains used for resolving IP addresses to host names, sometimes called reverse DNS or reverse lookup domains, such as `123.arpa`
xx	Domains within a specific country, where each country is represented by a two-letter code, such as `cbc.ca` (where `ca` stands for Canada)

The DNS domains in the next level down, under top-level domains, are called *second-level domains*. These domains are subdomains of top-level domains. Many businesses have a second-level domain that is a subdomain of the `com` domain, such as `microsoft.com`. Each person or organization using a second-level domain on the Internet is responsible for registering that unique DNS domain name with the appropriate authority — the appropriate authority being the one that manages the top-level domain containing the second-level domain. If your organization's network is *never* connected to the Internet, you can use any top-level and second-level domain names you want to, and you don't have to register these names with any naming authority.

Figure 7-1 shows a partial illustration of the DNS domain namespace, and includes the root domain, several top-level domains, and a couple of second-level domains.

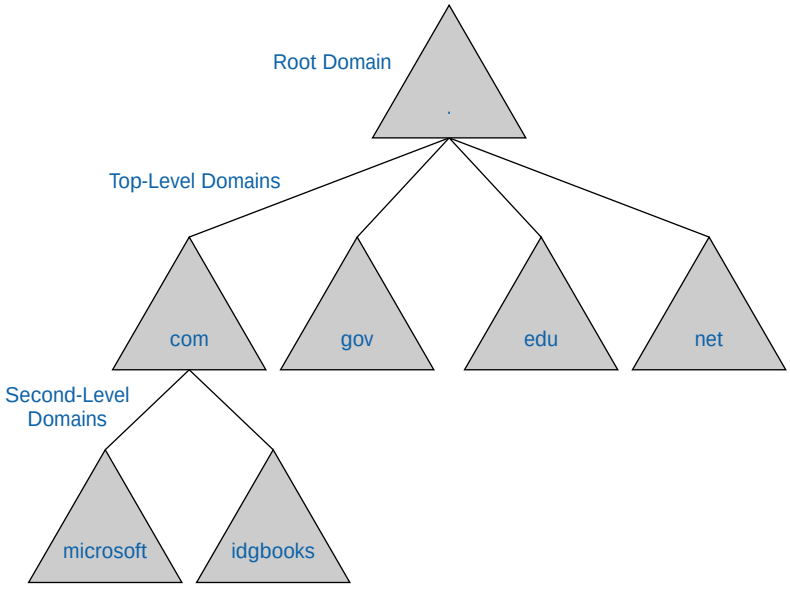

FIGURE 7-1 The DNS domain namespace

You may be wondering, at this point, if DNS domains are the same as Windows 2000 domains. In short, no, they're not the same. However, Windows 2000 domains directly correspond to and have the same names as their corresponding DNS domains. In addition, Windows 2000 Active Directory is designed to be tightly integrated with DNS.

DNS domain names (also called *fully qualified domain names* [FQDNs]) can contain a maximum of 63 characters. Allowed characters include uppercase letters (A–Z), lowercase letters (a–z), numbers (0–9), and the hyphen (-). Periods are used to separate domain and subdomain names, for example, `microsoft.com`.

How Host Name Resolution Works Using DNS

Earlier in this chapter I gave you a basic definition of host name resolution. What I didn't explain then (and I'm going to now) is a detailed account of *how* the host name resolution process works when using DNS.

So, suppose that a user wants to access the Microsoft Web site at `www.microsoft.com`. The user, in this example, is using a Windows 2000 Professional computer on IDG Books Worldwide, Inc.'s network. Here's a detailed account of how name resolution is accomplished in this case:

1. The user types in a URL of `www.microsoft.com` in Internet Explorer on his or her Windows 2000 Professional computer.
2. Internet Explorer asks the DNS client software (on the user's computer) to determine the IP address of `www.microsoft.com`.
3. The DNS client software (on the user's computer) sends a request (called a *query*) to the DNS server on the IDG Books Worldwide, Inc. network, asking that server to resolve `www.microsoft.com` to an IP address.
4. Because the DNS server on the IDG Books Worldwide, Inc. network primarily contains host name resolution information for only the computers in the `idgbooks.com` domain, it sends a query to a DNS server in the root domain, asking for the IP address of `www.microsoft.com`.
5. The DNS server in the root domain provides the IDG Books DNS server with the IP address of a DNS server in the `com` domain that can help the IDG Books DNS server resolve its query.
6. The IDG Books DNS server sends a query to the DNS server in the `com` domain, asking for the IP address of `www.microsoft.com`.
7. The DNS server in the `com` domain provides the IDG Books DNS server with the IP address of a DNS server in the `microsoft.com` domain that can help the IDG Books DNS server resolve its query.
8. The IDG Books DNS server sends a query to the DNS server in the `microsoft.com` domain, asking for the IP address of `www.microsoft.com`.
9. The DNS server in the `microsoft.com` domain provides the IDG Books DNS server with the IP address of `www.microsoft.com`.
10. When the IDG Books DNS server receives the IP address of `www.microsoft.com`, it performs two tasks:
    - It stores the IP address of `www.microsoft.com` in its cache, so it can quickly resolve this name when it is requested in the future.

- ▶ It sends the IP address of `www.microsoft.com` to the DNS client software on the user's computer that requested it.

11. When the DNS client software on the user's computer receives the IP address of `www.microsoft.com`, it caches this IP address for future use, and also forwards the IP address to Internet Explorer.
12. Internet Explorer then establishes TCP/IP network communications with `www.microsoft.com`, and opens the Web page for the user.

Zones and DNS Server Roles

Before I get into the actual nuts and bolts of implementing DNS, I need to explain some basic DNS terminology. In this section I'll define zones and several other DNS terms. I'll also describe the many types of roles DNS servers can play.

A *zone* is a storage database for either a DNS domain or for a DNS domain and one or more of its subdomains. This storage database is often implemented as a special text file, called a *zone file*.

TIP

The terms *zone* and *zone file* are often used interchangeably.

Zones are not created by default when the DNS Server service is installed — they are created and configured by an administrator.

DNS servers are computers that have the capability to use DNS to provide host name resolution to client computers. The Windows 2000 DNS Server service (or its equivalent), when installed on a server, is what gives that server the ability to provide host name resolution. A DNS server can provide host name resolution for more than one zone. In addition, copies of a zone can exist on multiple DNS servers for the purposes of providing load balancing and fault tolerance.

On all Windows 2000 DNS servers *except* Active Directory-integrated DNS servers, all DNS entries for a zone are contained in a single text file called a zone file. On Active Directory-integrated DNS servers, DNS entries are stored in the Active Directory data store instead of in a zone file.

A DNS server can play one (or more) of several different roles, depending on the type of zone(s) the server contains and how the DNS server is configured. The types of roles that a DNS server can perform include:

- **Standard primary:** This type of DNS server stores *DNS entries* (IP address to host name mapping information and other DNS resource records) in a zone file that is maintained on this server. The standard primary server is typically called the primary server for short. The primary server maintains the master copy of a zone file. Because of this, when changes need to be made to the zone, they should be made *only* on the standard primary server. There can only be one standard primary server for a zone.
- **Active Directory-integrated (primary):** This type of DNS server is just like a standard primary server, except that it stores DNS entries in the Active Directory data store, rather than in a zone file. Because Active Directory supports multiple master replication, there can be more than one Active Directory-integrated (primary) DNS server for a zone. When changes need to made to the zone, they can be made on any Active Directory-integrated (primary) DNS server that contains the zone.
- **Standard secondary:** This type of DNS server stores copies of zones that it obtains from the standard primary, Active Directory-integrated (primary), or another standard secondary DNS server. The standard secondary server is typically called the secondary server for short. The process of copying a zone to a standard secondary DNS server is called a *zone transfer*. Microsoft sometimes calls this process *replication*. There can be multiple secondary DNS servers for a zone.
- **Master:** This type of DNS server provides a copy of the zone to a standard secondary DNS server. The secondary DNS server receiving the copy of the zone is sometimes called the *slave* in this relationship. The types of DNS servers that can function as masters are standard primary, Active Directory-integrated (primary), and standard secondary.
- **Caching-only:** This type of DNS server does not store any zones whatsoever. It resolves host names to IP addresses for client computers, and stores the resulting mapping information in its cache. If a client computer requests resolution for a host name that exists in the cache, the DNS server provides the

cached information to the client computer without contacting other DNS servers to resolve the query. Mapping information remains in the cache for a specified amount of time (called *Time-To-Live* [TTL]), and then is "flushed" from the cache.

- **Forwarder:** This type of DNS server is designated to perform host name resolution for other DNS servers on a company's internal network when the host name to be resolved resides in an *external* DNS domain. The forwarder resolves the host name resolution request, caches the results, and returns the mapping information to the internal DNS server that requested it.

  The forwarder role is often played by the same computer that functions as the company's firewall. There are two primary advantages of this arrangement. First, *internal* network traffic is reduced because the forwarder (instead of many internal DNS servers) executes the numerous queries required to perform host name resolution. These queries are external rather than internal, thus reducing internal traffic. In addition, the forwarder maintains a cache of all externally resolved names, thus eliminating repeated queries for the same information. Second, because the forwarder is often configured as a caching-only DNS server, the company's internal zone information is protected from hackers on the Internet.

- **Root server:** This type of DNS server contains a copy of a zone for the root domain — either the root domain for the Internet, or the root domain for a company's private, internal network. The purpose of the root server is to enable other DNS servers on a network to access second-level domains on the Internet, or to access other second-level domains on the internal network. A root server should be used only when a network is not connected to the Internet, or when a network is connected to the Internet by using a proxy server.

EXAM TIP

DNS topics make up a large portion of the objectives for both the Network and Directory Services exams. Make sure that you understand DNS concepts and terminology, and get as much hands-on practice with DNS as possible before you take these exams.

Installing, Configuring, Managing, and Troubleshooting DNS

DNS is implemented in Windows 2000 via the *DNS Server service*. The DNS Server service is supported only on Windows 2000 Server and Advanced Server computers — you can't install the DNS Server service on a Windows 2000 Professional computer, but a Windows 2000 Professional computer can be a DNS client.

The Windows 2000 DNS Server service supports the dynamic update protocol. The term *dynamic update* means that client computers and servers can register and update their host names and IP addresses with the DNS server without administrator intervention. Previous versions of DNS, including the version that shipped with Windows NT 4.0, required the administrator to manually enter host names and their associated IP addresses for each computer on the network.

The Windows 2000 DNS Server service also supports the SRV (service) resource records that are required for the implementation of Active Directory. A *resource record* is any entry in a zone. The entry may be a host name to IP address mapping entry, a service name to IP address mapping entry, and so on. I'll discuss resource records in more depth later in this chapter when I explain how to manually create DNS resource records.

In the following sections I'll explain how to install and configure the DNS Server service on a Windows 2000 Server computer, including how to configure various properties of servers and how to configure zones; how to configure client computers to use a DNS server; and how to test, monitor, and troubleshot DNS.

Installing the DNS Server Service

The DNS Server service is not installed by default on Windows 2000 Server/Advanced Server computers — you must manually install this service on each computer that you want to function as a DNS server.

Before you can install the DNS Server service, the Windows 2000 Server/Advanced Server computer must be configured to use a static IP address. If your computer is configured to use DHCP to obtain its IP address dynamically, you must reconfigure the computer with a static IP address before you install DNS. In addition, before you install DNS, you should

configure the Windows 2000 Server/Advanced Server computer with a primary DNS suffix.

TIP

If you have a DHCP server on your network, and you chose the "Typical settings" option during the Windows 2000 installation, you probably need to reconfigure your computer to use a static IP address.

If you have to reconfigure your computer to use a static IP address prior to installing the DNS Server service, here's how to accomplish this task.

STEP BY STEP

CONFIGURING A STATIC IP ADDRESS

1. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the `Network and Dial-up Connections` folder.
3. In the `Network and Dial-up Connections` folder, right-click Local Area Connection and select Properties from the menu that appears.

TIP

If you have more than one Local Area Connection, you'll have to repeat this process for each one.

4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, select the "Use the following IP Address" option, and type in a static IP address, subnet mask, and default gateway. Click OK.
6. In the Local Area Connection Properties dialog box, click OK.
7. Close the `Network and Dial-up Connections` folder.

In order for DNS to function properly on your Windows 2000 Server/Advanced Server computer, you'll also want to configure the computer to use a primary DNS suffix, as the following steps explain.

STEP BY STEP

CONFIGURING A PRIMARY DNS SUFFIX

1. From the desktop, right-click My Computer and select Properties from the menu that appears.
2. In the System Properties dialog box, click the Network Identification tab.
3. On the Network Identification tab, click Properties.
4. In the Identification Changes dialog box, click More.
5. In the DNS Suffix and NetBIOS Computer Name dialog box, type your company's FQDN in the "Primary DNS suffix of this computer" text box (for example, mycompany.com). Click OK.
6. In the Identification Changes dialog box, click OK.
7. In the Network Identification dialog box, click OK.
8. On the Network Identification tab, click OK.
9. In the System Settings Change dialog box, click Yes to restart your computer.

Now you're ready to install the DNS Server service on your Windows 2000 Server/Advanced Server computer.

STEP BY STEP

INSTALLING THE DNS SERVER SERVICE

1. Place your Windows 2000 Server or Advanced Server compact disc into your computer's CD-ROM drive. Select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. The Windows Components Wizard starts. In the Windows Components screen, scroll down and highlight Networking Services. Click Details.
5. In the Networking Services dialog box, select the check box next to Domain Name System (DNS). Click OK.
6. In the Windows Components screen, click Next.
7. Windows 2000 Setup configures components. In the Completing the Windows Components Wizard screen, click Finish.
8. Close the Add/Remove Programs dialog box. Close Control Panel.

Configuring DNS

Now that you've installed the DNS Server service on a Windows 2000 Server/Advanced Server computer, you're ready to configure it.

Windows 2000 includes a tool specifically designed to help you configure and manage DNS servers — it's an administrative tool called DNS. To access this tool, select Start ➪ Programs ➪ Administrative Tools ➪ DNS. You must be a member of the Administrators group to use this tool.

Configuring DNS can include many different tasks, such as configuring a DNS server to be its own DNS client, configuring a server to play one or more server roles, configuring the properties of a DNS server, configuring zones, integrating an Active Directory DNS with a non–Active Directory DNS, managing replication of DNS, and manually creating DNS resource records. I'll show you how to perform each of these tasks in the following sections.

EXAM TIP

The Network exam contains at least five objectives dealing with configuring DNS. Ensure that you understand *why* and *how* each configuration is used, the steps involved in performing each task, and *which* computer you need to perform the necessary configuration on.

Configuring a DNS Server as Its Own DNS Client

One of the first things you should do after you install the DNS Server service on your Windows 2000 Server computer is to configure your new DNS server to be its own client. What I mean by this is that your DNS server needs to be configured *to use itself* to perform host name resolution.

CAUTION

If you don't make this configuration change on your DNS server, common DNS testing utilities and other TCP/IP-based programs on the server may not function correctly.

The steps involved in configuring the DNS server to be its own client are fairly straightforward.

STEP BY STEP

CONFIGURING YOUR DNS SERVER TO USE ITSELF

1. From the desktop, select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the `Network and Dial-up Connections` folder.
3. In the `Network and Dial-up Connections` folder, right-click Local Area Connection and select Properties from the menu that appears.

TIP

If you have more than one Local Area Connection, you'll have to repeat this process for each one.

4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, ensure that the "Use the following DNS server addresses" option is selected. Then, in the Preferred DNS server text box, type the IP address of this DNS server. Click Advanced.
6. In the Advanced TCP/IP Settings dialog box, click the DNS tab.
7. On the DNS tab, type the FQDN of the DNS domain that this DNS server belongs to in the "DNS suffix for this connection" text box. Generally it's okay to accept the remaining default settings on this tab. Click OK.
8. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
9. In the Local Area Connection Properties dialog box, click OK.
10. Close the `Network and Dial-up Connections` folder.

Configuring a Root Server

If this is the first DNS server on your network, and your network is *not* connected to the Internet, you may want to consider configuring it to be a root server. If you already have a root server on your network, or if your network is connected to the Internet, you'll need to configure this DNS server to use either the existing root server on your network or the root servers on the Internet.

In either case, you'll need to run the Configure DNS Server Wizard, which can be accessed by starting the DNS administrative tool. In addition to enabling you to configure a root server, the Configure DNS Server Wizard also enables you to create a forward lookup zone and a reverse lookup zone.

A *forward lookup zone* is a zone that contains the host name to IP address mappings and information about available services for either a DNS domain or a DNS domain and one or more of its subdomains. A *reverse lookup zone* is a zone that contains IP address to host name mappings. The mappings in a reverse lookup zone are the opposite of those contained in a forward lookup zone. A DNS server uses a forward lookup zone when a client computer knows the host name, but doesn't know the associated IP address. A DNS server uses a reverse lookup zone when a client computer knows the IP address, but doesn't know the associated host name.

The following steps explain how to configure a root server.

STEP BY STEP

CONFIGURING A ROOT SERVER

1. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the DNS dialog box, highlight your computer in the left pane.
3. Windows 2000 indicates that your DNS server has not yet been configured, as shown in Figure 7-2. Notice the two panes in the DNS administrative tool.

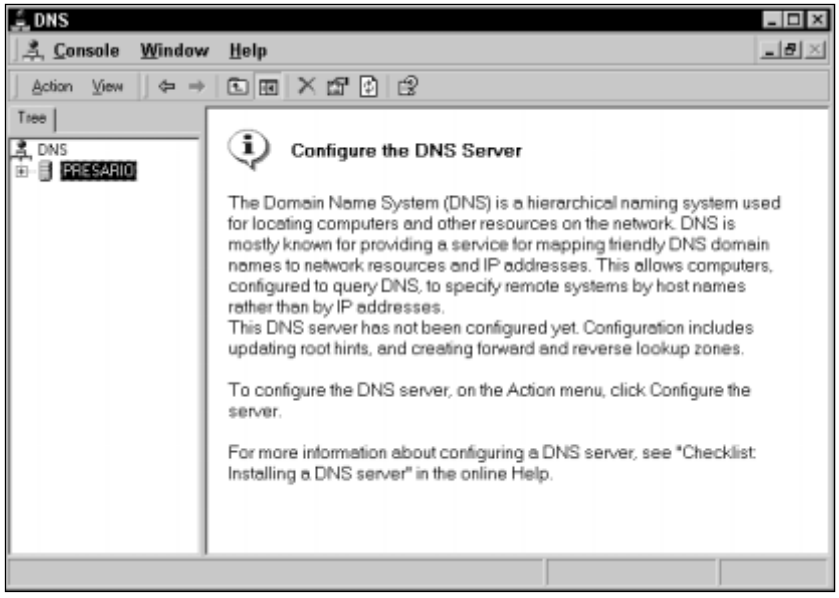

FIGURE 7-2 The DNS administrative tool

Select Action ➪ Configure the server.

4. The Configure DNS Server Wizard starts. Click Next.

STEP BY STEP *Continued*

5. The Root Server screen appears, as shown in Figure 7-3. Notice the two options available in this screen.

FIGURE 7-3 Configuring a root server

TIP

If your DNS server is connected to the Internet, this screen won't appear, because the DNS server will automatically configure itself to use the root servers on the Internet.

If you want to configure this server to be a root server, accept the default option of "This is the first DNS server on this network." Click Next.

If you want this DNS server to use an existing root server on your network, select the "One or more DNS servers are running on this network" option, and provide the IP address of a root server on your network that you want this server to use. Click Next.

6. In the Forward Lookup Zone screen, you can choose whether or not to create a forward lookup zone now.

   If you select the "Yes, create a forward lookup zone" option and click Next, the New Zone Wizard begins. (This wizard is explained fully in the next sections.) Follow the instructions presented on-screen to create your forward lookup zone, and a reverse lookup zone if desired. When you finish creating zones, skip to Step 7.

STEP BY STEP *Continued*

If you select the "No, do not create a forward lookup zone" option, click Next.

7. The Completing the Configure DNS Server Wizard screen appears. Click Finish.
8. The DNS dialog box reappears. This completes the configuration of a root server. Close the DNS dialog box.

Configuring Properties of a DNS Server

There are numerous properties of a DNS server that you can configure. These properties can be configured by using the DNS administrative tool. (To access this tool, select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)

To access a DNS server's Properties dialog box, in the DNS administrative tool, highlight the name of the DNS server you want to configure. Then select Action ➪ Properties.

The DNS server's Properties dialog box appears, as shown in Figure 7-4. Notice the six tabs in this dialog box: Interfaces, Forwarders, Advanced, Root Hints, Logging, and Monitoring.

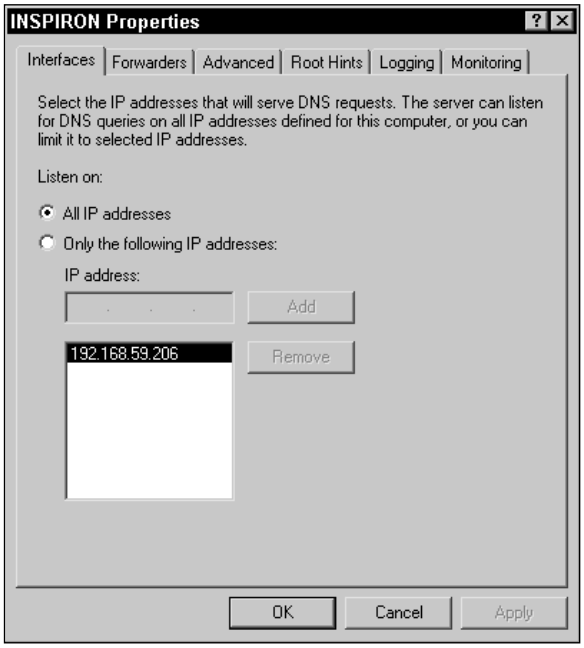

FIGURE 7-4 A DNS server's properties

Configuring Interfaces Also notice in Figure 7-4 that the Interfaces tab appears on top. On this tab, you can limit or specify the network adapters in this computer that will accept DNS queries from client computers. There are two basic options on this tab:

- **All IP addresses:** Selecting this option enables the DNS server to accept client DNS queries that are addressed to any network adapter in the server. This is the default setting.
- **Only the following IP addresses:** Selecting this option enables you to specify which network adapter(s) in the server will accept client DNS queries. Once configured, the server will only accept client DNS queries that are addressed to the specified network adapters (which have been identified on this tab by their associated IP addresses).

This feature is designed to help you protect your DNS server from attack through a network adapter that is connected to a public network, such as the Internet.

Configuring Forwarders The next tab in the DNS server's Properties dialog box is the Forwarders tab, which is shown in Figure 7-5.

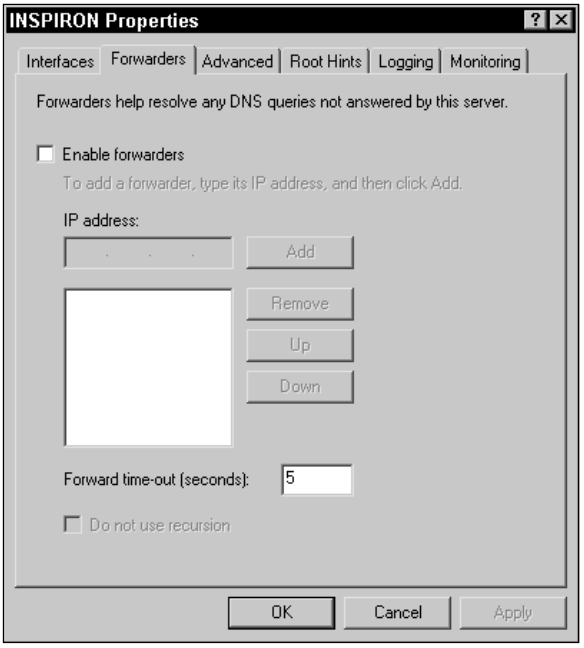

FIGURE 7-5 Enabling forwarders

On this tab, you can configure the DNS server to use one or more other existing DNS servers on your network as a forwarder. If you select this option, you need to specify the IP address of at least one other DNS server that will serve as a forwarder for this server.

TIP

If this DNS server is configured to be a root server, the options on this tab are grayed out. You can't configure a root server to use a forwarder.

Once you select the "Enable forwarders" check box on this tab and specify an appropriate IP address, the DNS server that uses the specified IP address automatically becomes a forwarder — no additional configuration on the forwarder is required.

If you configure this server to use a forwarder, the "Do not use recursion" option becomes available. Select this check box if you *don't* want this DNS server to attempt to contact a root server to resolve a DNS query if the forwarder is unable to resolve the query.

I recommend that you select the "Do not use recursion" option because it eliminates fruitless duplication of effort by this DNS server. If the forwarder isn't able to resolve the query, it's unlikely that this server will be able to, either.

Configuring Advanced DNS Server Options The next tab in the DNS server's Properties dialog box is the Advanced tab, which is shown in Figure 7-6.

In addition to displaying the version number of the DNS Server service, this tab offers several configurable server options:

- **Disable recursion:** The term *recursion* refers to repeating a process until a solution is found. By default, recursion is enabled on DNS servers. This means that a DNS server will contact as many other DNS servers as necessary, one after another, to resolve a client DNS query. Selecting the "Disable recursion" option prevents the DNS server from contacting any other DNS servers to resolve a query. If the DNS server does not have the mapping information required to resolve the query, it provides the requesting client with the IP address of the DNS server it *would* have contacted first if recursion were enabled. It's then up to the client computer to contact the referred DNS server in an attempt to resolve the host name.

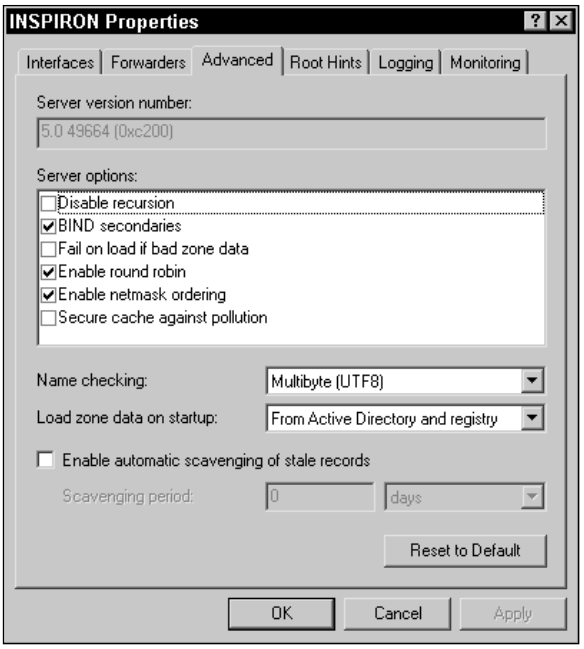

FIGURE 7-6 Configuring advanced options

- **BIND secondaries:** This option, which is selected by default, causes zones to be transferred from master DNS servers to secondary DNS servers by using a fast zone transfer format. If all of your secondary DNS servers are Windows 2000 DNS servers, you should accept the default setting for this option. If some of your secondary DNS servers are not Windows 2000 DNS servers, and if you have been unable to successfully complete zone transfers to any of these servers, consider clearing this check box.
- **Fail on load if bad zone data:** Normally, when the DNS Server service starts, it logs any errors it detects in its zone(s), but continues to use these zones anyway. Selecting this option causes the DNS Server service to log errors that it detects and to *not* use a zone that contains errors. This check box is not selected by default.
- **Enable round robin:** This option, which is selected by default, is a nifty Windows 2000 load balancing feature. The round robin feature is used when multiple servers (such as Web servers) have identical configurations and identical host names, but different IP addresses. The DNS server, when it contains multiple mappings for the same host name, cycles through its list to provide a different IP address to

the requesting client each time the host name is requested, thereby providing load balancing for the requested servers. If this option is deselected, the DNS server responds with the IP address of the first mapping entry in its zone that matches the client's query.

- **Enable netmask ordering:** This option, which is selected by default, determines how a DNS server responds when it receives a query to resolve a host name of a computer that has multiple network adapters. When this option is selected, the DNS server attempts to respond with the associated IP address that is physically located on the same subnet as the client, thus avoiding unnecessary routing traffic. If this option is deselected, the DNS server uses round robin (if enabled) to respond to client queries.
- **Secure cache against pollution:** This option determines how much information gathered by a DNS server (when it must contact multiple DNS servers to resolve a query) is cached for future use. By default, all responses to queries are cached. When this option is selected, only the final answer to the query is cached. This option is not selected by default.

The next configurable option on the Advanced tab is "Name checking." When you manually create a resource record, the DNS server checks the host name contained in this record, and verifies that it meets certain criteria. The drop-down list box contains three name checking methods that the DNS server can use: Strict RFC (ANSI), Non-RFC (ANSI), and Multibyte (UTF8). Multibyte (UTF8) is the default setting, and permits the DNS server to recognize more characters than either of the other two options. I recommend that you accept the default setting, unless you are using other DNS servers on your network that don't support this option.

The next option on this tab is "Load zone data on startup." This option determines where the DNS server will look for its initialization information when the DNS Server service starts. The three options available in the drop-down list box are "From registry," "From file," and "From Active Directory and registry." The default setting is "From Active Directory and registry," and is appropriate for most situations.

The last option on the Advanced tab is "Enable automatic scavenging of stale records." Selecting this option enables scavenging on the DNS server. *Scavenging* is the process of searching for and deleting stale resource records in zones. If you select this option, you can configure an additional option that defines how old a record must be in order to be considered stale. The

default scavenging period is seven days. In addition to enabling scavenging on the DNS server, you must also manually configure scavenging for each zone managed by this DNS server before any scavenging will occur. (I'll discuss how to do this later in the chapter when I explain how to configure a zone for dynamic updates.)

CAUTION

I recommend that you read all of the on-line Windows 2000 Help information on scavenging *before* you implement this feature. If this feature is incorrectly implemented, DNS resource records that you want to keep may be deleted.

Configuring Root Hints The next tab in the DNS server's Properties dialog box is the Root Hints tab, which is shown in Figure 7-7. Notice the server names and IP addresses listed on this tab.

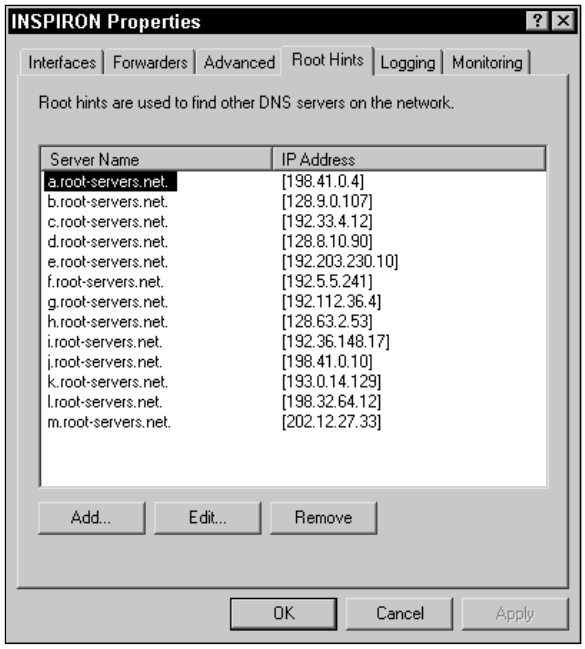

FIGURE 7-7 Root hints

Root hints are server name and IP address combinations that point to root servers located either on the Internet or on your organization's private network. The Root Hints tab contains a list of DNS servers that this DNS server can contact to resolve client DNS queries for host names that reside in another DNS domain.

If a Windows 2000 DNS server is connected to the Internet, its Root Hints tab should be similar to Figure 7-7. Figure 7-7 shows the list of root servers on the Internet.

If a Windows 2000 DNS server is configured to be a root server, the command buttons on the Root Hints tab are grayed out, because a root server doesn't need to contact other root servers.

TIP

You can't configure root hints on a Windows 2000 DNS server that is a root server.

If your Windows 2000 DNS server is *not* configured as a root server, Windows 2000 should have automatically configured root hints when you used the Configure DNS Server Wizard. If root hints are not automatically configured on your Windows 2000 DNS server, or if they are configured incorrectly, you can manually specify the root DNS servers this DNS server should contact. To add, edit, or remove root hints, click the appropriate command button on the Root Hints tab.

There are two remaining tabs in the DNS server's Properties dialog box — Logging and Monitoring. I'll cover both of these tabs later in this chapter when I discuss testing, monitoring, and troubleshooting DNS.

Configuring a Caching-only Server

Once you've installed the DNS Server service on your Windows 2000 Server/Advanced Server computer and configured it to use a root server, your computer is, by default, a caching-only DNS server. The only additional configuration required is to configure client computers to use this DNS server. I'll explain how to configure client computers to use a DNS server a little later in this chapter.

Creating and Configuring Zones

Before you can add resource records to your DNS server, you need to create and configure one or more zones to contain those resource records.

You can create and configure several different types of DNS zones:

- **Forward lookup zone:** This type of zone contains host name to IP address mappings and information about available services for either a DNS domain or a DNS domain and one or more of its subdomains.

- **Reverse lookup zone:** This type of zone contains IP address to host name mappings.
- **Standard primary zone:** This type of zone can be either a forward lookup or reverse lookup zone. In either case, the standard primary zone is the master copy of that zone. All other copies of the standard primary zone are standard secondary zones.
- **Active Directory-integrated zone:** This type of zone can be either a forward lookup or reverse lookup zone. In either case, the Active Directory-integrated zone is the master copy of that zone. However, because Active Directory supports multiple master replication, there can be more than one instance of the Active Directory-integrated zone on different DNS servers. In addition, copies of the Active Directory-integrated zone can be created as standard secondary zones.
- **Standard secondary zone:** This type of zone is a copy of either a standard primary zone or an Active Directory-integrated zone. Standard secondary zones must be created on different DNS servers than the DNS server that contains the master copy of the zone. The purpose of standard secondary zones is to provide load balancing and fault tolerance for the zone.

Zones and DNS domains have an interesting relationship. When you create a standard primary forward lookup zone or an Active Directory-integrated forward lookup zone, you also create (without performing any additional steps) a DNS domain that has the same name as your newly created zone. The new DNS domain is *not* a separate entity from the new zone — in fact, unless subdomains are created within this zone, the new zone and the new DNS domain are one and the same.

The DNS administrative tool contains a handy wizard for creating and configuring zones. It's called the New Zone Wizard, and I'll show you how to use this wizard in the next several sections.

Creating and Configuring a Standard Primary Zone

Creating and configuring a standard primary zone is typically one of the first zone configuration tasks performed when implementing DNS. In the next sections I'll show you how to create a standard primary forward lookup zone, a standard primary reverse lookup zone, and finally, how to configure your newly created standard primary zones.

STEP BY STEP

CREATING A STANDARD PRIMARY FORWARD LOOKUP ZONE

1. Select Start➪ Programs➪ Administrative Tools➪ DNS.
2. In the DNS dialog box, click the + next to the DNS server's name in the left pane.
3. In the left pane, highlight the `Forward Lookup Zones` folder. Select Action➪ New Zone.
4. The New Zone Wizard begins. Click Next.
5. The Zone Type screen appears, as shown in Figure 7-8. Notice the three types of zones you can create.

FIGURE 7-8 Creating a standard primary zone

Also notice that the option next to "Active Directory-integrated" is grayed out—this option is only available *after* you install Active Directory and the DNS Server service on a Windows 2000 Server/Advanced Server computer.

Accept the default option of "Standard primary" and click Next.

6. In the Zone Name screen, type in the name of the zone you are creating. This name is usually the FQDN of the DNS domain that the zone will contain, such as `microsoft.com`. Click Next.
7. The Zone File screen appears. In this screen, you can either create a new zone file for the new zone, or configure the new zone to use an existing file. I recommend you accept the default option of "Create a new file with this file name," and also that you accept the default filename presented. Click Next.

STEP BY STEP *Continued*

8. The Completing the New Zone Wizard screen appears. Click Finish.
9. The DNS dialog box reappears. Notice that the new zone you created appears in the right pane.

After creating a forward lookup zone to resolve host names to IP addresses, you'll probably want to create a reverse lookup zone so that client computers can resolve IP addresses to host names. The following steps explain how to accomplish this.

STEP BY STEP

CREATING A STANDARD PRIMARY REVERSE LOOKUP ZONE

1. Start the DNS administrative tool if it is not already running. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)
2. In the DNS dialog box, click the + next to the DNS server's name in the left pane if this computer is not already expanded.
3. In the left pane, highlight the `Reverse Lookup Zones` folder. Select Action ➪ New Zone.
4. The New Zone Wizard begins. Click Next.
5. The Zone Type screen appears. Accept the default option of "Standard primary" and click Next.
6. The Reverse Lookup Zone screen appears, as shown in Figure 7-9. Notice the two options available on this screen: you can either identify the reverse lookup zone you're creating by network ID, or by typing in a name for the new reverse lookup zone.

   Because it's difficult to construct the correct name for a reverse lookup zone, I recommend that you select the default "Network ID" option and enter the network ID of the zone. This network ID is really the network ID of the subnet for which this reverse lookup zone will provide IP address to host name resolution. Click Next.

CROSS-REFERENCE

For more information on network IDs, subnets, and other TCP/IP issues, see Chapter 16.

STEP BY STEP *Continued*

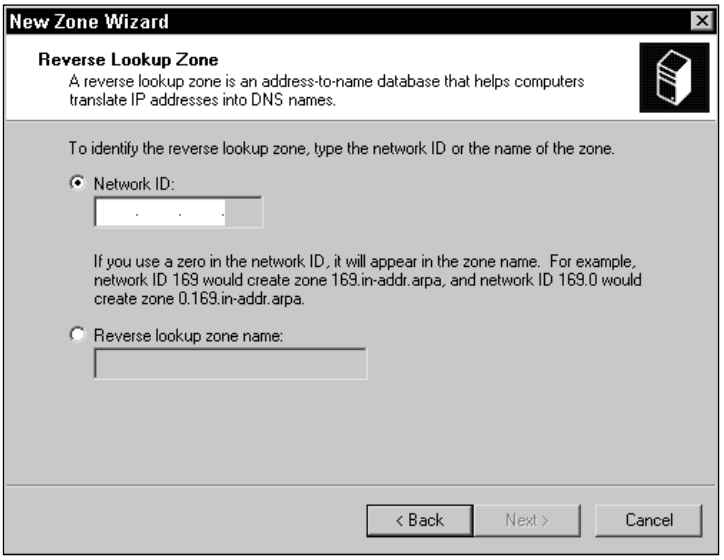

FIGURE 7-9 Creating a reverse lookup zone

7. The Zone File screen appears. In this screen, you can either create a new zone file for the new zone, or configure the new zone to use an existing file. I recommend you accept the default option of "Create a new file with this file name," and also that you accept the default filename presented. Click Next.
8. The Completing the New Zone Wizard screen appears. Click Finish.
9. The DNS dialog box reappears. Notice that the new zone you created appears in the right pane.

Now that you've created your forward lookup and reverse lookup zones, you may want to consider configuring the properties of these zones if the default settings don't meet your needs.

STEP BY STEP

CONFIGURING A STANDARD PRIMARY ZONE (FORWARD LOOKUP OR REVERSE LOOKUP)

1. Start the DNS administrative tool if it is not already running. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)

STEP BY STEP *Continued*

2. In the DNS dialog box, click the + next to the DNS server's name in the left pane if this computer is not already expanded.
3. If you want to configure a forward lookup zone, click the + next to the `Forward Lookup Zones` folder in the left pane.

   If you want to configure a reverse lookup zone, click the + next to the `Reverse Lookup Zones` folder in the left pane.

   In the left pane, highlight the specific zone you want to configure. Select Action ➪ Properties.
4. The zone's Properties dialog box appears, as shown in Figure 7-10. Notice the five tabs in this dialog box.

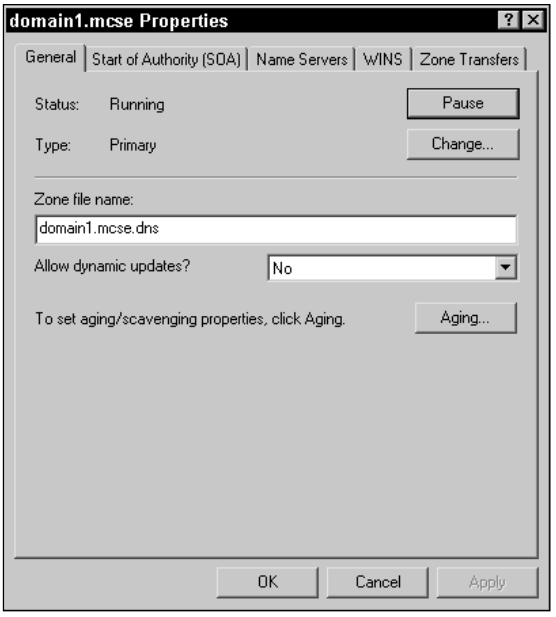

FIGURE 7-10 Configuring a zone

Figure 7-10 shows the zone properties of a standard primary forward lookup zone.

On the General tab, notice that the status of the zone and type of the zone are indicated. You can pause the zone (if it is running), or start the zone (if it is paused) on this tab. You can also change the type of the zone on this tab. (I'll discuss changing zone types in more depth later in this chapter.)

Also notice that the zone filename is displayed on the General tab, and that you can configure the zone to allow dynamic updates. (See the section on "Configuring zones for dynamic updates" later in this chapter for more information.)

Make any appropriate configurations on this tab, and click the Start of Authority (SOA) tab.

STEP BY STEP *Continued*

5. The Start of Authority (SOA) tab appears, as shown in Figure 7-11.

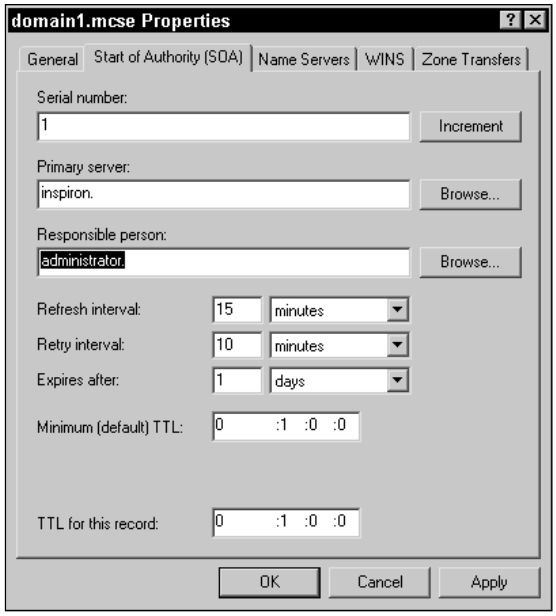

FIGURE 7-11 Configuring a zone's SOA properties

The default settings on this tab are acceptable in most situations, with the exception of the entry in the "Responsible person" text box. (This entry should be the e-mail address of the DNS administrator responsible for maintaining this DNS server.) That said, here are descriptions of the each of the configurable options on the Start of Authority (SOA) tab:

- **Serial number:** This number represents the version number, if you will, of the zone. Each time a resource record is added, modified, or deleted from a zone, the serial number increases by one. Secondary servers use the serial number to determine whether they have the most recent copy of the zone. This number is normally not modified by administrators.
- **Primary server:** This is the host name of this DNS server. This field should not be modified unless you designate a different server to be the standard primary server for this zone.
- **Responsible person:** This field should contain the e-mail address of the administrator responsible for this DNS server. Normally, e-mail addresses contain an @ sign, for example, `alan_carter@usa.net`. In this field, you should *not* use the @ sign—use a period (**.**) instead of the @ sign. The previous e-mail name would be entered in this field as `alan_carter.usa.net`.

STEP BY STEP *Continued*

- **Refresh interval:** This is the amount of time a secondary server waits between attempts to update its copy of the zone.
- **Retry interval:** This is the amount of time a secondary server waits (after a failed attempt to update its copy of the zone) before it tries again. This interval is usually shorter than the refresh interval.
- **Expires after:** This is the amount of time a secondary server will continue to respond to queries for this zone after a successful refresh. If the secondary server is unable to refresh its copy of the zone before this time expires, it will stop responding to client queries for this zone. The interval specified here should be longer than the refresh interval.
- **Minimum (default) TTL:** This field specifies the minimum length of time other DNS servers should cache query results received from this DNS server. Values are entered in this text box in the format *days*:*hours*:*minutes*:*seconds*. As Figure 7-11 shows, the default setting is 0 days, 1 hour, 0 minutes, 0 seconds.
- **TTL for this record:** This field specifies the length of time other DNS servers should cache this DNS server's Start of Authority (SOA) record when they request and receive it. Values are entered in this text box in the same format as the Minimum (default) TTL text box.

Make any appropriate configurations on this tab, and click the Name Servers tab.

6. The Name Servers tab appears, as shown in Figure 7-12.

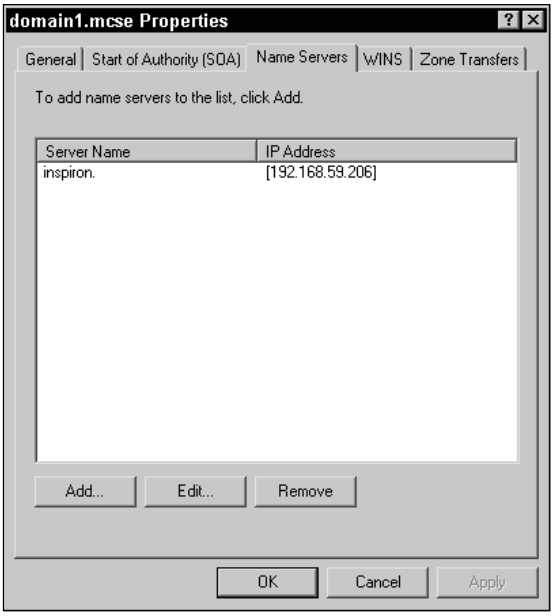

FIGURE 7-12 Configuring a list of DNS servers for the zone

STEP BY STEP *Continued*

This tab shows a list of known DNS servers for this zone. By default, only the primary server for the zone is listed. You must manually add entries for each secondary server for the zone.

Use the Add, Edit, and Remove command buttons on this tab to make any necessary configurations. Then click the WINS tab.

7. The WINS tab appears, as shown in Figure 7-13.

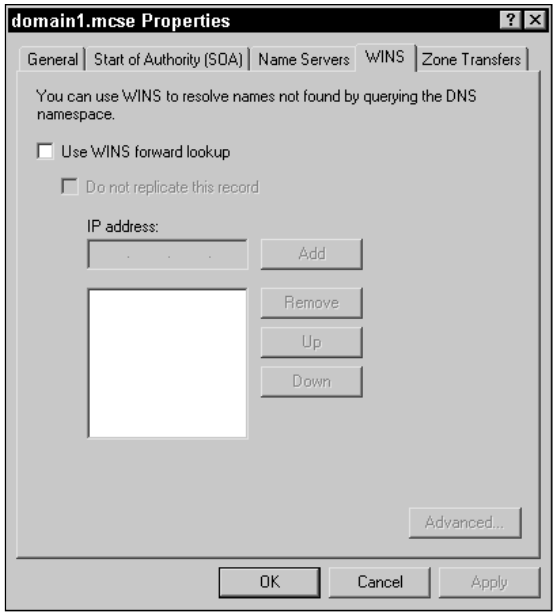

FIGURE 7-13 Enabling WINS lookup

On this tab you can configure the DNS server to query a specified WINS server to resolve host names that the DNS server is unable to resolve by searching the resource records contained in this zone. A WINS server is used to resolve NetBIOS computer names into IP addresses. For more information on WINS, see chapter 16.

TIP

Reverse lookup zones don't have a WINS tab—they have a WINS-R tab. The WINS-R tab is used to configure the DNS server to use a specified WINS server to resolve IP addresses that the DNS server is unable to resolve by searching the resource records in this zone.

To enable WINS lookup, select the check box next to "Use WINS forward lookup" and add the IP address of at least one WINS server that you want this DNS server to use.

STEP BY STEP *Continued*

Make any appropriate configurations on this tab, and click the Zone Transfers tab.

8. The Zone Transfers tab appears, as shown in Figure 7-14.

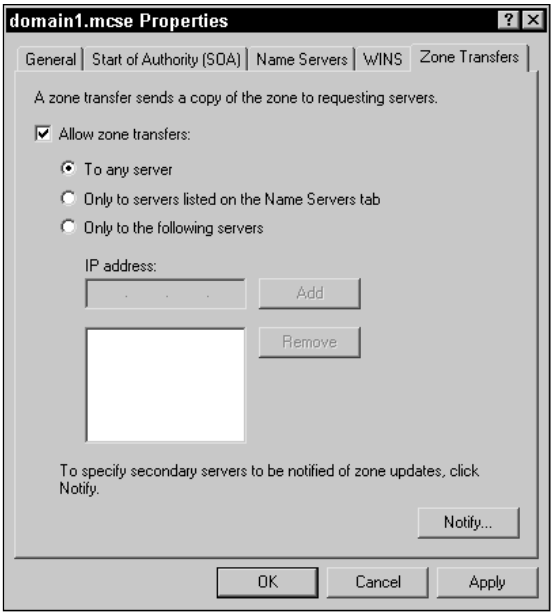

FIGURE 7-14 Configuring zone transfers

The settings on this tab determine how this zone handles the process of copying this zone (in other words, performing *zone transfers*) to secondary servers. By default, the zone is configured to allow zone transfers to any secondary DNS server that requests a copy of the zone. If you want to protect your zone's data, you can configure the zone to only transfer copies of the zone to servers listed on the Name Servers tab, or only to a list of specified servers.

You can also specify which secondary servers will be notified of updates to the zone. This means that when the zone's serial number increases, the specified secondary servers will be notified of the change. By default, all servers listed on the Name Servers tab are notified of updates.

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

Creating and Configuring a Standard Secondary Zone Before you can create a standard secondary zone, you must have first created a standard primary zone on another DNS server. This is important — a standard

secondary zone is created on a *different server* than the DNS server that contains the standard primary zone. In addition, the zone name of a standard secondary zone must match the name of the standard primary zone as it will be copied to the secondary server.

A standard secondary zone can be either a forward lookup or reverse lookup zone.

In the remainder of this section I'll explain how to create and configure a standard secondary zone.

STEP BY STEP

CREATING A STANDARD SECONDARY ZONE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the DNS dialog box, click the + next to the DNS server's name in the left pane.
3. In the left pane, highlight either the `Forward Lookup Zones` or `Reverse Lookup Zones` folder, depending on the type of secondary zone you want to create. Select Action ➪ New Zone.
4. The New Zone Wizard begins. Click Next.
5. The Zone Type screen appears. Select the option next to "Standard secondary" and click Next.
6. If you're creating a standard secondary forward lookup zone, the Zone Name screen appears. On this screen, type the name of the secondary zone you are creating. This zone name *must match* the name of a zone on another DNS server that you want to copy to this DNS server. If you don't know the name of the zone, click Browse and browse for it. Click Next.

   If you're creating a standard secondary reverse lookup zone, the Reverse Lookup Zone screen appears. On this screen, identify the reverse lookup zone either by entering a network ID or by typing in the name of the reverse lookup zone. Click Next.
7. The Master DNS Servers screen appears. In the IP address text box, type the IP address of the DNS server that contains the zone you want to copy to this DNS server. If you don't know the IP address of this server, you can click Browse and browse for it. Click Add. Then click Next.
8. The Completing the New Zone Wizard screen appears. Click Finish.

Once you've created a secondary zone, you can configure it if necessary. Normally, though, configuration of a secondary zone is not required.

The process of configuring a secondary zone is just like configuring a primary zone, except that the Start of Authority (SOA) and Name Servers tabs are grayed out (not configurable) for secondary zones.

Configuring Zones for Dynamic Updates As I mentioned earlier, dynamic update enables client computers and servers to register and update their host names and IP addresses with a DNS server without administrator intervention. Dynamic update is defined and specified in RFC 2136. However, dynamic update is *not* enabled by default on Windows 2000 DNS servers. Dynamic update must be enabled on a zone-by-zone basis.

During the process of configuring a zone for dynamic updates, you have the option to enable and configure scavenging. *Scavenging* is the process of searching for and deleting stale resource records in a zone. Enabling scavenging can help keep a zone from becoming overloaded with stale resource records. Before the advent of dynamic update, it was the administrator's job to manually add and remove resource records as needed. Now, with client computers and servers dynamically registering with a DNS server, scavenging becomes a necessity so that old, outdated resource records are removed from the zone.

STEP BY STEP

CONFIGURING A ZONE FOR DYNAMIC UPDATES

1. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the DNS dialog box, click the + next to the DNS server's name in the left pane. Then, under the DNS server's name, click the + next to the `Forward Lookup Zones` or `Reverse Lookup Zones` folder, depending on the zone you want to configure. In the left pane, highlight the zone you want to configure for dynamic updates, and select Action ➪ Properties.
3. The zone's Properties dialog box appears, as shown in Figure 7-15. Notice the drop-down list box next to "Allow dynamic updates?" Also notice that the default setting for this option is No.

   Select Yes in the "Allow dynamic updates?" drop-down list box.

   If you want to enable and configure scavenging for this zone, click Aging. Otherwise, skip to Step 6.
4. The Zone Aging/Scavenging Properties dialog box appears, as shown in Figure 7-16.

STEP BY STEP *Continued*

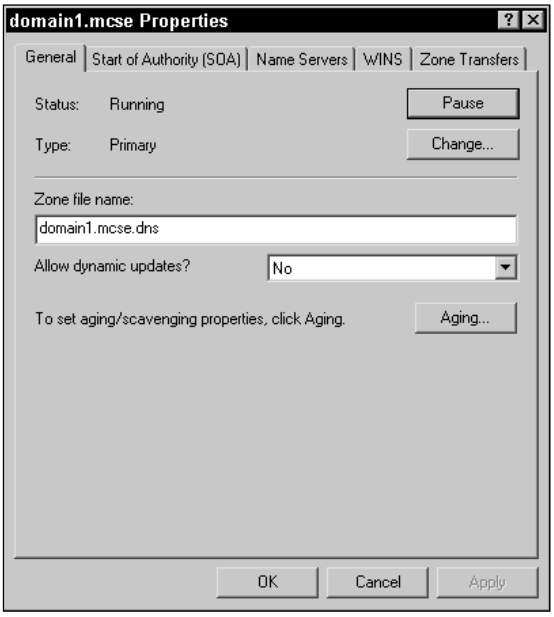

FIGURE 7-15 Configuring a zone for dynamic updates

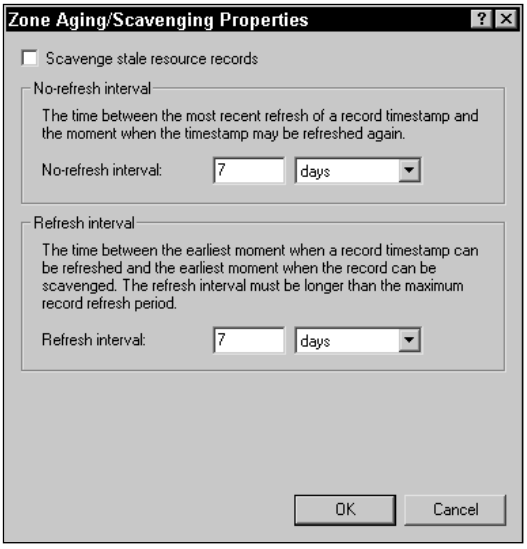

FIGURE 7-16 Configuring scavenging

STEP BY STEP *Continued*

In this dialog box, there are three configuration options:

- **Scavenge stale resource records:** Selecting this check box causes this DNS server to scavenge (search for and delete) stale resource records in the zone. If you select this option, you should configure the other two options to define how old a record must be in order to be considered stale.
- **No-refresh interval:** This option specifies the number of hours or days a client computer of this DNS server must wait, from the time it creates (or refreshes) a record in the zone, until it is permitted to refresh that record. If the record changes during this period, however, the client is permitted to update it. The purpose of limiting refresh frequency is to limit the load on the DNS server.
- **Refresh interval:** This option specifies the amount of time that must elapse, *in addition to* the amount of time specified for the no-refresh interval, before the DNS server is permitted to scavenge the record. The client computer is permitted to refresh the record during this time.

TIP

When a client computer refreshes a record, the timestamp on the record is updated, and the no-refresh interval begins again.

Microsoft recommends that you set the refresh interval to the same length of time as the no-refresh interval. The default time interval for both options is seven days.

Select and/or configure the appropriate options. Click OK.

5. If you are configuring a standard primary zone for dynamic updates and you enabled scavenging, a DNS warning dialog box appears. Click Yes to continue.
6. The zone's Properties dialog box reappears. Click OK.

Converting a Standard Primary Zone to an Active Directory-integrated Zone

When Active Directory is installed on a Windows 2000 Server (or Advanced Server) computer, that computer becomes a domain controller. After you install Active Directory on a Windows 2000 Server/Advanced Server computer that has the DNS Server service installed, you might want to consider converting the server's standard primary zone to an Active Directory-integrated zone. Although this conversion is not mandatory, there are several advantages to converting to an Active Directory-integrated zone:

- **Increased performance of DNS server:** Because resource records in an Active Directory-integrated zone are stored in a

database, rather than in a text file (as is the case in a standard primary zone), the DNS Server service can respond faster to client DNS queries. Query performance is increased because it's faster to search a database than a text file.

- **No need to use secondary servers:** When Active Directory-integrated zones are used, DNS resource records are stored in the Active Directory data store, and Active Directory replicates these resource records to all other domain controllers in the domain. Because of this, DNS servers that are also domain controllers automatically receive a copy of all Active Directory-integrated zones. Because Active Directory is performing the replication, it's not necessary to create secondary servers that will initiate zone transfers.
- **More masters available for updates:** Because Active Directory supports multiple master replication, each DNS server/domain controller that receives a copy of an Active Directory-integrated zone can accept updates for that zone.

The steps that follow explain how to convert a standard primary zone to an Active Directory-integrated zone after Active Directory has been installed. You can also use this same basic set of steps to change a zone's type for any other reason.

STEP BY STEP

CHANGING A ZONE TYPE: CONVERTING TO AN ACTIVE DIRECTORY-INTEGRATED ZONE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the left pane of the DNS dialog box, click the + next to the name of the DNS server that contains the zone you want to change. Then, under this computer's name, click the + next to the `Forward Lookup Zones` or `Reverse Lookup Zones` folder, depending on the zone you want to change. In the left pane, highlight the zone you want to change, and select Action ➪ Properties.
3. The zone's Properties dialog box appears. Click Change.
4. The Change Zone Type dialog box appears, as shown in Figure 7-17. Notice the three zone types you can select in this dialog box: Active Directory-integrated, standard primary, and standard secondary.

STEP BY STEP *Continued*

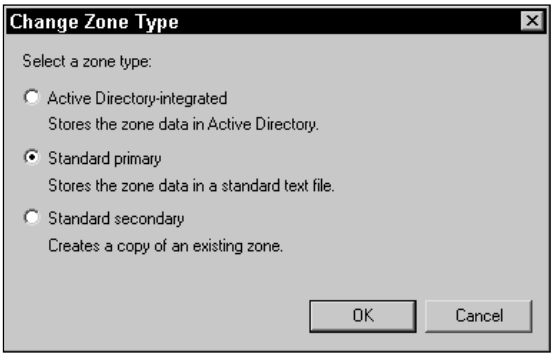

FIGURE 7-17 Changing a zone type

Select the "Active Directory-integrated" option, and click OK.

5. When a DNS warning message appears, asking if you're sure you want this zone to become an Active Directory-integrated primary zone, click OK.
6. In the zone's Properties dialog box, click OK.

Integrating an Active Directory DNS with a Non–Active Directory DNS

In today's mixed networks, it's not too uncommon to have an Active Directory-integrated DNS server on the same network as a non–Active Directory DNS server. The non–Active Directory DNS server may run Windows 2000, or it may run UNIX or any other operating system that supports DNS servers. As long as the non–Active Directory DNS server supports SRV (service) resource records, you can configure it to integrate with the Active Directory-integrated DNS server.

When a non–Active Directory DNS server is configured to integrate with an Active Directory-integrated DNS server, the non–Active Directory DNS server will maintain a secondary copy of one or more zones from the Active Directory-integrated DNS server. The non–Active Directory DNS server will then be able to respond to client queries for host name resolution in the zone(s) it has received from the Active Directory-integrated DNS server.

To configure a non–Active Directory DNS server to integrate with an Active Directory-integrated DNS server, you need to create a standard secondary zone on the non–Active Directory DNS server. When you

create this secondary zone, you must assign it the same name as the Active Directory-integrated zone, and specify the IP address of the Active Directory-integrated DNS server.

TIP

If you want the non–Active Directory DNS server to maintain a copy of *more than one* Active Directory-integrated zone, you must create a secondary zone for *each* Active Directory-integrated zone that you want the server to maintain a copy of.

The actual steps involved in creating and configuring a secondary zone on a non–Active Directory DNS server vary depending on the operating system and type of DNS server software being used. To create a secondary zone on a Windows 2000 DNS server, see the step-by-step section earlier in this chapter titled "Creating a standard secondary zone."

Managing Replication of DNS

As I mentioned earlier, Microsoft sometimes refers to zone transfers as *replication*. DNS replication tasks don't normally require much administrative time, but there are a few considerations to take into account.

The easiest way to manage replication of DNS data on a Windows 2000 network is to simply let Active Directory do the replicating. To do this, all DNS servers need to be installed on Windows 2000 Server/Advanced Server domain controllers, and all zones need to be Active Directory-integrated zones. In this scenario, Active Directory automatically manages the replication of all DNS zones and their resource records.

If you choose to *not* use Active Directory or to not use Active Directory-integrated zones, you can implement replication of zone data by creating secondary servers. Once you've implemented replication, there are a few DNS configuration options to help you manage zone transfers.

One way you can manage replication is by configuring the properties of the zone. For example, suppose that you want to protect the data in a standard primary zone so that it can only be replicated to secondary servers that you specify. By default, standard primary zones are configured to allow zone transfers to any server. So, in order to restrict zone transfers to specific servers, you'll need to select the "Only to the following servers" option and then specify the IP addresses of the secondary servers you want the standard primary zone to allow zone transfers to. This configuration is made on the Zone

Transfers tab in the standard primary zone's Properties dialog box. (See the "Configuring a standard primary zone" section earlier in this chapter for details on how to perform this task.) Figure 7-18 shows the Zone Transfers tab after it has been configured to limit zone transfers to a specified list of DNS servers.

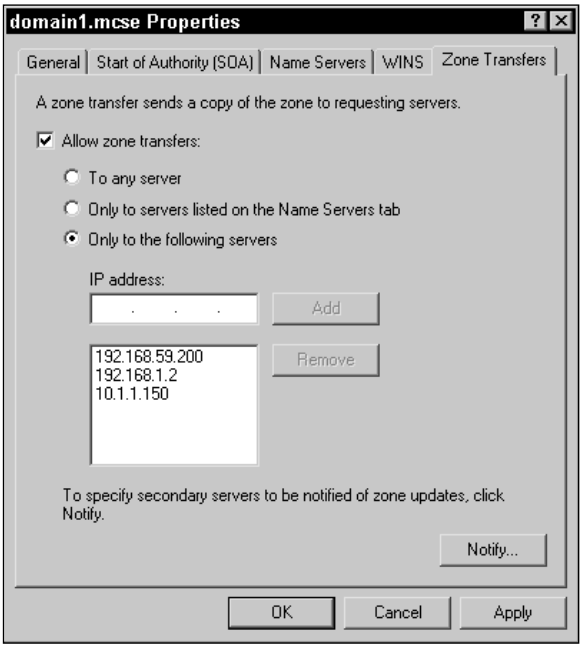

FIGURE 7-18 Limiting zone transfers

You might also want to configure notification of secondary servers so that they will request a zone transfer immediately after updates are made to the standard primary zone. To do this, you can click Notify on the Zone Transfers tab in the standard primary zone's Properties dialog box. After you click Notify, you can specify the IP addresses of the secondary servers that will be notified of zone updates. Figure 7-19 shows the Notify dialog box after it has been configured to automatically notify a specified list of secondary DNS servers of an update to the zone.

If your network structure requires it, you can make these same types of configurations to secondary servers to specify the additional secondary servers they are allowed to make zone transfers to, or the additional secondary servers they will notify of updates to the zone.

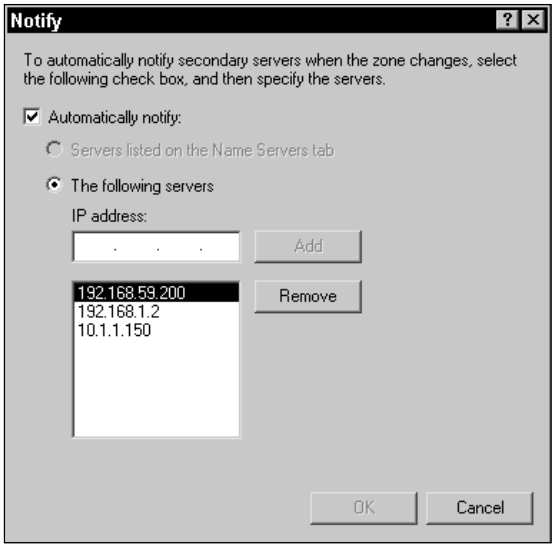

FIGURE 7-19 Configuring notification of secondary servers

Another way to manage replication is by configuring the properties of the DNS server. For example, if you have secondary servers that don't support the fast zone transfer format, such as older DNS servers or non-Windows 2000 DNS servers, you should consider configuring the properties of the primary (or secondary) DNS server that is replicating to the secondary servers that don't support the fast zone transfer format. To do this, in the server's Properties dialog box, clear the "BIND secondaries" check box on the Advanced tab. (See Figure 7-6 and the "Configuring advanced DNS server options" section earlier in this chapter for details on how to perform this task.)

Manually Creating DNS Resource Records

At one time or another, you'll probably have to manually create DNS resource records. Although the Windows 2000 DNS Server service supports dynamic update of many types of DNS resource records, some types of computers don't support dynamic update and some types of resource records can't be dynamically created.

You can manually create DNS resource records only in standard primary zones and in Active Directory-integrated zones. In other words, you can't add resource records to secondary zones.

DNS servers support a wide variety of resource record types. Each type of resource record has a different purpose. Table 7-2 lists and describes the types of resource records supported by the Windows 2000 DNS Server service.

TABLE 7-2 Windows 2000 DNS Resource Record Types

Record Type	Description
A	Standard host name resource record. Contains host name to IP address mapping.
AAAA	Host name resource record used when IPv6 is used on a network.
AFSDB	Andrew File System Database (AFSDB) resource record. Identifies servers that support this file system and specific server subtypes.
ATMA	Asynchronous Transfer Mode (ATM) address resource record. Used to map DNS names to ATM addresses.
CNAME	Alias resource record. Used to map an additional host name (that is, an alias) to the actual name of the host.
HINFO	Host information resource record. Used to specify information about a host, such as CPU type and operating system type.
ISDN	Integrated Services Digital Network (ISDN) resource record. Used to map DNS names to ISDN telephone numbers.
MB	Mailbox resource record. Used to map an e-mail address to a specific host name.
MG	Mail group resource record. Used to specify a list of mailbox records that are members of a mail group.
MINFO	Mailbox mail list information (MINFO) resource record. Used to specify a mailbox that will receive error messages for another specified mailbox. Also used to specify the mailbox of the Responsible Person (RP) for the specified mailbox.
MR	Mailbox renamed resource record. Used to map an old mailbox name to its new name.
MX	Mail exchanger resource record. Used to map a DNS domain name to the host name of the mail server for that domain.
PTR	Pointer (PTR) resource record. Used to map IP addresses to their associated host names. These records are only used in reverse lookup zones.
RP	Responsible Person (RP) resource record. Used to specify the e-mail address of the Responsible Person (RP) for a DNS domain.
RT	Route through (RT) resource record. Used to specify routing information for specific DNS domain names.

Record Type	Description
SRV	Service locator (SRV) resource record. Used to map a specific service (or TCP/IP port number) to a list of servers that provide that service.
TXT	Text (TXT) resource record. Used to map a DNS name to a string of descriptive text.
WKS	Well-known service (WKS) resource record. Used to map a host name to the specific list of well-known services that host supports.
X25	X.25 resource record. Used to map a host name to an X.25 address.

Now that you have a good understanding of the different types of DNS resource records, I'll show you how to manually create DNS resource records.

STEP BY STEP

MANUALLY CREATING DNS RESOURCE RECORDS

1. Start the DNS administrative tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)
2. In the left pane of the DNS dialog box, click the + next to the name of the DNS server.
3. In the left pane, click the + next to the `Forward Lookup Zones` folder or the `Reverse Lookup Zones` folder, depending on the type of zone you want to add a resource record to. In the left pane, highlight the specific zone you want to add a resource record to. Select one of the following commands, depending on the type of resource record you want to add:
   - ► Action ➪ New Host
   - ► Action ➪ New Alias
   - ► Action ➪ New Mail Exchanger
   - ► Action ➪ New Pointer (only available on reverse lookup zones)
   - ► Action ➪ Other New Records

   Probably the most common type of resource record created is a new host record. If you selected any command other than Action ➪ New Host, follow the directions presented on-screen to create your new record. Otherwise, continue to Step 4.
4. The New Host dialog box appears, as shown in Figure 7-20. Notice that when you create a new record you can also create an associated pointer (reverse lookup) record at the same time.

STEP BY STEP *Continued*

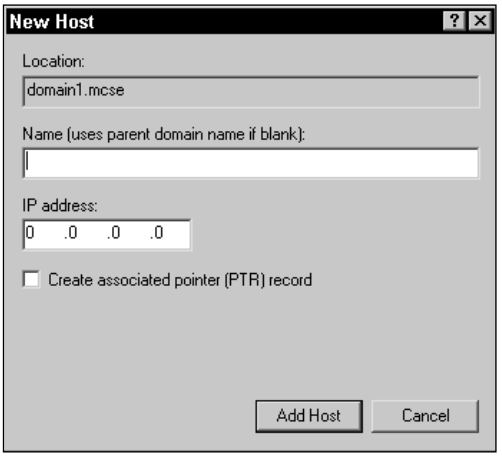

FIGURE 7-20 Creating a new host resource record

In the Name text box, type the name of the host you want to add a record for. Then, in the IP address box, type the IP address of the host.

Finally, if you want to create an associated pointer (reverse lookup) record, select the check box next to "Create associated pointer (PTR) record."

Click Add Host.

5. A DNS message appears, indicating that the host record was successfully created. Click OK.
6. Repeat Steps 4 and 5 until you have added all of the new host records you need. Then, in the New Host dialog box, click Done.

Creating DNS Subdomains and Implementing Zone Delegation

Some organizations are so large that administrators find it easier to break their second-level domain (such as `microsoft.com`) into multiple DNS subdomains (such as `marketing.microsoft.com`, `development.microsoft.com`, and so on). There are two possible approaches to implementing DNS subdomains in this type of situation.

The first way is to create the DNS subdomains within the zone that contains the second-level domain. This method is called "creating subdomains." You can create DNS subdomains within standard primary and Active Directory-integrated zones.

The second way involves creating new zones and is called "creating delegated zones." This process involves two steps: first, you create a new standard primary or Active Directory-integrated zone to implement each new subdomain; and second, you configure zone delegation for each of the newly created zones. The key point to remember about delegation is that it must be performed on the standard primary or Active Directory-integrated zone *that contains the parent domain* of the new DNS subdomain(s). For example, suppose that I create two new zones to implement two new subdomains (for example, `marketing.microsoft.com` and `development.microsoft.com`). I then need to configure delegation for the two new zones on the standard primary or Active Directory-integrated zone that contains the `microsoft.com` domain.

TIP

If you create the zones for the new subdomains on the Windows 2000 DNS server that contains the standard primary or Active Directory-integrated zone for the parent domain, delegation is automatically configured by Windows 2000, and you can skip that part of the process.

Now I'll explain how to implement the first approach to implementing DNS subdomains: creating a new subdomain within a zone.

STEP BY STEP

CREATING A NEW SUBDOMAIN

1. Start the DNS administrative tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)
2. In the left pane of the DNS dialog box, click the + next to the name of the DNS server that contains the standard primary or Active Directory-integrated zone for the DNS domain in which you want to create a subdomain.
3. In the left pane, click the + next to the `Forward Lookup Zones` folder (under the DNS server that you just expanded). In the left pane, highlight the specific zone you want to add a subdomain to. Select Action ➪ New Domain.
4. The New Domain dialog box appears. Type in the name of the new subdomain, for example, *subdomain* and click OK.
5. When the DNS dialog box reappears, the new subdomain appears in the right pane as a folder within the zone.

In the next section I'll explain how to create and delegate a new zone for a new subdomain. Remember, if you create the zones for the new subdomains on the Windows 2000 DNS server that contains the standard primary or Active Directory-integrated zone for the parent domain, delegation is automatically configured by Windows 2000, and you can skip the steps in Part 2 of this process.

STEP BY STEP

CREATING THE ZONE

1. Start the DNS administrative tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)
2. In the left pane of the DNS dialog box, click the + next to the name of the DNS server on which you want to create the new zone.
3. In the left pane, highlight the `Forward Lookup Zones` folder (under the DNS server that you just expanded). Select Action ➪ New Zone.
4. The New Zone Wizard begins. Click Next.
5. In the Zone Type screen, select the "Standard primary" or "Active Directory-integrated" option, depending on your needs and your network configuration. Click Next.
6. In the Zone Name screen, type the name of the zone. This should be the FQDN of the new DNS subdomain, such as `marketing.microsoft.com`. Click Next.
7. In The Zone File screen, accept the default options and click Next.
8. In the Completing the New Zone Wizard screen, click Finish.

DELEGATING THE NEW ZONE

1. Start the DNS administrative tool if it is not already running. (Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.)
2. In the left pane, click the + next to the name of the DNS server that contains the standard primary or Active Directory-integrated zone that contains the parent domain of the subdomain you just created.
3. In the left pane, click the + next to the `Forward Lookup Zones` folder. In the left pane, highlight the parent domain. Select Action ➪ New Delegation.
4. The New Delegation Wizard begins. Click Next.
5. The Delegated Domain Name screen appears. In the "Delegated domain" text box, type the name of the subdomain, for example, marketing. Click Next.

STEP BY STEP *Continued*

6. The Name Servers screen appears. On this screen, specify the names and associated IP addresses of all DNS servers you plan to configure to maintain a copy of the zone you created in Part 1. The list you create here is a DNS referral list that this DNS server will use to refer other DNS servers attempting to resolve names in the new, delegated zone.

TIP

Listing servers here does *not* cause a copy of the zone to be automatically replicated to these DNS servers—you'll have to configure these servers as secondary servers (or as Active Directory-integrated servers) in order for them to receive a copy of the zone.

You must add at least one server name and IP address to this screen in order to continue. To add a server name and IP address to the list, click Add.

7. The New Resource Record dialog box appears. In the Server name text box, type the name of the server you want to add. In the IP address box, type the IP address of the server you want to add. Click Add. Click OK.
8. Repeat Steps 6 and 7 until you are finished adding server names and IP addresses. Figure 7-21 shows the Name Servers screen after server names and IP addresses have been added. Click Next.

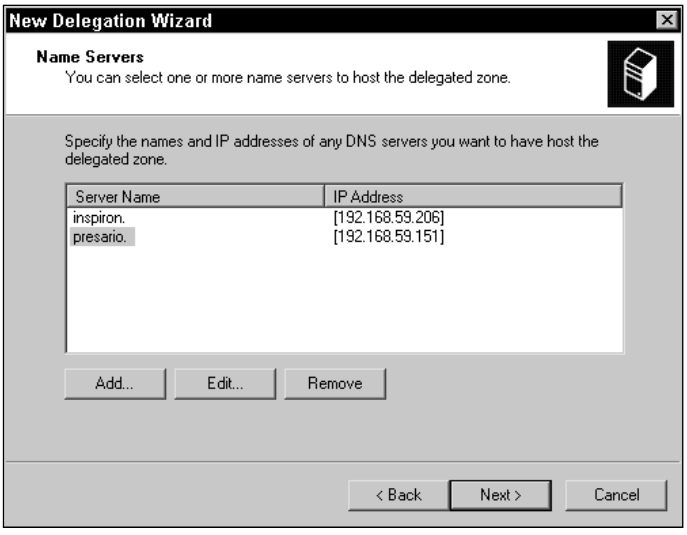

FIGURE 7-21 Specifying DNS servers for the delegated zone

9. In the Completing the New Delegation Wizard screen, click Finish.

Configuring Clients to Use a DNS Server

Before client computers can use a DNS server, they must be configured to do so. Specifically, client computers must be configured with the IP address(es) of the DNS server(s) they will use.

The following steps explain how to configure a Windows 2000 computer to be a client of a DNS server.

STEP BY STEP

CONFIGURING A WINDOWS 2000 COMPUTER TO USE A DNS SERVER

1. From the desktop, select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the `Network and Dial-up Connections` folder.
3. In the `Network and Dial-up Connections` folder, right-click Local Area Connection and select Properties from the menu that appears.

TIP

If you have more than one Local Area Connection, you'll have to repeat this process for each one.

4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, ensure that the "Use the following DNS server addresses" option is selected. Then, in the Preferred DNS server text box, type the IP address of the DNS server you want this computer to use. You can also specify, in the "Alternate DNS server" text box, an IP address of an alternate DNS server that this computer will use if the preferred DNS server is not available. Click Advanced.
6. In the Advanced TCP/IP Settings dialog box, click the DNS tab.
7. On the DNS tab, type the FQDN of the DNS domain that the computer you're configuring belongs to in the "DNS suffix for this connection" text box. Generally you can accept the remaining default settings on this tab. Click OK.
8. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
9. In the Local Area Connection Properties dialog box, click OK.
10. Close the `Network and Dial-up Connections` folder.

Installing DNS for Active Directory

If you're installing DNS in preparation for installing Active Directory, you should ensure that the following tasks are performed prior to the Active Directory installation:

- The DNS Server service should be installed on a Windows 2000 Server/Advanced Server computer.
- A forward lookup zone must be created on the DNS server. In addition, I recommend that you also create a reverse lookup zone on this server.
- All zones that will be used by Active Directory should be configured for dynamic updates.
- The Windows 2000 Server/Advanced Server computer that Active Directory will be installed on (this can be either the DNS server or another computer) must be configured to be a client of the DNS server.

For details on how to perform any of these tasks, see the earlier sections in this chapter.

Testing, Monitoring, and Troubleshooting DNS

Once your DNS server(s) and clients are up and running, you may want to do some periodic testing and monitoring to make sure that all components are functioning properly. You may also need to troubleshoot DNS operations and events from time to time. In this section, I'll explore some tools you can use to perform these tasks.

Using the Monitoring Tab to Test and Monitor DNS

You can use the Monitoring tab in your DNS server's Properties dialog box to test and monitor your DNS server. You can also use this tab to verify your DNS installation.

To access the Monitoring tab, select Start ➪ Programs ➪ Administrative Tools ➪ DNS. Then, in the DNS dialog box, highlight the name of the DNS server you want to test or monitor. Then select Action ➪ Properties. Finally, in the DNS server's Properties dialog box, click the Monitoring tab.

The Monitoring tab appears, as shown in Figure 7-22. Notice the types of testing that you can configure on this tab. Also notice that monitoring is *not* configured, by default.

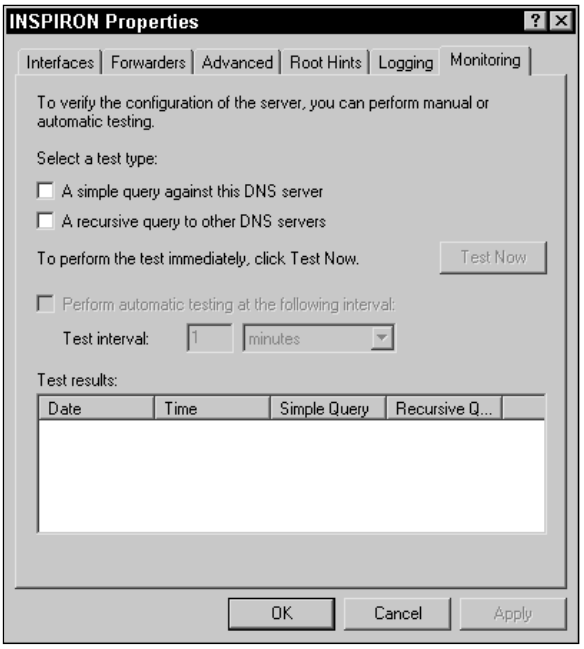

FIGURE 7-22 The Monitoring tab

There are two types of tests that you can configure on the Monitoring tab: a simple query, and a recursive query. A *simple query* is a query that this DNS server can resolve without contacting any other DNS servers. In other words, it's a query for a resource record in one of the zones that this DNS server contains. If you select the check box next to "A simple query against this DNS server" and then click Test Now, you'll be instructing your DNS server to immediately test itself to see if it can resolve a standard client DNS query.

The results of this test are displayed in the Test results box at the bottom of the Monitoring tab. If a PASS result is displayed, this indicates that the DNS Server service was successfully installed on the computer, and that this DNS server can resolve queries. Instead of clicking Test Now, you can configure the DNS server to automatically perform the simple query test at the intervals you specify. This type of testing can be useful for monitoring your DNS server.

A *recursive query* is a query that this DNS server can't resolve by itself—it must contact one or more additional DNS servers to resolve the query. If you select the check box next to "A recursive query to other DNS servers" and then click Test Now, you'll be instructing your DNS server to immediately query another DNS server in an attempt to resolve the query. The results of this test are displayed in the Test results box at the bottom of the Monitoring tab. Or, instead of clicking Test Now, you can configure the DNS server to automatically perform this test at the intervals you specify. This type of testing can also be useful for monitoring your DNS server.

Troubleshooting DNS

There are several tools you can use when you need to troubleshoot a DNS problem, including the Monitoring tab, `Nslookup.exe`, the DNS Server log in Event Viewer, Windows 2000 Help, and the Logging tab. I'll discuss each of these resources in the sections that follow.

Using the Monitoring Tab

You can use the Monitoring tab in a DNS server's Properties dialog box to determine whether the DNS server can resolve a query, as explained in the previous section.

Using Nslookup.exe

You can use the `Nslookup.exe` command-line utility to test whether a DNS server can resolve various types of queries. This is probably the most common tool for troubleshooting DNS.

STEP BY STEP

USING NSLOOKUP.EXE

1. From the desktop, select Start ➪ Programs ➪ Accessories ➪ Command Prompt.
2. Maximize the Command Prompt dialog box when it appears.
3. At the command prompt, type **nslookup** and press Enter.
4. `Nslookup.exe` displays the name and IP address of the default DNS server for this computer. (If you run `Nslookup.exe` on a DNS server, it will probably display its own name and IP address.)
5. To use `Nslookup.exe` to test name resolution on your DNS server, type the FQDN of a host in a zone on your DNS server, for example, *host_name.your_domain.com,* and press Enter.

STEP BY STEP *Continued*

6. If the DNS server is functioning correctly, `Nslookup.exe` should display the name and IP address of the DNS server resolving the query (this may be itself) and the name and IP address of the specified host.

   If `Nslookup.exe` displays a message that it can't find a specified FQDN or that a nonexistent domain was specified, retry your query, carefully checking your typing, and making sure that you are attempting to resolve a host that is located on this server.

7. To obtain detailed information on the syntax for using `Nslookup.exe` to perform specific queries, type **help** at the prompt and press Enter. Figure 7-23 shows the results of running the help command in `Nslookup.exe`.

FIGURE 7-23 Nslookup.exe help

8. When you're finished using `Nslookup.exe`, type **exit** and press Enter to close `Nslookup.exe`. Then type **exit** and press Enter to close the Command Prompt.

Using the DNS Server Log Another DNS troubleshooting tool is the DNS Server log in Event Viewer. You can use this tool to view event detail about DNS Server service events. Sometimes the detailed information displayed can be useful for troubleshooting DNS problems.

STEP BY STEP

USING THE DNS SERVER LOG IN EVENT VIEWER

1. From the desktop, select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.
2. In the left pane of the Event Viewer dialog box, highlight the DNS Server log. The DNS Server log is displayed in the right pane, as shown in Figure 7-24.

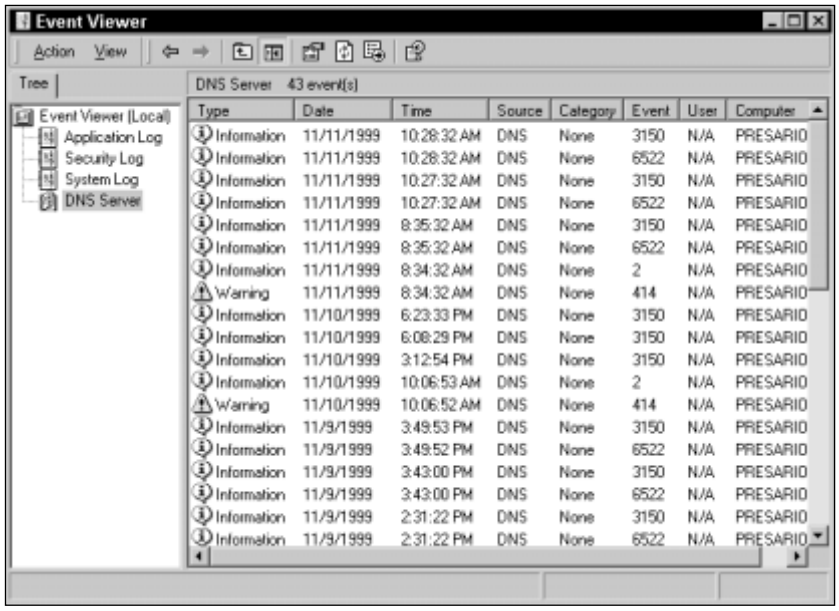

FIGURE 7-24 The DNS Server log

To view the detail on a specific DNS event, double-click that event in the right pane.

3. The Event Properties dialog box is displayed, as shown in Figure 7-25. Notice the detailed description of the DNS event and possible solutions listed.

STEP BY STEP *Continued*

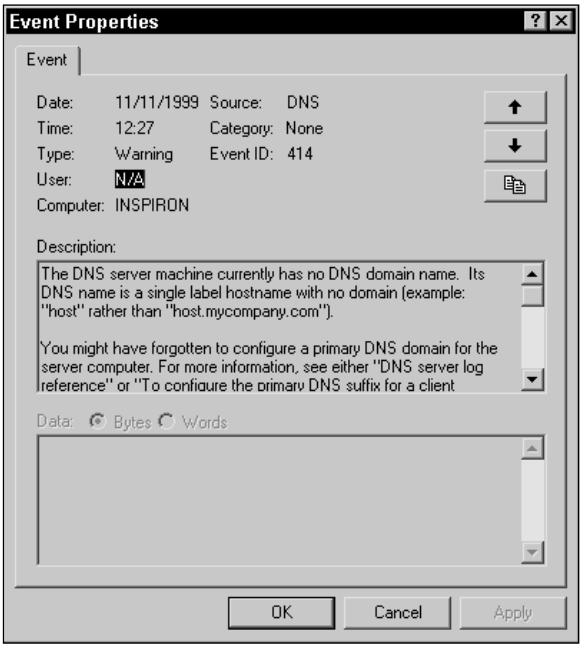

FIGURE 7-25 Viewing DNS event detail

Also notice the up arrow and down arrow in this dialog box. You can use these buttons to view event detail for other events in the list. When you're finished viewing event details, click OK.

4. Close Event Viewer.

Using Windows 2000 Help You can also use Windows 2000 Help to obtain a wealth of information on common DNS problems. Windows 2000 Help is a good troubleshooting resource because it contains detailed descriptions of many specific DNS problems and recommended solutions to these problems.

STEP BY STEP

USING WINDOWS 2000 HELP TO LOCATE DNS TROUBLESHOOTING INFORMATION

1. From the desktop, select Start ➪ Help.
2. Click the Contents tab if it does not appear on top.

STEP BY STEP *Continued*

3. On the Contents tab, double-click Networking.
4. In the list that appears under Networking, double-click DNS.
5. In the list that appears under DNS, double-click Troubleshooting. Figure 7-26 shows the DNS Troubleshooting section in Windows 2000 Help. Notice the various DNS troubleshooting topics listed.

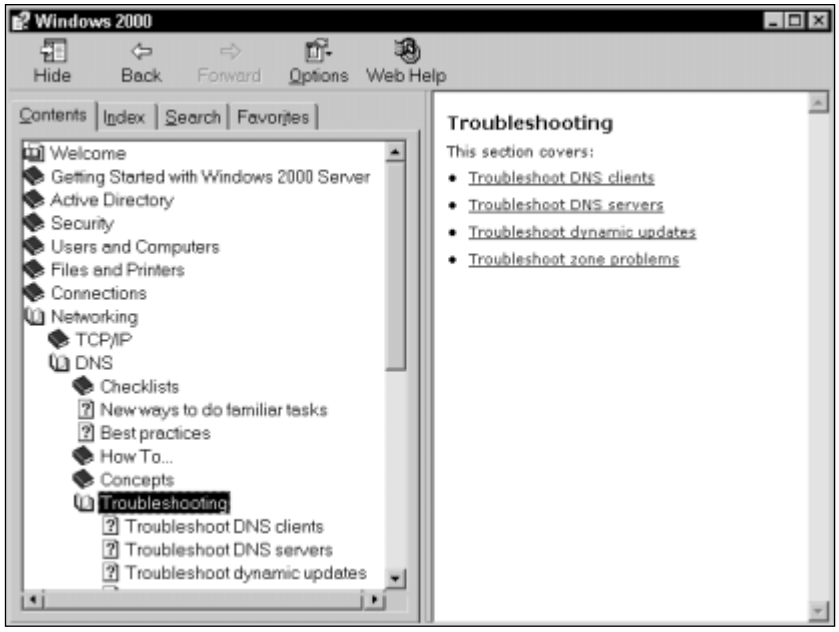

FIGURE 7-26 DNS troubleshooting topics

To access any of the topics listed, click the topic in the *right* pane.

6. When you are finished using Windows 2000 Help, close the Windows 2000 dialog box.

Using the Logging Tab Finally, you can use the Logging tab in a DNS server's Properties dialog box to create detailed logs of DNS activity. These logs can be particularly helpful when troubleshooting DNS. By default, logging is *not* enabled on a Windows 2000 DNS server.

To access the Logging tab, select Start ➪ Programs ➪ Administrative Tools ➪ DNS. Then, in the DNS dialog box, highlight the name of the DNS server for which you want to configure logging. Then select Action ➪ Properties. Finally, in the DNS server's Properties dialog box, click the Logging tab.

The Logging tab appears, as shown in Figure 7-27. Notice the various logging options, and that none of these options are selected by default.

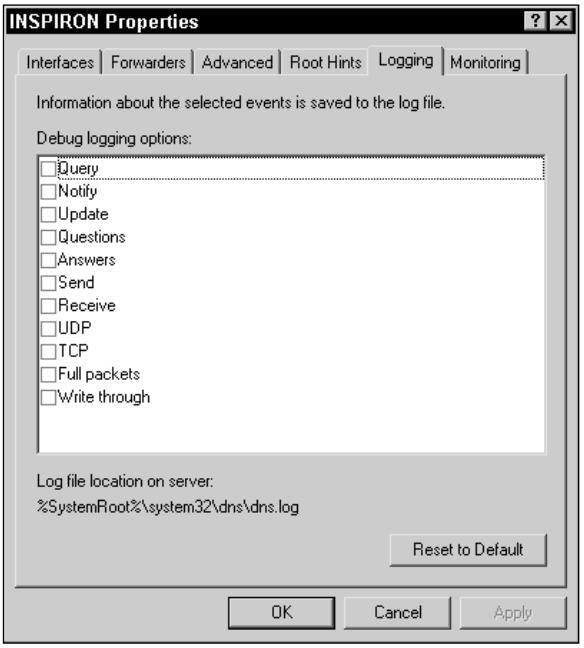

FIGURE 7-27 Enabling logging

Also notice, in Figure 7-27, the location of the log file. The DNS log file is stored as `%SystemRoot%\system32\dns\dns.log`. (Remember that `SystemRoot` represents the folder that Windows 2000 is installed in.)

Each of the logging options on the Logging tab represents a specific type of DNS event. For example, selecting the check box next to Query causes each query received to be logged. Likewise, selecting the check box next to Update causes each resource record update request received to be logged.

To enable logging, select the check box(es) next to the events you want logged, and click OK. To view the log file after logging has been enabled, use Notepad to open the `%SystemRoot%\system32\dns\dns.log` file.

Installing Active Directory

Now that you have a good understanding of DNS, you're ready to move on to installing Active Directory. You can run Windows 2000 without ever installing Active Directory, but if you do so, you'll miss out on most of the benefits of using Windows 2000.

Active Directory can be installed on any Windows 2000 Server or Advanced Server computer. Like DNS, Active Directory is not supported on Windows 2000 Professional computers.

There are a couple of prerequisites that must be met prior to installing Active Directory:

- At least one volume on the Windows 2000 Server/Advanced Server computer must be formatted with NTFS.
- Because Active Directory requires DNS, you either need to have a DNS server installed on your network prior to installing Active Directory, or you can choose to install DNS at the same time that you perform the Active Directory installation. (If you install DNS before installing Active Directory, see the "Installing DNS for Active Directory" section earlier in this chapter for specific requirements.)

Another fact to consider when preparing to install Active Directory is that any computer that you install Active Directory on will become a domain controller. Because domain controllers provide extensive network services, you'll probably want to make sure this computer is reliable and powerful enough to handle the extra load. You should also consider the services and functions currently being performed by this computer. For example, if a computer is already a SQL server, an Exchange server, or a heavily used Web server, you may decide not to increase the burden on this computer by installing Active Directory.

Finally, before you charge right off and install Active Directory, ensure that you've taken the time to learn how Active Directory is implemented, planned your domain design (including domain structure, organizational unit structure, and the upgrade of previous domains), decided on the naming conventions you will use, and determined how client computers will fit into your overall Windows 2000 Active Directory implementation plan.

CROSS-REFERENCE

See Chapter 2 for detailed information on how Active Directory is implemented and for practical tips on planning for Active Directory on your network.

Windows 2000 includes a wizard that helps you install Active Directory, called the Active Directory Installation Wizard. There are two ways to start this wizard:

- From the desktop, select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.
- From the desktop, select Start ➪ Programs ➪ Administrative Tools ➪ Configure Your Server. Then, in the Windows 2000 Configure Your Server dialog box, click the Active Directory link. On the Active Directory page, scroll down and click Start the Active Directory wizard.

In the next several sections, I'll show you how to install Active Directory. Because the installation steps vary depending on the computer's role in Active Directory and your network configuration, I'll try to cover the most common installation scenarios you'll encounter.

Installing Active Directory for the First Time

This section explains how to install Active Directory for the *first* time on your network.

When Active Directory is installed for the first time, the following events take place:

- The computer on which Active Directory is installed becomes a domain controller for a new Windows 2000 domain.
- The Active Directory Installation Wizard creates the new Windows 2000 domain, using the domain name you specify in the process.
- The Active Directory Installation Wizard creates a new domain tree and forest.

In the steps that follow I'll show you how to perform your first Active Directory installation.

CAUTION

The Active Directory Installation Wizard requires you to restart your computer at the end of the installation process. Because of this, consider performing this task at a time when service to clients won't be interrupted by a shutdown and restart.

STEP BY STEP

INSTALLING ACTIVE DIRECTORY

1. Start the Active Directory Installation Wizard. (Select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.)
2. The Active Directory Installation Wizard starts. Click Next.
3. The Domain Controller Type screen appears. Accept the default option of "Domain controller for a new domain" and click Next.
4. The Create Tree or Child Domain screen appears. Accept the default option of "Create a new domain tree" and click Next.
5. The Create or Join Forest screen appears. Accept the default option of "Create a new forest of domain trees" and click Next.
6. The New Domain Name screen appears. In the "Full DNS name for new domain" text box, type the FQDN of the new domain. Figure 7-28 shows this screen after the name of the new domain has been entered. Click Next.

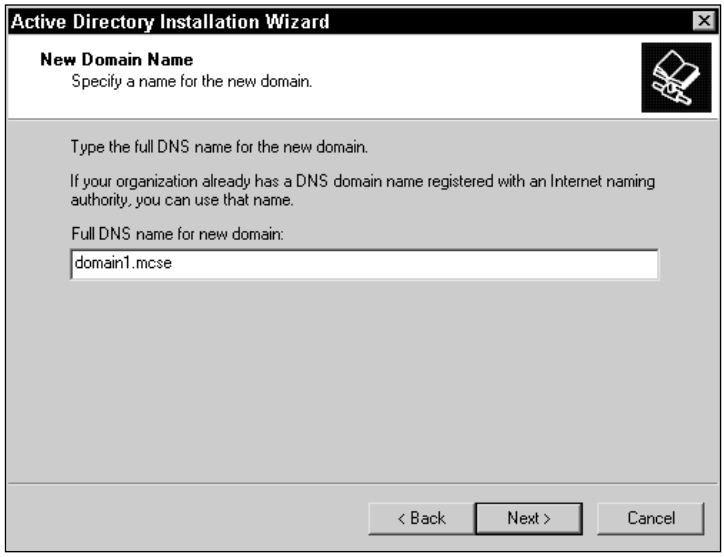

FIGURE 7-28 Specifying a domain name

7. The NetBIOS Domain Name screen appears. Accept the default name displayed, and click Next.
8. The Database and Log Locations screen appears. In this screen, you specify the location where the Active Directory database and log will be stored. Microsoft recommends that, for best recoverability, you store the database and log on separate physical hard disks. However, the default locations are on the *same* hard disk. Either accept the default locations or type in the locations you want to use and click Next.

STEP BY STEP *Continued*

9. The Shared System Volume screen appears. On this screen you specify the location of the folder that will be shared as the system volume. *This folder must be located on a Windows 2000 NTFS volume.* Either accept the default location or type in the location you want to use and click Next.
10. If you have not previously configured a DNS server on your network, or if this computer is not correctly configured to use a DNS server, the Active Directory Installation Wizard may display a message indicating that it can't contact the DNS server. If this message is displayed, click OK.
11. If you don't have a DNS server on your network, or if your DNS server does not support dynamic updates, the Configure DNS screen appears, as shown in Figure 7-29.

FIGURE 7-29 Configuring DNS options

If you haven't yet installed a DNS server on your network, accept the default option of "Yes, install and configure DNS on this computer."

If you have a DNS server but it doesn't support dynamic updates, select the "No, I will install and configure DNS myself" option.

Click Next.

12. The Permissions screen appears.

    If your network includes Windows NT 4.0 Server computers as well as Windows 2000 Server computers, accept the default option of "Permissions compatible with pre-Windows 2000 Servers."

STEP BY STEP *Continued*

If the servers on your network all run Windows 2000, select the "Permissions compatible only with Windows 2000 servers" option.

Click Next.

13. The Directory Services Restore Mode Administrator Password screen appears. In this screen, type in and confirm an Administrator password that will be used if Active Directory ever needs to be restored on this computer from a backup. I recommend that you write down this password and store it in a safe place. Click Next.
14. The Summary screen appears, summarizing the choices you selected while using this wizard. If you are satisfied with the configurations, click Next. (Otherwise, you can click Back to change the options you selected.)
15. The wizard installs and configures Active Directory. This process may take several minutes to complete.
16. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
17. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the Active Directory installation.

If you selected the "No, I will install and configure DNS myself" option in Step 11 because your DNS server doesn't support dynamic updates, you will need to manually add Active Directory resource records to the zone file on your DNS server.

To do this, first copy the *SystemRoot*`\System32\Config\Netlogon.dns` file from the server on which you installed Active Directory to your DNS server. Then, on the DNS server, use your favorite text editor to copy the contents of this file and then paste these contents onto the end of the zone file of the DNS domain with the same name as the Windows 2000 domain you created during the Active Directory installation process.

TIP

I recommend that you reboot your DNS server and your new Windows 2000 domain controller after you complete this process to ensure that the changes to the DNS server are correctly recognized by the Windows 2000 domain controller.

Installing Active Directory on Additional Servers in a Domain

For load balancing and fault tolerance purposes, it's often a good idea to install Active Directory on more than one server in a Windows 2000 domain. When you install Active Directory on an additional server in a Windows 2000 domain, you create an additional domain controller for that domain.

In the steps that follow, I'll explain how to install Active Directory on an additional server in a domain.

TIP

In these steps, I assume that you have previously configured the additional server as a client of a DNS server that supports dynamic updates.

STEP BY STEP

INSTALLING ACTIVE DIRECTORY ON AN ADDITIONAL SERVER

1. Start the Active Directory Installation Wizard. (Select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.)
2. The Active Directory Installation Wizard starts. Click Next.
3. The Domain Controller Type screen appears, as shown in Figure 7-30. Notice the warnings displayed in the bottom of this dialog box.

FIGURE 7-30 Selecting the type of domain controller

STEP BY STEP *Continued*

Select the option next to "Additional domain controller for an existing domain" and click Next.

4. The Network Credentials screen appears. Type in the user name, password, and domain name of the Administrator account for the domain. Figure 7-31 shows the Network Credentials screen after this information has been entered. Click Next.

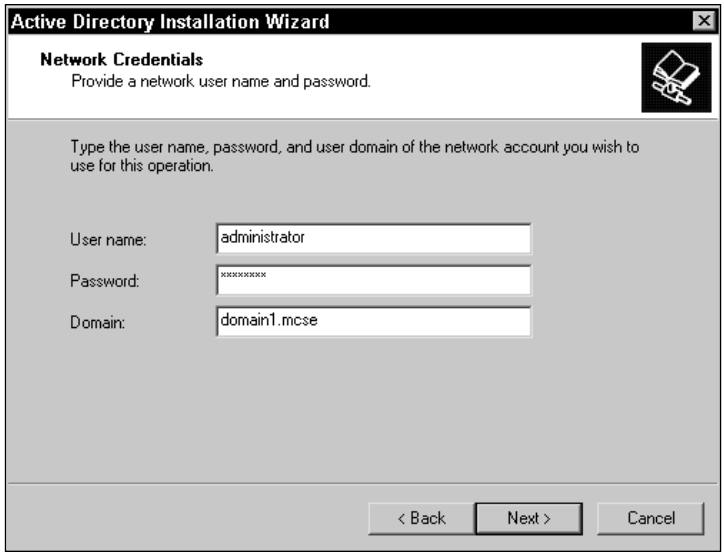

FIGURE 7-31 Specifying network credentials

5. The Additional Domain Controller screen appears. Type in the FQDN of the Windows 2000 domain to which this domain controller will belong. You can browse for the domain name if you don't know it. Click Next.
6. The Database and Log Locations screen appears. In this screen, you specify the location where the Active Directory database and log will be stored. Microsoft recommends that, for best recoverability, you store the database and log on separate physical hard disks. However, the default locations are on the *same* hard disk. Either accept the default locations or type in the locations you want to use and click Next.
7. The Shared System Volume screen appears. On this screen you specify the location of the folder that will be shared as the system volume. *This folder must be located on a Windows 2000 NTFS volume.* Either accept the default location or type in the location you want to use and click Next.
8. The Directory Services Restore Mode Administrator Password screen appears. In this screen, type in and confirm an Administrator password that will be used if Active Directory ever needs to be restored on this computer from a backup. Click Next.

STEP BY STEP *Continued*

9. The Summary screen appears, summarizing the choices you selected while using this wizard. If you are satisfied with the configurations, click Next. (Otherwise, you can click Back to change the options you selected.)
10. The wizard installs and configures Active Directory. This process may take several minutes to complete.
11. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
12. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the Active Directory installation.

Creating a New Child Domain

Sometimes organizations choose to further subdivide their Windows 2000 domains into one or more subdomains. These subdomains are often called *child domains*.

For example, suppose that a company's Windows 2000 domain name is `idgbooks.com`. The company might decide to create two child domains, named `editorial.idgbooks.com` and `production.idgbooks.com`. To create these new child domains, you must install Active Directory on the first domain controller in each new child domain.

In the steps that follow, I'll show you how to install Active Directory on a Windows 2000 Server computer and thereby cause that computer to become the first domain controller in a new child domain. In these steps, I assume that you have previously configured this computer as a client of a DNS server that supports dynamic updates.

STEP BY STEP

CREATING A NEW DOMAIN CONTROLLER IN A NEW CHILD DOMAIN

1. Start the Active Directory Installation Wizard. (Select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.)
2. The Active Directory Installation Wizard starts. Click Next.
3. The Domain Controller Type screen appears. Accept the default option of "Domain controller for a new domain" and click Next.
4. The Create Tree or Child Domain screen appears. Select the option "Create a new child domain in an existing domain tree" and click Next.

STEP BY STEP *Continued*

5. The Network Credentials screen appears. Type in the user name, password, and domain name of the Administrator account for the parent domain of the new child domain you are creating. Click Next.
6. The Child Domain Installation screen appears. In the "Parent domain" text box, type the name of the parent domain—in other words, the name of the domain in which you are creating a new child domain. In the "Child domain" text box, type the name of the new child domain. Figure 7-32 shows this screen after it has been configured. Click Next.

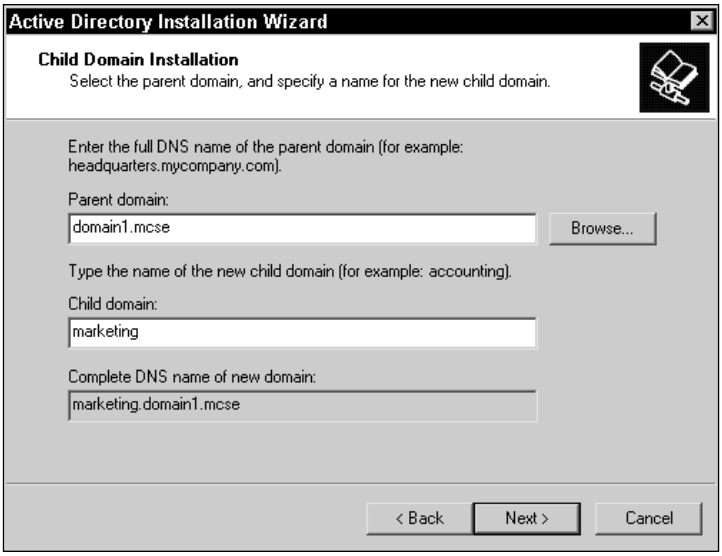

FIGURE 7-32 Naming the child domain

7. The NetBIOS Domain Name screen appears. Accept the default name displayed, and click Next.
8. The Database and Log Locations screen appears. In this screen, you specify the location where the Active Directory database and log will be stored. Either accept the default locations or type in the locations you want to use and click Next.
9. The Shared System Volume screen appears. On this screen you specify the location of the folder that will be shared as the system volume. *This folder must be located on a Windows 2000 NTFS volume.* Either accept the default location or type in the location you want to use, and then click Next.
10. The Permissions screen appears.

    If your network includes Windows NT 4.0 Server computers as well as Windows 2000 Server computers, accept the default option of "Permissions compatible with pre-Windows 2000 Servers."

STEP BY STEP *Continued*

If the servers on your network all run Windows 2000, select the "Permissions compatible only with Windows 2000 servers" option.

Click Next.

11. The Directory Services Restore Mode Administrator Password screen appears. In this screen, type in and confirm an Administrator password that will be used if Active Directory ever needs to be restored on this computer from a backup. Click Next.
12. The Summary screen appears, summarizing the choices you selected while using this wizard. If you are satisfied with the configurations, click Next.
13. The wizard installs and configures Active Directory. This process may take several minutes to complete.
14. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
15. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the Active Directory installation.

Creating a New Tree in the Forest

There may come a time when you need to create a new tree in your Active Directory forest. Although it's not all that common, sometimes the situation warrants this treatment. For example, suppose your organization has recently acquired another company. You want to place the acquired company's computers in a separate domain and tree, but want to keep them in the same forest so that trust relationships are easier for you to manage.

The following steps explain how to install Active Directory on a Windows 2000 Server computer and thereby cause that computer to become the first domain controller in a new domain tree in the forest. In these steps, I assume that you have previously configured this computer as a client of a DNS server that supports dynamic updates. In addition, I assume that you have created a new zone on the DNS server for the new domain tree, and that you have configured this zone for dynamic updates.

STEP BY STEP

CREATING A NEW DOMAIN CONTROLLER IN A NEW DOMAIN TREE

1. Start the Active Directory Installation Wizard. (Select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.)

STEP BY STEP *Continued*

2. The Active Directory Installation Wizard starts. Click Next.
3. The Domain Controller Type screen appears. Accept the default option of “Domain controller for a new domain” and click Next.
4. The Create Tree or Child Domain screen appears. Accept the default option of “Create a new domain tree” and click Next.
5. The Create or Join Forest screen appears. Select the “Place this new domain tree in an existing forest” option. Figure 7-33 shows the Create or Join Forest screen after it has been configured. Click Next.

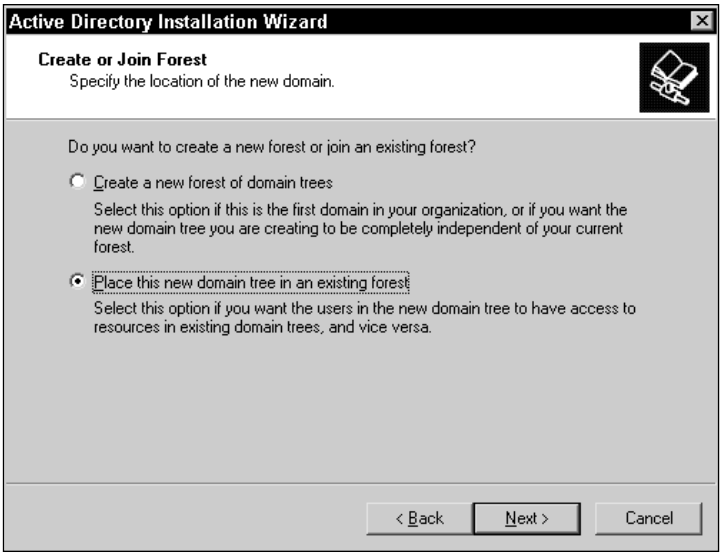

FIGURE 7-33 Creating a new tree

6. The New Domain Tree screen appears. In the text box, type the FQDN of the new domain tree. (This is the name of the new domain you’re creating.) Click Next.
7. The NetBIOS Domain Name screen appears. Accept the default name displayed, and click Next.
8. The Database and Log Locations screen appears. In this screen, you specify the location where the Active Directory database and log will be stored. Either accept the default locations or type in the locations you want to use and click Next.
9. The Shared System Volume screen appears. On this screen you specify the location of the folder that will be shared as the system volume. This folder *must* be located on a Windows 2000 NTFS volume. Either accept the default location or type in the location you want to use and click Next.
10. The Permissions screen appears.

STEP BY STEP *Continued*

If your network includes Windows NT 4.0 Server computers as well as Windows 2000 Server computers, accept the default option of "Permissions compatible with pre-Windows 2000 Servers."

If the servers on your network all run Windows 2000, select the "Permissions compatible only with Windows 2000 servers" option.

Click Next.

11. The Directory Services Restore Mode Administrator Password screen appears. In this screen, type in and confirm an Administrator password that will be used if Active Directory ever needs to be restored on this computer from a backup. Click Next.
12. The Summary screen appears, summarizing the choices you selected while using this wizard. If you are satisfied with the configurations, click Next.
13. The wizard installs and configures Active Directory. This process may take several minutes to complete.
14. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
15. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the Active Directory installation.

Creating a New Forest

Creating a new forest is something most network administrators will never do. In the first place, most companies aren't large enough to even think about using multiple forests. And even large companies typically use only a single forest to manage their Windows 2000 network resources.

However, consider the situation where your company is composed of two distinct divisions. Because the divisions manufacture and market unrelated products, the divisions have been run as separate entities since the inception of the company. Each division maintains its own information services staff, and company management has no plans to integrate the networks or management of the two divisions. In addition, management is considering selling one of the divisions in the not-too-distant future. This is the type of situation in which it *might* make sense to use multiple forests.

The process of creating a new forest is the same as installing Active Directory for the first time on your network. The only difference is that when you create a new forest, you're installing Active Directory on a computer that

will become the first domain controller in the new *forest* (instead of the first domain controller on your network). For details on how to perform this task, see the section titled "Installing Active Directory for the First Time" earlier in this chapter.

Removing Active Directory

There may come a time when you need to remove Active Directory from a computer. For example, you might want to move a domain controller from one domain to another domain. In this situation, you'd need to remove Active Directory from the domain controller, move the server to the new domain, and then reinstall Active Directory if you want that server to function as a domain controller in its new domain.

Removing Active Directory from a domain controller changes that computer into a member server.

The steps that follow explain how to remove Active Directory from a Windows 2000 Server or Advanced Server computer.

STEP BY STEP

REMOVING ACTIVE DIRECTORY

1. From the desktop, select Start ➪ Run.
2. In the Run dialog box, type **dcpromo** and click OK.
3. The Active Directory Installation Wizard starts. Click Next.
4. The Remove Active Directory screen appears. Select the check box on this screen if this server is the *only* domain controller in the domain. Otherwise, leave the check box cleared. Click Next.
5. The Administrator Password screen appears. Type in and confirm the password that you want to assign to the Administrator account for this server. Click Next.
6. The Summary screen appears. Click Next.
7. The wizard removes Active Directory.
8. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
9. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the removal of Active Directory.

Verifying and Troubleshooting an Active Directory Installation

After you install Active Directory, you should verify that the installation was successful. There are two parts to the verification process:

1. On the computer that you installed Active Directory, use Active Directory Users and Computers to verify that the new Active Directory domain has been created, and that the computer on which you installed Active Directory is listed as a domain controller for that domain.
2. On your DNS server, use the DNS administrative tool to verify that the Active Directory DNS entries for the new domain are listed in the zone.

   I'll show you how to perform these two tasks in the following steps.

STEP BY STEP

VERIFYING AND TROUBLESHOOTING YOUR ACTIVE DIRECTORY INSTALLATION

1. *From the desktop of the computer on which you installed Active Directory,* select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain you've just created.

TIP

If the Active Directory domain you created *isn't* listed in this dialog box, your Active Directory installation was not successful. You'll probably have to reinstall Active Directory.

3. In the left pane, highlight the `Domain Controllers` folder. In the right pane, the name of your computer should be displayed. (This is the computer on which you installed Active Directory.) Figure 7-34 shows an Active Directory domain (`domain1.mcse`) and a domain controller (INSPIRON) displayed after a successful Active Directory installation.

   If your Active Directory domain and/or domain controller *aren't* displayed, your Active Directory installation was not successful. You'll probably have to reinstall Active Directory. Close the Active Directory Users and Computers dialog box.

STEP BY STEP *Continued*

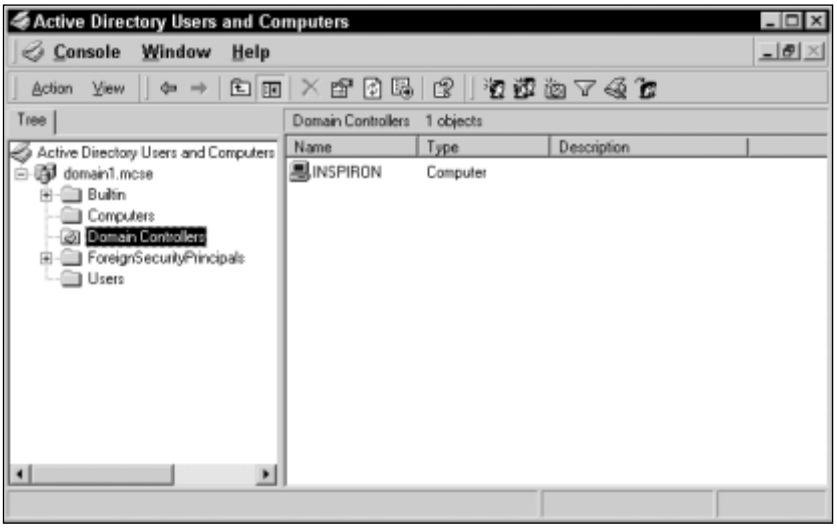

FIGURE 7-34 Verifying Active Directory installation

If your Active Directory domain and domain controller are displayed, close Active Directory Users and Computers and proceed to Step 4.

4. *From the desktop of your DNS server,* select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
5. In the left pane of the DNS dialog box, click the + next to the name of your DNS server. Then click the + next to the `Forward Lookup Zones` folder. Then highlight the folder that has the same name as the Active Directory domain you just created.

   In the right pane of the DNS dialog box, four folders should be displayed, as shown in Figure 7-35. Notice the four folders: `_msdcs`, `_sites`, `_tcp`, `_udp`. (If you just installed Active Directory, you may need to wait several minutes for all of these folders to be displayed. Click Action ➪ Refresh to update your display.)

   If these four folders are present, Active Directory is correctly installed and registered with your DNS server. Close DNS.

   If these folders are not present, Active Directory has not correctly registered itself with the DNS server. In this situation, you probably don't have to reinstall Active Directory, but you do need to register Active Directory with the DNS server, as explained in the next section.

STEP BY STEP *Continued*

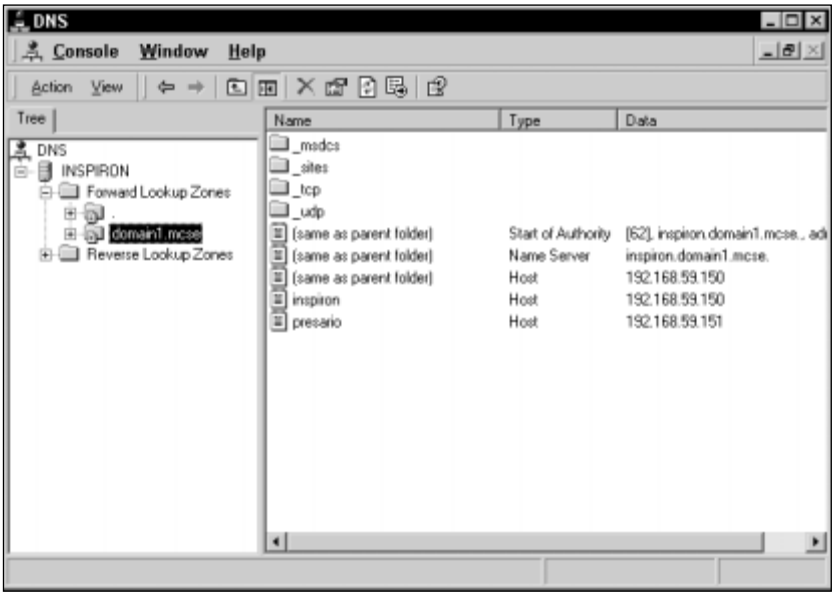

FIGURE 7-35 Verifying the existence of Active Directory DNS entries

If your Active Directory domain and domain controller are displayed in Active Directory Users and Computers, but for some reason Active Directory has not correctly registered itself with your DNS server, there are two ways you can remedy the situation:

- If the zone that contains your Active Directory domain supports dynamic updates, on the DNS server, ensure that the zone is configured to permit dynamic updates. Then, on the domain controller, stop and restart the Net Logon service. This should force Active Directory to register itself with the DNS server.

TIP

To stop and restart the Net Logon service, use the Services administrative tool. For information on using this tool, see Chapter 15. Or, at a command prompt, you can type **net stop netlogon** (and press Enter), and then type **net start netlogon** (and press Enter) to stop and restart this service.

- If the zone that contains your Active Directory domain *doesn't* support dynamic updates, you'll need to manually add Active Directory resource records to the zone file on your DNS server. (I explained how to do this at the end of the section titled "Installing Active Directory for the First Time" earlier in this chapter.)

If the solutions recommended above don't resolve your Active Directory installation problem, or if you encounter other problems with Active Directory, I recommend that you consult Windows 2000 Help for troubleshooting assistance. Windows 2000 Help contains detailed descriptions of many specific Active Directory problems and recommended solutions to these problems.

STEP BY STEP

USING WINDOWS 2000 HELP TO LOCATE ACTIVE DIRECTORY TROUBLESHOOTING INFORMATION

1. From the desktop, select Start ➪ Help.
2. Click the Contents tab if it does not appear on top.
3. On the Contents tab, double-click Active Directory.
4. In the list that appears under Active Directory, click Troubleshooting.

   Several common Active Directory problems are displayed in the right pane, as shown in Figure 7-36.

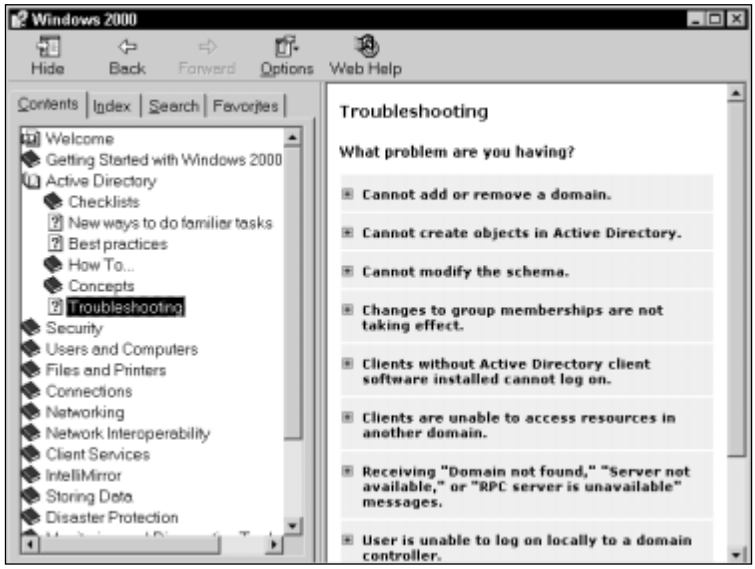

FIGURE 7-36 Using Help to troubleshoot Active Directory problems

STEP BY STEP *Continued*

To view more information and possible solutions for any of the problems listed, click the problem.

5. When you are finished using Windows 2000 Help, close the Windows 2000 dialog box.

KEY POINT SUMMARY

This chapter introduced several DNS and Active Directory topics:

- DNS stands for the Domain Name System. The primary purpose of DNS is to provide host name resolution.
- Active Directory is dependent on DNS.
- DNS is implemented as a hierarchical structure often called the DNS domain namespace. The trees and subtrees that make up the DNS domain namespace are called DNS domains.
- A zone is an administrator-created storage database for either a DNS domain or for a DNS domain and one or more of its subdomains. This storage database is often implemented as a special text file, called a zone file.
- A DNS server can play one (or more) of several different roles, depending on the type of zone(s) the server contains and how the DNS server is configured. The types of roles that a DNS server can perform include standard primary, Active Directory-integrated (primary), standard secondary, master, slave, caching-only, forwarder, and root server.
- DNS is implemented in Windows 2000 via the DNS Server service. The DNS Server service is supported only on Windows 2000 Server and Advanced Server computers.

- After you install the DNS Server service, numerous configurations can be made to a DNS server. You can:
  - Configure the DNS server to be or to use a root server and to be a caching-only server
  - Configure the properties of the DNS server
  - Create and configure zones, including standard primary zones and standard secondary zones
  - Configure zones for dynamic updates
  - Convert a standard primary zone to an Active Directory-integrated zone
  - Integrate an Active Directory DNS with a non–Active Directory DNS
  - Manage replication of DNS
  - Manually create DNS resource records
  - Create DNS subdomains and implement zone delegation
- Before client computers on your network can utilize a DNS server, they must be configured to do so.
- `Nslookup.exe` is a command-line utility that is used to test a DNS server.
- Active Directory can be installed on Windows 2000 Server and Windows 2000 Advanced Server computers. Two prerequisites must be met prior to installing Active Directory:
  - At least one volume on the Windows 2000 Server/Advanced Server computer must be formatted with NTFS.
  - Because Active Directory requires DNS, you either need to have a DNS server installed on your network prior to installing Active Directory, or, you can choose to install DNS at the same time that you perform the Active Directory installation.
- The specific steps to install Active Directory vary depending on the computer's role in Active Directory and your network configuration.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about DNS and Active Directory, and help you prepare for the Network and Directory Services exams:

- **Assessment Questions:** These questions test your knowledge of the DNS and Active Directory topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The problems in scenarios challenge you to apply your understanding of the material to a hypothetical situation. In this chapter's scenarios, you'll be asked to spell out the specific steps you would take to perform several complex DNS tasks. You don't need to be at a computer to do scenarios. Answers to the scenarios are presented at the end of this chapter.
- **Lab Exercises:** These exercises are hands-on practice activities that you perform on a computer. The two labs in this chapter give you an opportunity to install, configure, test, monitor, and troubleshoot DNS; and to install, verify, and troubleshoot Active Directory.

Assessment Questions

1. What type of DNS domain is `microsoft.com`?
   A. Root domain
   B. Top-level domain
   C. Second-level domain
   D. Third-level domain
2. You install the DNS Server service on a Windows 2000 Server computer. You configure this DNS server to use a root server, but you do *not* create any zones whatsoever on this DNS server. What type of DNS server have you configured?
   A. Master
   B. Forwarder
   C. Root server
   D. Caching-only

3. You want to configure root hints on a Windows 2000 DNS server. What tool should you use?
   A. `Nslookup.exe`
   B. DNS administrative tool
   C. Active Directory Users and Computers
   D. `Network and Dial-up Connections` folder
4. You want to configure a static IP address on a Windows 2000 Server computer on which you want to install the DNS Server service and Active Directory. What tool should you use to configure the static IP address?
   A. `Ipconfig.exe`
   B. DNS administrative tool
   C. Active Directory Users and Computers
   D. `Network and Dial-up Connections` folder
5. You want client computers and servers on your Windows 2000 network to be able to register and revise their host names and IP addresses with the network Windows 2000 DNS server without administrator intervention. What should you configure on the Windows 2000 DNS server, and where should you make the necessary configuration?
   A. Enable forwarding — in the zone's Properties dialog box
   B. Enable dynamic updates — in the zone's Properties dialog box
   C. Enable forwarding — in the DNS server's Properties dialog box
   D. Enable dynamic updates — in the DNS server's Properties dialog box
6. When will the Configure DNS Server Wizard *not* permit you to configure a Windows 2000 DNS server as a root server?
   A. When Active Directory is installed on the DNS server
   B. When the DNS server has a dynamic IP address
   C. When the DNS server is connected to the Internet
   D. When another server is configured to use the DNS server as a forwarder
7. What must be installed and/or configured prior to (or during) the installation of Active Directory? (Choose all that apply.)
   A. An NTFS volume
   B. DNS Server service

C. Certificate Services

D. Windows 2000 Server or Advanced Server

8. Which of the following statements about Active Directory are true? (Choose all that apply.)

   A. You can install Active Directory on any Windows 2000 Professional, Server, or Advanced Server computer.

   B. When you install Active Directory on a Windows 2000 Server computer, the computer becomes a domain controller.

   C. You can use Active Directory Users and Computers to install Active Directory.

   D. At least one volume must be formatted with FAT or FAT32 prior to installing Active Directory.

9. You want to install Active Directory on a Windows 2000 Server computer. How can you start the Active Directory Installation Wizard? (Choose all that apply.)

   A. Select Start ➪ Run. Then, in the Run dialog box, type **dcpromo** and click OK.

   B. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS. Then, in the DNS dialog box, select Action ➪ New Host.

   C. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers. Then, in the Active Directory Users and Computers dialog box, select Action ➪ Connect to Domain.

   D. Select Start ➪ Programs ➪ Administrative Tools ➪ Configure Your Server. Then, in the Windows 2000 Configure Your Server dialog box, click the Active Directory link. On the Active Directory page, scroll down and click Start the Active Directory wizard.

Scenarios

Scenarios provide you with an opportunity to apply the knowledge you've gained in this chapter. In this chapter's scenarios, you'll get an opportunity to revisit two specific DNS configuration tasks. Because each of these tasks involve multiple DNS servers, you probably won't have the computer resources to practice the tasks directly. However, these scenario problems enable you to act as if you were performing each task, and spell out the steps you would take on each DNS server to complete the task.

For each problem, consider the given information and identify the steps required to accomplish the specified task.

1. You have two DNS servers on your network. One DNS server is a Windows 2000 Active Directory-integrated DNS server, and the other is a DNS server that runs on a UNIX host. You want the UNIX DNS server to maintain a copy of the zone that is located on the Active Directory-integrated DNS server. What steps would you take (and on which server) to accomplish this?
2. Your company's network has five locations: a central office and four satellite offices. Each location has a server that functions both as an Active Directory domain controller and as a Windows 2000 DNS server. The DNS server at your central office currently has one standard primary zone. You want to replicate this zone to the other four DNS servers in the most efficient manner possible. What steps would you take (and on which servers) to accomplish this?

Lab Exercises

The following two labs are designed to give you practical experience working with DNS and Active Directory.

Lab 7-1 Installing and Configuring DNS

- Network
- Directory Services

The purpose of this lab is to provide you with hands-on experience installing, configuring, managing, testing, and troubleshooting DNS on a Windows 2000 Server computer.

There are seven parts to this lab:

- Part 1: Configuring your server and installing the DNS Server service
- Part 2: Configuring a DNS client
- Part 3: Configuring a root server and a caching-only server
- Part 4: Configuring zones and zone delegation
- Part 5: Manually creating a DNS resource record

- Part 6: Testing the DNS Server service
- Part 7: Troubleshooting DNS

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator. Follow the steps in the lab carefully.

Part 1: Configuring Your Server and Installing the DNS Server Service

In this part, you assign your Windows 2000 Server computer a primary DNS suffix, and then install the DNS Server service.

1. From the desktop, right-click My Computer and select Properties from the menu that appears.
2. In the System Properties dialog box, click the Network Identification tab.
3. On the Network Identification tab, click Properties.
4. In the Identification Changes dialog box, click More.
5. In the DNS Suffix and NetBIOS Computer Name dialog box, type **domain1.mcse** in the "Primary DNS suffix of this computer" text box. Click OK.
6. In the Identification Changes dialog box, click OK.
7. In the Network Identification dialog box, click OK.
8. On the Network Identification tab, click OK.
9. In the System Settings Change dialog box, click Yes to restart your computer. When your computer restarts, boot to Windows 2000 Server and log on as Administrator.
10. Place your Windows 2000 Server compact disc in your computer's CD-ROM drive. Close the Microsoft Windows 2000 CD dialog box. Select Start ➪ Settings ➪ Control Panel.
11. In the Control Panel dialog box, double-click Add/Remove Programs.
12. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
13. The Windows Components Wizard starts. In the Windows Components screen, scroll down and highlight Networking Services. Click Details.
14. In the Networking Services dialog box, select the check box next to Domain Name System (DNS). Click OK.
15. In the Windows Components screen, click Next.

16. Windows 2000 Setup configures components. In the Completing the Windows Components Wizard screen, click Finish.
17. Close the Add/Remove Programs dialog box. Close Control Panel. Remove the Windows 2000 compact disc from your computer's CD-ROM drive.

Part 2: Configuring a DNS Client

In this part you configure your DNS server to be its own DNS client.

1. From the desktop, select Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click the `Network and Dial-up Connections` folder.
3. In the `Network and Dial-up Connections` folder, right-click Local Area Connection and select Properties from the menu that appears.
4. In the Local Area Connection Properties dialog box, highlight Internet Protocol (TCP/IP) and click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, ensure that the "Use the following DNS server addresses" option is selected. Then, in the Preferred DNS server text box, type the IP address of this DNS server. (Use **192.168.59.101** unless your network administrator or instructor supplies you with a different IP address.) Click Advanced.
6. In the Advanced TCP/IP Settings dialog box, click the DNS tab.
7. On the DNS tab, in the "DNS suffix for this connection" text box, type **domain1.mcse** and click OK.

   If you're performing this lab in a classroom setting, your instructor may provide you with a different domain name to enter in this step.
8. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
9. In the Local Area Connection Properties dialog box, click OK.
10. Close the `Network and Dial-up Connections` folder.

Part 3: Configuring a Root Server and a Caching-only Server

In this part you configure a root server and a caching-only server.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the DNS dialog box, highlight your computer in the left pane.
3. Windows 2000 indicates that your DNS server has not yet been configured. Select Action ➪ Configure the server.

4. The Configure DNS Server Wizard starts. Click Next.
5. The Root Server screen appears. Accept the default option of "This is the first DNS server on this network." Click Next.
6. In the Forward Lookup Zone screen, select the "No, do not create a forward lookup zone" option, and click Next.
7. The Completing the Configure DNS Server Wizard screen appears. Click Finish.
8. The DNS dialog box reappears. This completes the configuration of a root server.

Because you've installed and configured the DNS Server service, your DNS server is now configured as a caching-only server.

Part 4: Configuring Zones and Zone Delegation

In this part you create three standard primary forward lookup zones and one standard primary reverse lookup zone. You also configure zones for dynamic updates and implement zone delegation.

1. In the DNS dialog box, click the + next to your computer's name in the left pane.
2. In the left pane, highlight the `Forward Lookup Zones` folder. Select Action ➪ New Zone.
3. The New Zone Wizard begins. Click Next.
4. The Zone Type screen appears. Accept the default option of "Standard primary" and click Next.
5. In the Name text box on the Zone Name screen, type **domain1.mcse** and click Next.
6. The Zone File screen appears. Accept the default options presented on this screen. Click Next.
7. The Completing the New Zone Wizard screen appears. Click Finish.
8. The DNS dialog box reappears. Notice that the new zone you created appears in the right pane.
9. Repeat Steps 2 through 8 two more times to create two additional forward lookup zones. When prompted to name these zones in Step 5, uses the names **sales.domain1.mcse** and **manufacturing.domain1.mcse** for the two new zones.

10. In the left pane of the DNS dialog box, highlight the `Reverse Lookup Zones` folder. Select Action ➪ New Zone.
11. The New Zone Wizard begins. Click Next.
12. The Zone Type screen appears. Accept the default option of "Standard primary" and click Next.
13. The Reverse Lookup Zone screen appears. Accept the default "Network ID" option. Type in a Network ID of **192.168.59** unless your network administrator or instructor supplies you with a different Network ID. Click Next.
14. The Zone File screen appears. Accept the default options presented on this screen. Click Next.
15. The Completing the New Zone Wizard screen appears. Click Finish.
16. The DNS dialog box reappears. Notice that the new zone you created appears in the right pane.

    In the left pane of the DNS dialog box, click the + next to the `Forward Lookup Zones` folder. Also click the + next to the `Reverse Lookup Zones` folder.
17. In the left pane, highlight the domain1.mcse zone. Select Action ➪ Properties.
18. The zone's Properties dialog box appears. On the General tab, select Yes in the "Allow dynamic updates?" drop-down list box. Click OK.
19. Repeat Steps 17 through 18 for each of the other three zones you created, configuring each zone to allow dynamic updates.
20. In the left pane of the DNS dialog box, highlight the `domain1.mcse` folder. Select Action ➪ Refresh.
21. In the *right* pane of the DNS dialog box, notice the `manufacturing` and `sales` folders that are displayed. Also notice that both folders are gray, which indicates that zone delegation is enabled for the manufacturing and sales zones. You don't have to manually configure zone delegation because you created the subdomains on the *same* DNS server that contains the `domain1.mcse` parent domain.

Part 5: Manually Creating a DNS Resource Record

In this part you manually create a Pointer (PTR) record for your DNS server.

1. In the left pane of the DNS dialog box, highlight the `192.168.59.`*`x`* `Subnet` folder. Select Action ➪ New Pointer.

2. The New Resource Record dialog box appears. Type **101** in the white space at the end of the "Host IP number" box. Type **server01.domain1.mcse** in the "Host name" text box. Click OK.
3. When the DNS dialog box reappears, notice that the new record you just created appears in the right pane. Close the DNS dialog box.

Part 6: Testing the DNS Server Service

In this part, you use `Nslookup.exe` to test your DNS server.

1. From the desktop, select Start ➪ Programs ➪ Accessories ➪ Command Prompt.
2. Maximize the Command Prompt dialog box when it appears.
3. At the command prompt, type **nslookup** and press Enter.
4. `Nslookup.exe` displays your computer's name and IP address. At the `Nslookup.exe` prompt (>) type **192.168.59.101** and press Enter.
5. `Nslookup.exe` displays two pairs of computers and their IP addresses. The first pair consists of the name of the DNS server that resolved this request and its associated IP address. The second pair consists of the computer name and IP address of the host that you supplied the IP address for in Step 4. The DNS server used the Pointer (PTR) record you created earlier in this lab to perform this reverse lookup from IP address to host name.
6. At the `Nslookup.exe` prompt (>) type **help** and press Enter. Notice the syntax for the `Nslookup.exe` commands and options.
7. At the `Nslookup.exe` prompt (>) type **exit** and press Enter to close `Nslookup.exe`. Then type **exit** and press Enter to close the Command Prompt.

Part 7: Troubleshooting DNS

1. From the desktop, select Start ➪ Help.
2. Click the Contents tab if it does not appear on top.
3. On the Contents tab, double-click Networking.
4. In the list that appears under Networking, double-click DNS.
5. In the list that appears under DNS, double-click Troubleshooting. Notice the various DNS troubleshooting topics listed.

6. In the *right* pane, click "Troubleshoot DNS servers." Notice the various problems this Help feature can help you resolve.
7. Close the Windows 2000 dialog box.

Lab 7-2 Installing Active Directory

- ▶ Network
- ▶ Directory Services

The objective of this lab is to give you hands-on experience installing Active Directory on a Windows 2000 Server computer. Then, after the Active Directory installation, you'll have an opportunity to verify the installation, practice troubleshooting Active Directory problems, and monitor the DNS Server service.

There are four parts to this lab:

- Part 1: Installing Active Directory
- Part 2: Verifying Your Active Directory Installation
- Part 3: Troubleshooting Active Directory
- Part 4: Monitoring the DNS Server Service

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

Part 1: Installing Active Directory

1. Select Start ➪ Run. In the Run dialog box, type **dcpromo** and click OK.
2. The Active Directory Installation Wizard starts. Click Next.
3. The Domain Controller Type screen appears. Accept the default option of "Domain controller for a new domain" and click Next.
4. The Create Tree or Child Domain screen appears. Accept the default option of "Create a new domain tree" and click Next.
5. The Create or Join Forest screen appears. Accept the default option of "Create a new forest of domain trees" and click Next.
6. The New Domain Name screen appears. In the "Full DNS name for new domain" text box type **domain1.mcse** and click Next.

7. The NetBIOS Domain Name screen appears. Accept the default name displayed and click Next.
8. The Database and Log Locations screen appears. Accept the default locations displayed and click Next.
9. The Shared System Volume screen appears. Accept the default folder location displayed and click Next.
10. The Permissions screen appears. Select the "Permissions compatible only with Windows 2000 servers" option. Click Next.
11. The Directory Services Restore Mode Administrator Password screen appears. In this screen, type **password** in the Password text box. Then type **password** in the "Confirm password" text box. Click Next.
12. The Summary screen appears. Click Next.
13. The wizard installs and configures Active Directory. This process may take several minutes to complete.
14. The Completing the Active Directory Installation Wizard screen appears. Click Finish.
15. When the Active Directory Wizard dialog box appears, click Restart Now to restart your computer and complete the Active Directory installation.

Part 2: Verifying Your Active Directory Installation

1. When your computer restarts, boot to Windows 2000 Server and log on as Administrator. From the desktop select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to `domain1.mcse`.

   If `domain1.mcse` *isn't* listed in the left pane of this dialog box, your Active Directory installation was not successful. You'll probably have to reinstall Active Directory.
3. In the left pane, highlight the `Domain Controllers` folder. In the right pane, the name of your computer (Server01) should be displayed.

   If your computer *isn't* listed in this pane, your Active Directory installation was not successful. You'll probably have to reinstall Active Directory.

   Close the Active Directory Users and Computers dialog box.
4. From the desktop select Start ➪ Programs ➪ Administrative Tools ➪ DNS.

5. In the left pane of the DNS dialog box, click the + next to the name of your DNS server (Server01). Then click the + next to the `Forward Lookup Zones` folder. Then highlight the `domain1.mcse` folder.

   In the right pane of the DNS dialog box, four folders should be displayed: `_msdcs`, `_sites`, `_tcp`, `_udp`. (You may need to wait several minutes after the computer reboots for all of the folders to be displayed. Click Action ➪ Refresh to update your display.)

   If these four folders are present, Active Directory is correctly installed and registered with your DNS server. Close the DNS dialog box.

Part 3: Troubleshooting Active Directory

1. From the desktop, select Start ➪ Help.
2. Click the Contents tab if it does not appear on top.
3. On the Contents tab, double-click Active Directory.
4. In the list that appears under Active Directory, click Troubleshooting. Notice that several common Active Directory problems are displayed in the right pane.
5. In the right pane, click "Cannot add or remove a domain" and view the possible causes and recommended solutions for this problem.
6. Close the Windows 2000 dialog box.

Part 4: Monitoring the DNS Server Service

In this part, you use the Monitoring tab in the DNS administrative tool to monitor your DNS server.

1. From the desktop, select Start ➪ Programs ➪ Administrative Tools ➪ DNS.
2. In the left pane of the DNS dialog box, highlight the name of your computer, and select Action ➪ Properties.
3. In the DNS server's Properties dialog box, click the Monitoring tab.
4. The Monitoring tab appears. Select the check box next to "A simple query against this DNS server." Then, select the check box next to "Perform automatic testing at the following interval." From the drop-down list box, select "seconds." The test interval should now be configured for every 30 seconds. Click Apply.

5. The test results (either PASS or FAILED) will begin appearing in the box at the bottom of the dialog box. Monitor this dialog box for two minutes. Notice that the time field is automatically updated every 30 seconds. Also notice that only the most recent test is displayed in this box.

TIP

The monitoring feature doesn't appear to be rock-solid (although it does work better after Active Directory is installed). Sometimes a PASS result is displayed, and sometimes a FAILED result is displayed. Even if a FAILED result is displayed, this doesn't necessarily mean your DNS server is not functioning properly.

6. Clear the check boxes next to "A simple query against this DNS server" and "Perform automatic testing at the following interval." Click OK.
7. Close the DNS dialog box.

Answers to Chapter Questions

Chapter Pre-Test

1. DNS stands for the Domain Name System.
2. Host name resolution is the process of resolving a computer's user-friendly host name (such as `www.idgbooks.com`) to the IP address of that computer.
3. The DNS domain at the top of the DNS domain namespace is called the *root* domain. This domain is often represented by a *period* (.).
4. Any four of the following:
   - Standard primary
   - Active Directory integrated (primary)
   - Standard secondary
   - Master
   - Slave
   - Caching-only
   - Forwarder
   - Root server

5. TTL stands for Time-To-Live.
6. The prerequisites that must be met prior to installing Active Directory are:
   - At least one volume on the Windows 2000 Server/Advanced Server computer must be formatted with NTFS.
   - Because Active Directory requires DNS, you either need to have a DNS server installed on your network prior to installing Active Directory, or you can choose to install DNS at the same time that you perform the Active Directory installation.

Assessment Questions

1. **C.** `Microsoft.com` is a second-level domain. The root domain is `.` and the top-level domain is `com`.
2. **D.** A caching-only server is a DNS server that has been configured to use (or to be) a root server. A caching-only DNS server does *not* store any zones.
3. **B.** Use the Root Hints tab in a DNS server's Properties dialog box in the DNS administrative tool to configure root hints.
4. **D.** A static IP address is specified by configuring the Local Area Connection in the `Network and Dial-up Connections` folder.
5. **B.** You should select Yes in the drop-down list box next to "Allow dynamic updates?" in the zone's Properties dialog box.
6. **C.** When a Windows 2000 DNS server is connected to the Internet, the Configure DNS Server Wizard does *not* permit you to configure this server as a root server.
7. **A, B, D.** Windows 2000 Server (or Advanced Server) must be installed and at least one volume formatted with NTFS prior to installing Active Directory. In addition, the DNS Server service must be installed either before installing Active Directory or during the process of installing Active Directory.
8. **B.** When Active Directory is installed on a Windows 2000 Server or Advanced Server computer, the computer becomes a domain controller. None of the other statements are true.
9. **A, D.** These are the only two ways to start the Active Directory Installation Wizard.

Scenarios

1. On the UNIX DNS server, create a standard secondary zone. When you create this secondary zone, assign it the same name as the Active Directory-integrated zone, and specify the IP address of the Active Directory-integrated DNS server that contains the master copy of the zone.
2. The most efficient way to achieve replication, in this situation, is to:
   a. Convert the standard primary zone on the Windows 2000 DNS server at the central office to an Active Directory-integrated zone.
   b. Configure each of the four Windows 2000 DNS servers at the four satellite offices to load zone data on startup from "Active Directory and registry."

   Once these two steps have been performed, Active Directory will automatically replicate the zone data to each of the four satellite Windows 2000 DNS servers.

MCSE
EXAM
MATERIAL