CHAPTER

1

Basic Windows 2000/ Windows 2000 Server Installation and Configuration

This chapter steps you through the installation process of your Windows-based Tiger Box operating system. Although the configurations in this chapter feature the Windows 2000 Server, they can also be applied to Windows 2000 and Windows 2000 Professional versions.

Launching Windows 2000 Server

To launch Windows 2000 Server, power up the system with the Microsoft Windows 2000 Server CD in your primary CD-ROM drive. Be sure that your system's Setup specifies the primary boot process, starting with CD-ROM. Then follow these steps:

Step 1. In the Welcome to Setup screen, you are given three options:

- Press Enter to set up Windows 2000.
- Press R to repair a Windows 2000 installation.
- Press F3 to quit Setup without installing Windows 2000.

In this case, press Enter to continue with the installation process.

Step 2. License Agreement. View the entire Windows 2000 Licensing Agreement by pressing Page Down. At the end of the agreement, press F8 to accept its terms and continue.

Step 3. Location Selection and Drive Format. Select an installation location for Windows. In this step, you may create/delete active hard drive partitions; after which, select the partition to which you want to install the operating system, and press Enter. By pressing Enter, you may now choose to format the partition by using the File Allocation Table (FAT) system or the NT File System (NTFS). In this case, select NTFS.

FAT OR NTFS? THAT IS THE QUESTION

FAT is the least complicated type of Windows-supported file system. Because it begins with very little overhead, it is most applicable to drives and/or partitions under 400 MB. It resides at the top of the fixed quantity of allocated storage space, or *volume,* on the hard disk. For security purposes, two copies of the FAT are maintained in case one copy becomes corrupt.

The FAT system establishes a table that the operating system uses to locate files on a disk. Even if a file is fragmented into many sections—that is, scattered around the disk—the table makes it possible for the FAT to monitor and find all the sections.

FAT formats are allocated in groups or clusters, the sizes of which are determined by the correlating volume size. For example, when a file is created, an entry is made in the directory and the first cluster number—set by the system—containing data is recognized. This entry either indicates that this cluster is the last of the file or points to the next cluster.

It's important to note that the FAT must be updated regularly; otherwise, it can lead to data loss. However, also note that each time the FAT is updated, the disk-read heads must be repositioned to the drive's logical track zero. This is a time-consuming process. Note, too, that because there is typically no organization to the FAT directory structure, files are given the first open location on the drive. It's important to be aware that for successful booting, the FAT and the root directory must be stored in a predetermined location.

The FAT supports only read-only, hidden, system, and archive file attributes. A filename or directory name may be up to eight characters long, be followed by a period (.), and then have an extension of up to three characters. The FAT uses the traditional 8.3 filenaming convention—that is, all filenames must be created with the ASCII character set. All FAT names must start with either a letter or a number; they may contain any characters except the following:

- **Period (.)**
- **Double quotation marks ("")**
- **Forward and backward slashes (/ \)**
- **Square brackets ([ ])**
- **Colon (:)**
- **Semicolon (;)**
- **Pipe symbol (|)**
- **Equals sign (=)**
- **Comma (,)**

(continues)

FAT OR NTFS? THAT IS THE QUESTION *(Continued)*

FAT has two primary advantages:

- **In the case of hard disk failures, a bootable DOS floppy can be used to access the partition for problem troubleshooting.**
- **Under Windows, it is not possible to perform an undelete. However, if the file was located on a FAT partition, and the system is restarted under MS-DOS, the file can be undeleted.**

FAT has the following two disadvantages:

- **As the size of the volume increases, FAT performance decreases; therefore, the FAT file system is not recommended when one works with drives or partitions larger than 400 MB.**
- **It is not possible to set security permissions on files located in FAT partitions. Also, FAT partitions are, under Windows, limited to a maximum size of 4 GB.**

The NTFS has features that improve manageability, including transaction logs and file security that help resolve disk failures. Access control permissions can be set for directories and/or individual files. For large disk-space requirements, NTFS supports *spanning volumes,* which make possible the distribution of files and directories across several physical disks. Because NTFS performance does not degrade, it is best used on volumes of 400 MB or more.

NTFS file and directory names may be up to 255 characters long, including extensions separated by a period (.). Although these names preserve whatever case the names are typed in, they are not case-sensitive. NTFS names must start with either a letter or a number; they may contain any characters except the following:

Question mark (?)

Double quotation marks (“”)

Forward and backward slashes (/ \)

Asterisk (*)

Pipe symbol (|)

Colon (:)

The advantages of the NTFS are the following:

- **Its recoverability functions mean that disk-repair utilities would never be required.**
- **It enables setting file and directory control permissions.**
- **Activity logging makes troubleshooting failures easier.**
- **It enables large disk-space management and long filename support (up to 255 mixed-case characters).**

The disadvantages of the NTFS are the following:

- **Because of the amount of space overhead, NTFS should not be used on volumes smaller than 400 MB.**

(continues)

FAT OR NTFS? THAT IS THE QUESTION *(Continued)*

- **It does not have integrated file encryption. Therefore, it is possible to boot under MS-DOS or another operating system, and use a low-level disk-editing utility to view data stored on an NTFS volume.**
- **The NTFS overhead does not fit on a floppy disk; therefore, it is not possible to format a floppy with the NTFS. Windows always uses FAT during the formatting procedure.**

Permission control, whether on a FAT or an NTFS partition, is a simple process as long as you keep in mind the limitations of each type of file system. Basically, NTFS supports both local and remote user permissions on both local and shared files and/or folders, whereas FAT supports only network shares. For example, by setting control access to a shared folder on a FAT partition, all of its files and subfolders inherit the same permissions.

Step 4. Setup will copy the installation files to the selected partition. When Setup is finished, press Enter to restart the system and continue with the installation.

Step 5. Windows 2000 Setup Wizard. Windows 2000 Server Setup wizard will complete the installation process. Press Next to acknowledge. The wizard will detect and install devices on the system.

Step 6. Regional Settings. You can customize Windows 2000 Server for different regions and settings. For local settings, click Customize and set the current local, time, date, and currency. Click OK to accept the changes. For keyboard settings, click Customize and select your keyboard properties. Click OK to accept the settings. Click Next when you are ready to continue with the installation.

Step 7. Personalizing Windows 2000. Type your full name and the name of your company or organization; then click Next.

Step 8. Licensing Mode. Based on Microsoft's definitions as they are extracted here, choose either the *per-seat* or the *per-server* licensing type; then click Next.

PER-SEAT LICENSING *A per-seat license associates a Client Access License with a specific computer or "seat." Client computers are allowed access to any Windows NT Server or Windows NT Server, Enterprise Edition on the network, as long as each client machine is licensed with the appropriate Client Access License. The per-seat mode is most economical in distributed computing environments where multiple servers within an organization provide services to clients, such as a company that uses Windows NT Server for file and print services.*

PER-SERVER LICENSING *A per-server license associates a Client Access License with a particular server. This alternative allows concurrent-use licensing: If customers decide to use the server in per-server mode, they must have at least as many Client Access Licenses dedicated to that server to accommodate the maximum number of clients that will connect to that server at any one point in time. The server assigns Client Access Licenses temporarily to client computers; there is no permanent Client*

Access License association with a specific client machine. If a network environment has multiple servers, then each server in per-server mode must have at least as many Client Access Licenses dedicated to it as the maximum number of clients that will connect to it at any one point in time. Under this option, the customer designates the number of client access licenses that apply to the server during setup. The per-server mode is most economical in single-server, occasional-use, or specialty-use server solutions (with multiple concurrent connections). Some examples include Remote Access Service solutions, CD-ROM servers, or the initial server of a planned larger deployment.

Step 9. Server Name and Password. Enter a name for the computer and the administrator password (up to 14 characters); then click Next.

Step 10. Windows 2000 Components. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. You may elect to install services such as DNS from the Components window; however, for our purposes here we'll accept the default settings for accessories, utilities, and services (including Internet International Server [IIS]) and then click Next to continue.

Step 11. Date and Time. Verify the correct date, time, and time zone; click Next to confirm and accept.

Step 12. Networking Settings. The setup wizard will install the networking components. Choose whether to use typical (auto install of common services) or custom settings (manually configure networking components). For now, select Typical settings and click Next.

Step 13. Workgroup or Computer Domain. Select to make this computer a member of a domain or workgroup. Click Next to continue.

Step 14. Installing Components and Completing Setup. The setup wizard will install your component selections (this may take several minutes) and will also perform final tasks, such as registering components, saving settings, and removing temporary files.

Step 15. Click Finish to complete the setup wizard. Remove the CD-ROM; then restart the computer.

Step 16. Logging in. After you restart the system, you'll have to log in with the administrative password configured during the setup process. For security, the password will display as asterisks as you type it in.

Basic Windows 2000/Windows 2000 Server Configuration

Thanks to updated management utilities and a slightly enhanced user interface, Windows 2000 Server can be easily configured by using new and improved configuration wizards. If this is your first boot-up of the new operating system, you'll see the Configure Your Server utility shown in Figure 1.1, which will facilitate some of the basic configuration techniques. From the flexible interface at the left menu, simply choose the services that you want to run on this server. We'll start with Active Directory.

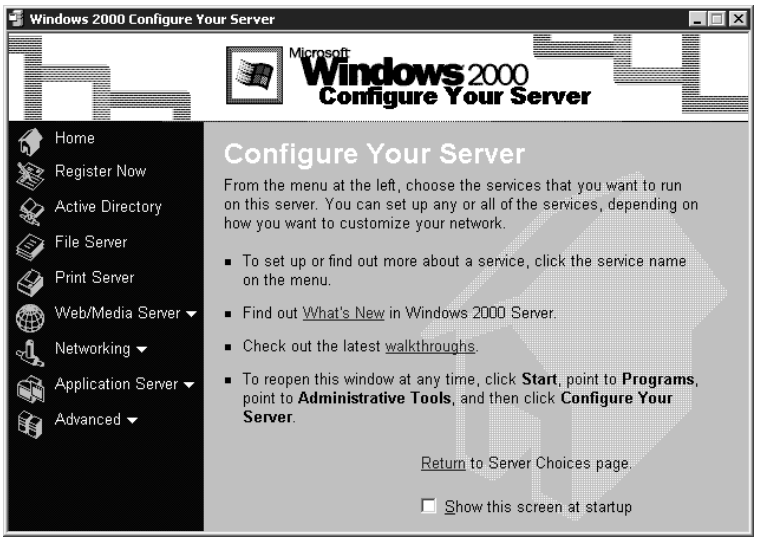

Figure 1.1 Windows 2000 Configure Your Server.

NOTE **If this is not the first boot-up of the new operating system, and you've elected not to be greeted by the configuration utility, you can retrieve it from Start/Programs/Administrative Tools/Configure Your Server. It's a good idea to do that now so you can follow along here.**

Active Directory

Active Directory stores information about network objects, such as user accounts and shared printers, and provides access to that information. Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network.

To make this server a new domain controller, you must install Active Directory. A domain controller in a Windows 2000 Server domain is a computer running Windows 2000 Server that manages user access to a network, which includes logons, authentication, and access to the directory and shared resources. The Active Directory Installation wizard configures this server as a domain controller and sets up the DNS if it is not already available on the network. DNS is a system for naming computers and network services; these names are organized into a hierarchy of domains. DNS is used in

TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names. When a user enters a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address.

You can use this wizard for the following scenarios:

No Existing Domain Controller. Sets up your server as the first domain controller on the network.

Domain Controller Already on Network. Sets up your server as an *additional domain controller*, a *new child domain*, a *new domain tree*, or a *new forest*. These entities are defined in the following paragraphs.

An additional domain controller is a Windows 2000 domain controller installed into an existing domain. All domain controllers participate equally in Active Directory replication, but by default the first domain controller installed into a domain is assigned ownership of at least three floating single-master operations. Additional domain controllers installed into an existing domain do not assume ownership of these operations by default.

A child domain is a domain located in the namespace tree directly beneath another domain name (the parent domain). For example, example.microsoft.com would be a child domain of the parent domain, microsoft.com. A child domain is also known as a *subdomain*.

The domain tree is the hierarchical structure that is used to index domain names. Domain trees are similar in purpose and concept to directory trees, which are used by computer filing systems for disk storage. For example, when numerous files are stored on disk, directories can be used to organize the files into logical collections. When a domain tree has one or more branches, each branch can organize domain names used in the namespace into logical collections.

A forest is a set of one or more trees that do not form a contiguous namespace. All trees in a forest share a common schema, configuration, and global catalog. The trees must trust one another through transitive, bidirectional trust relationships. Unlike a tree, a forest does not need a distinct name. A forest exists as a set of cross-reference objects and trust relationships known to the member trees. Trees in a forest form a hierarchy for the purpose of trust.

NOTE To host Active Directory, you need a partition formatted with the version of NTFS used in Windows 2000.

Creating a New Domain

To create a new domain, we'll install Active Directory using the Active Directory Installation wizard, which installs and configures components that provide Active Directory service to network users and computers. In the menu listing of the configuration utility shown in Figure 1.1, click the Active Directory icon to reach the screen shown in Figure 1.2. At that screen, click Next; then click Start the Active Directory Installation wizard shown in Figure 1.3. Click Next to continue.

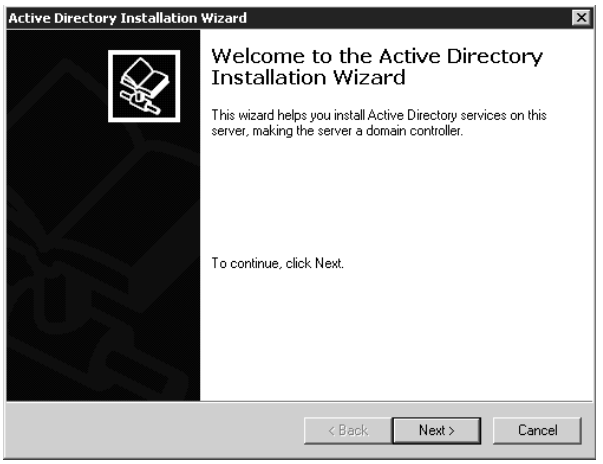

Figure 1.2 Active Directory wizard front end.

Recall that a domain controller is a computer running Windows 2000 Server, which stores directory data and manages user domain interactions, including user logon processes, authentication, and directory searches. Windows 2000 Server domain controllers provide an extension of the capabilities and features provided by Windows NT Server 4.0 domain controllers. A domain can have one or more domain controllers. For high availability and fault tolerance, a small organization using a single local area network (LAN) might need only one domain with two domain controllers, whereas a large company with many network locations would need one or more domain controllers in each location.

A domain controller in Windows 2000 is also configured using the Active Directory Installation wizard. Active Directory supports *multimaster replication* of directory data between all domain controllers in the domain. Multimaster replication is an evolution of the primary and backup domain controller (BDC) model used in Windows NT Server 4.0, in which only one server, the primary domain controller (PDC), had a read-and-write copy of the directory. Windows 2000 Server multimaster replication synchronizes directory data on each domain controller, ensuring consistency of information over time. Changes in the PDC can be impractical to perform in a multimaster fashion; therefore, only one domain controller, the *operations master,* accepts requests for such changes. In any Active Directory forest, there are at least five different operations' master roles that are assigned to one or more domain controllers.

Figure 1.3 Starting the Active Directory wizard.

Let's create a new domain in Active Directory:

Step 1. Once Active Directory is installed, from the Configure Your Server utility, click Active Directory; from the Active Directory window, choose the domain controller type to create a new domain by selecting Domain controller for a new domain; then click Next.

Step 2. In the next window, choose to create a new domain tree by selecting Create a new domain tree; then click Next.

Step 3. Next, choose to create a new forest of domain trees by selecting Create a new forest of domain trees; then click Next.

Step 4. Specify a name for the new domain by typing the full DNS name (see Figure 1.4); then click Next.

Step 5. Specify the Network Basic Input/Output System (NetBIOS) name for the new domain. Earlier versions of Windows will use this to identify the new domain. Click Next.

Step 6. In the next window, specify in the fields provided the locations of the Active Directory database and log, either by accepting the default locations or by clicking Browse to find new ones. Click Next to continue.

Step 7. In the next window, you must specify the folder to be shared as the system volume. The Sysvol folder stores the server's copy of the domain's public files. Either accept the default location or click Browse to find a new one. Click Next to continue.

Step 8. DNS must be installed. If DNS is not available; the wizard will configure it for the new domain. Select Yes to install DNS, as shown in Figure 1.5; then click Next.

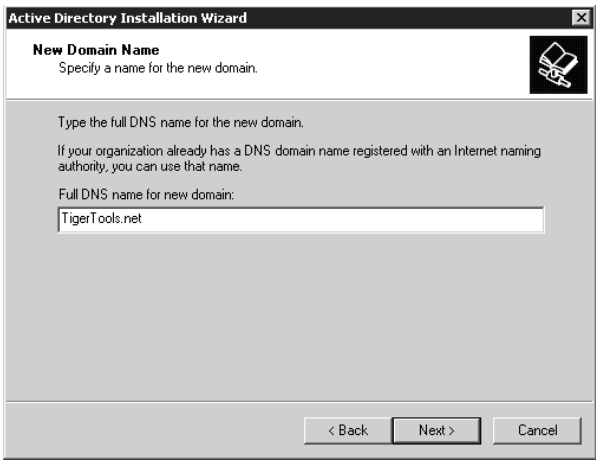

Figure 1.4 Specifying a new domain.

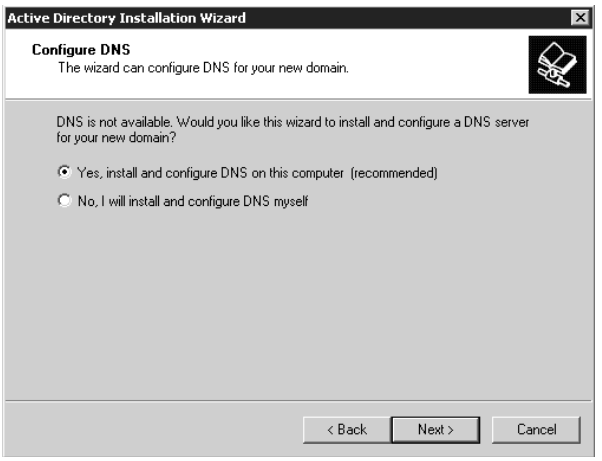

Figure 1.5 Installing DNS for the new domain.

Step 9. In the next window, you must select the default permissions for user and group objects. You do this by selecting Permissions compatible with pre-Windows 2000 servers *over* Permissions compatible only with Windows 2000 servers to be compatible with our NT server programs. Click Next to continue.

Step 10. In Figure 1.6, specify an administrator password to use when starting the computer in restore mode; then click Next.

Step 11. In the next window, review and confirm the previously selected options; then click Next. The wizard will configure Active Directory, as shown in Figure 1.7.

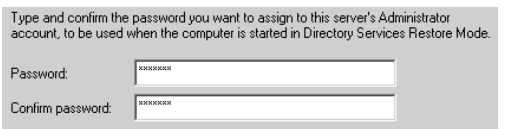

Figure 1.6 Specifying an administrator password for directory restore mode.

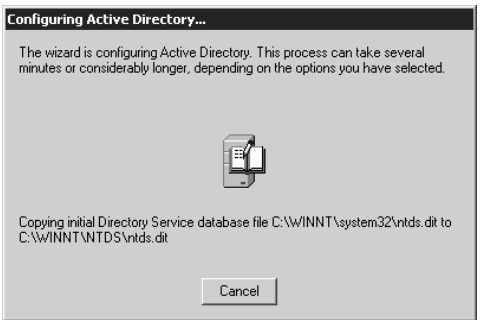

Figure 1.7 Configuring the Active Directory installation.

Step 12. In the next window, click Finish to close the wizard; then click Restart Now to reboot the server.

Now you're ready to learn how to manage Active Directory.

Managing Active Directory

From Start/Programs/Administrative Tools/Configure Your Server, start the wizard again by clicking Active Directory in the menu listing on the left (refer back to Figure 1.1). Click Manage user accounts and group settings, shown in Figure 1.8, to start the Active Directory admin utility, shown in Figure 1.9. This utility is used to manage domain controllers, user accounts, computer accounts, groups, organizational units, and published resources. We'll begin our investigation of these processes by learning how to manage domain controllers.

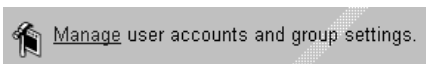

Figure 1.8 Starting the Active Directory admin utility.

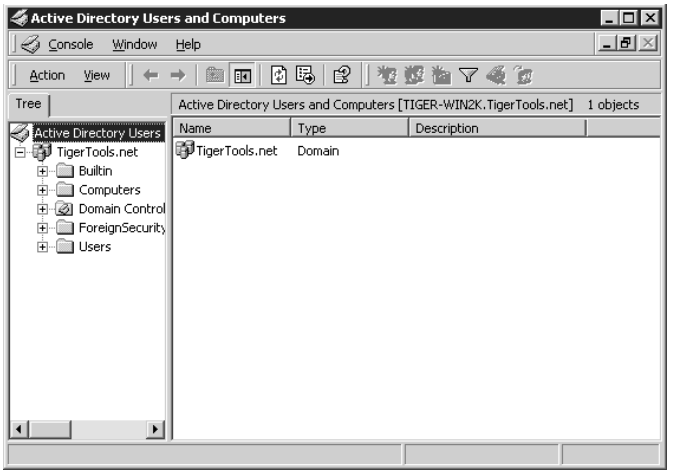

Figure 1.9 Active Directory admin utility.

Managing Domain Controllers

To find a domain controller by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, right-click any node or folder; then click Find.

Step 2. Under Find, click Computers; in Role, click Domain Controller (see Figure 1.10). If you know which folder contains the domain controller, click the folder in the In field; to search the entire directory, click Entire Directory.

Step 3. Click the Find Now button.

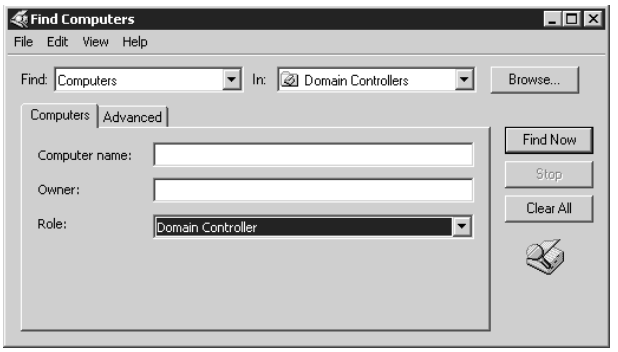

Figure 1.10 Searching for a domain controller.

You can delegate administrative control of a particular domain or organizational unit to individual administrators who are responsible for only that domain or organizational unit. To delegate control by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node to expand the domain tree.

Step 2. Right-click the folder that you want another user or group to control; then click Delegate Control to start the Delegation of Control wizard, whose welcome page is shown in Figure 1.11. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory. Click Next to begin the wizard.

Step 3. Click Add and/or select one or more users or groups to which you want to delegate control (see Figure 1.12); then click Next.

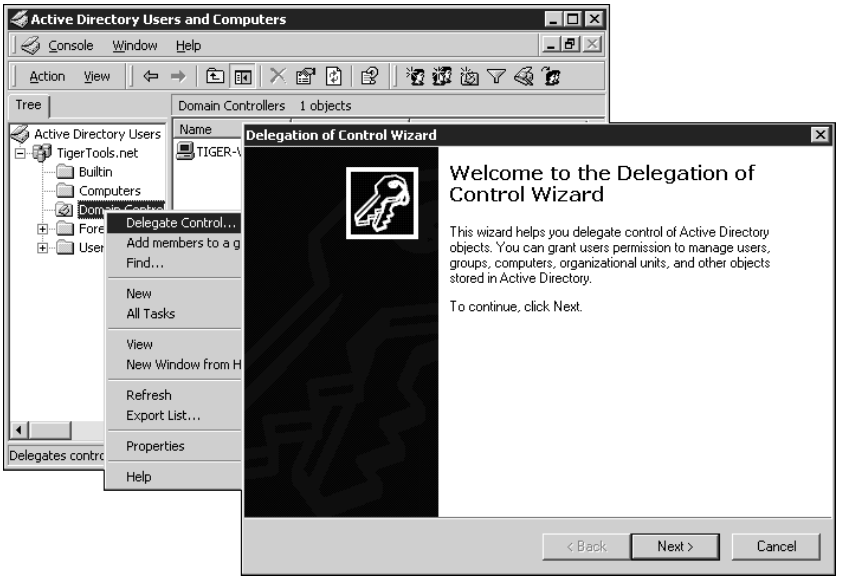

Figure 1.11 Delegation of Control wizard.

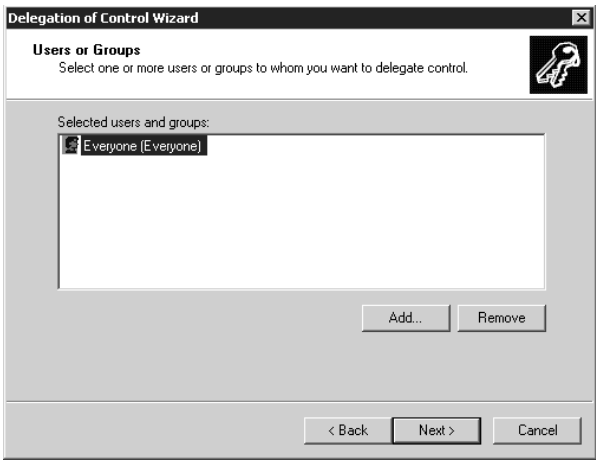

Figure 1.12 Selecting to whom to delegate control.

Step 4. Select from the common-task list shown in Figure 1.13 or select Create a custom task to delegate to customize your own. When you're finished, click Next and then Finish to complete the control delegation.

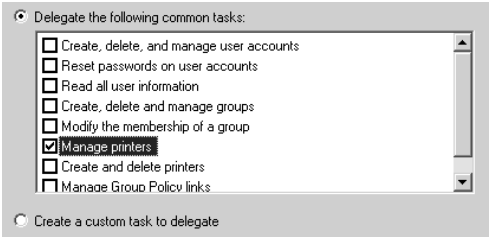

Figure 1.13 Selecting control from the common tasks list.

By default, domain controllers are installed in the Domain Controllers folder. Certain properties (e.g., Name, Role, and Operating System) are automatically assigned when the computer is added to the domain or whenever it is started, and these properties cannot be modified by the administrator. Other domain controller properties can be modified by using the Active Directory admin utility. To do so, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. Click the folder containing the domain controller. In the details panel, right-click the domain controller that you want to modify; then click Properties. As you can see in Figure 1.14, the following property tabs will be displayed:

- General
- Operating System
- Member Of
- Location
- Managed By

Step 3. Click the property tab that contains the property you want to modify.

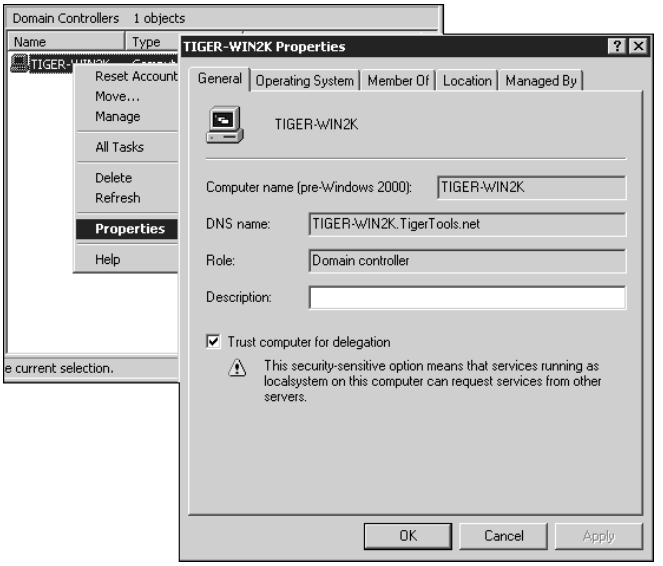

Figure 1.14 Modifying domain controller properties.

Managing User and Computer Accounts

Microsoft defines Active Directory user and computer accounts as representing physical entities such as a computer or a person. Accounts provide security credentials for users or computers, enabling those users and computers to log on to the network and access domain resources. An account is used to:

- Authenticate the identity of the user or computer
- Authorize access to domain resources
- Audit actions performed using the user or computer account

An Active Directory user account enables a user to log on to computers and domains with an identity that can be authenticated and authorized for access to domain resources. Each user who logs on to the network should have his or her own unique user account and password. User accounts can also be used as service accounts for some applications.

By default, Windows 2000 provides predefined user accounts, known as *Administrator* and *Guest* accounts, that you can use for logging on to a computer that is running Windows 2000. Predefined accounts are designed to let users log on to a local computer and access resources from that computer. As such, these accounts are designed primarily for initial logon and configuration of a local computer. Each predefined account has a different combination of rights and permissions. As you might assume, the Administrator account has the most extensive rights and permissions; the Guest account, the least.

Though convenient, predefined accounts pose a significant problem: If their rights and permissions are not modified or disabled by a network administrator, they could be used by any user or service to log on to a network by using the Administrator or Guest identity. To implement the security of user authentication and authorization, you must create an individual user account for each user who will participate, by way of the Active Directory Users and Computers utility, on your network. Each user account (including the Administrator and Guest accounts) can then be added to Windows 2000 groups to control the rights and permissions assigned to the account. Using accounts and groups that are appropriate for your network ensures that users logging on to a network can be identified and can access only the permitted resources.

Each Active Directory user account has a number of security-related options that determine how someone logging on with that particular user account is authenticated on the network. Several of these options are specific to passwords:

- User must change password at next logon.
- User cannot change password.
- Password never expires.
- Password is saved as encrypted clear text.

These options are self-explanatory except for the last one. If you have users logging on to your Windows 2000 network from Apple computers, you should select this option for those user accounts.

User and computer accounts are added, disabled, reset, and deleted with the Active Directory Users and Computers utility. Note the following in regard to these actions:

- If you create a new user account with the same name as that of a previously deleted user account, the new account will not automatically assume the permissions and memberships of the deleted account, because the security descriptor for each account is unique.
- To duplicate a deleted user account, all permissions and memberships must be manually re-created.

To add a user account by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node. In the details panel, right-click the organizational unit where you want to add the user, point to New, and click User (see Figure 1.15).

- In First name, type the user's first name.
- In Initials, type the user's initials.
- In Last name, type the user's last name.
- Modify Full name as desired.
- In User logon name, type the name with which the user will log on, and from the drop-down list, click the user principal name (UPN) suffix that must be appended to the user logon name (following the @ symbol). If the user will use a different name with which to log on from computers running Windows NT, Windows XP (which adds fast user switching), Windows Millennium, Windows 98, or Windows 95, change the user logon name as it appears in User logon name (pre-Windows 2000) to the different name.
- In Password and Confirm password, type the user's password.
- Select the appropriate password options.

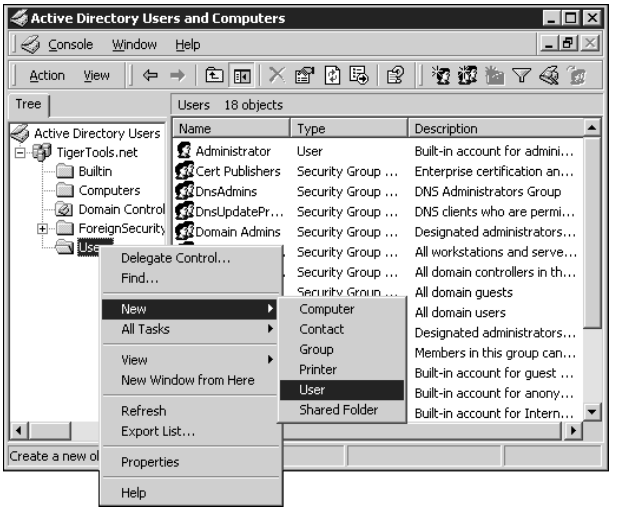

Figure 1.15 Adding a user account.

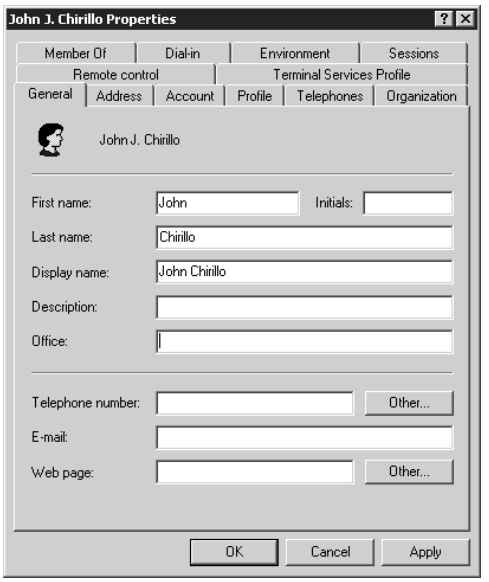

Figure 1.16 Editing a user account.

Step 2. After creating the user account, right-click the new user and click Properties to edit the user account and/or enter additional user account information, as shown in Figure 1.16. You can edit general user information, group memberships, dial-in access, terminal server access, and session settings.

Rather than deleting an unused user account, you can disable it as a security measure to prevent a particular user from logging on. Disabled accounts can also serve a useful purpose. Disabled user accounts with common group memberships can be used as account templates to simplify user account creation. Therefore, instead of manually creating the exact same type of account for, say, 20 new users, an account template can be copied, renamed, and activated for each. Doing so could save a great deal of administrative time.

To disable/enable a user account by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node to expand the domain tree.

Step 2. In the Console Tree, click Users or click the folder that contains the desired user account.

Step 3. In the details panel, right-click on the user and click Disable or Enable Account (see Figure 1.17).

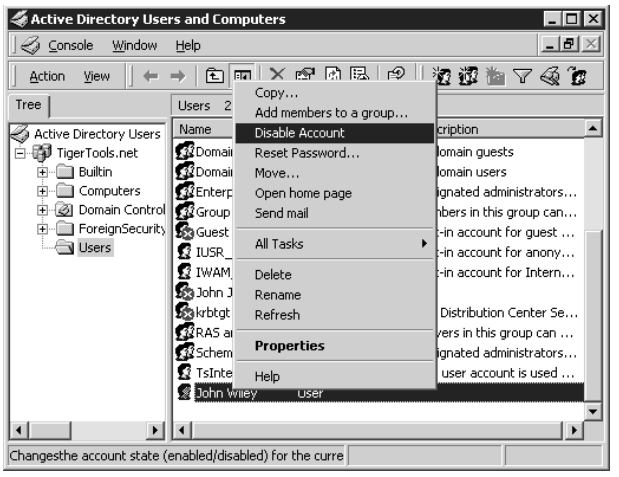

Figure 1.17 Enabling/disabling a user account.

To copy, delete, rename, or move a user account by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node to expand the domain tree.

Step 2. In the Console Tree, click Users or click the folder that contains the desired user account.

Step 3. In the details panel, right-click on the user and select the appropriate course of action.

Managing Computer Accounts

As set up by Microsoft, every computer running Windows 2000, Windows XP, or Windows NT that joins a domain has a computer account. Similar to user accounts, computer accounts provide a means for authenticating and auditing the computer's access to the network and to domain resources. Each computer connected to the network should have its own unique computer account.

By default, domain policy settings enable only domain administrators (members of the group Domain Admins) to add a computer account to a domain.

To add a computer account to a domain by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, click Computers or click the container (the directory service object that includes subcontainers for computer and user Group Policy information) in which you want to add the computer.

Step 2. Right-click Computers or the container in which you want to add the computer, point to New, and then click on the computer.

Step 3. Type the computer name (see Figure 1.18).

Step 4. Click the Change button to specify a different user or group that can add this computer to the domain.

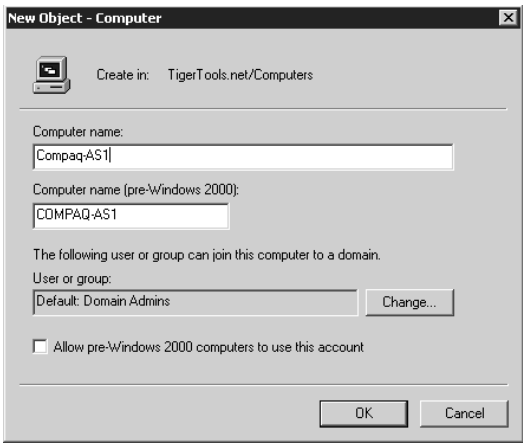

Figure 1.18 Adding a computer account to a domain.

To view or change the full computer name of a computer and the domain to which a computer belongs, on the desktop right-click My Computer, click Properties, and then click the Network Identification tab.

Group Policy settings are components of a user's desktop environment that a system administrator needs to manage—programs and Start menu options. Group Policy settings are contained in a Group Policy object, which is associated with selected Active Directory objects—sites, domains, or organizational units. They are settings for User or Computer Configuration, affecting users and computers, respectively.

Adding a computer to a group allows you to assign permissions to all of the computer accounts in that group and to filter Group Policy settings on all accounts in that group. To add a computer account to a group by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, click Computers or click the folder in which the computer is located.

Step 2. In the details panel right-click the computer, then click Properties (see Figure 1.19).

Step 3. Click the Member Of tab, then Add, then the group to which you want to add the computer, and then Add again. To add the computer to more than one group, press the Ctrl key and simultaneously click the groups to which you want to add the computer; then click Add.

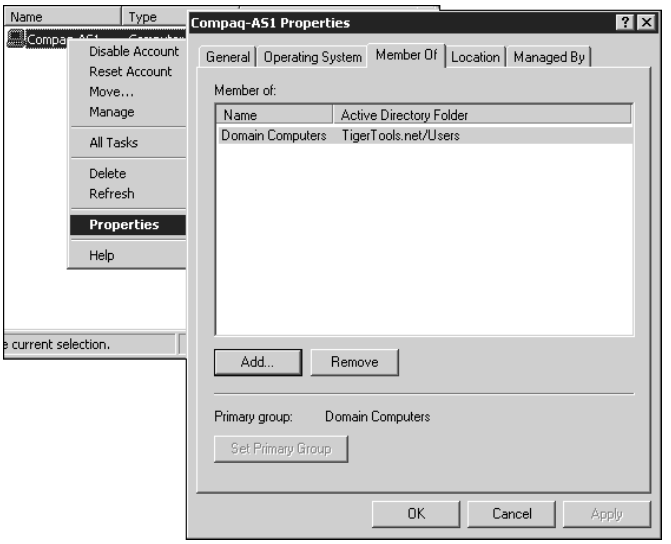

Figure 1.19 Adding a computer to a group.

To disable/enable, move, or delete a computer account by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, click Computers or click the folder in which the computer is located.

Step 2. In the details panel, right-click on the computer and select the appropriate course of action.

Managing Groups

Microsoft has set up two types of groups in Windows 2000: *security* and *distribution.* Security groups are listed in discretionary access control lists (DACLs) that define permissions on resources and objects. Security groups can also be used as an e-mail entity, which means that sending an e-mail message to the group sends the message to all members of the group.

In contrast, distribution groups are not security-enabled; they cannot be listed in DACLs. Distribution groups can be used only with e-mail applications (e.g., Exchange) to send e-mail to collections of users. If for security purposes you do not need a group, you would create a distribution group instead of a security group.

Each security group and distribution group has a scope that identifies the extent to which that group is applied in the domain tree or forest. There are three scopes: *universal*, *global*, and *domain local*.

- Groups with universal scope, or *universal groups*, can have as their members groups and accounts from any Windows 2000 domain in the domain tree or forest. They can be granted permissions in any domain in the domain tree or forest.
- Groups with global scope, or *global groups*, can have as their members groups and accounts only from the domain in which the group is defined. They can be granted permissions in any domain in the forest.
- Groups with domain local scope, or *domain local groups*, can have as their members groups and accounts from any Windows 2000 or Windows NT domain. They can be used to grant permissions within a domain only.

If you have multiple forests, users defined in only one forest cannot be placed into groups defined in another forest, and groups defined in only one forest cannot be assigned permissions in another forest.

The installation of a domain controller causes several default groups to be installed in the Built-in and Users folders of the Active Directory Users and Computers console. These are security groups that represent common sets of rights and permissions that you can use to grant certain roles, rights, and permissions to the accounts and groups that you place into the default groups.

Default groups with domain local scope are located in the Built-in folder. Predefined groups with global scope are located in the Users folder. You can move the domain local and predefined groups to other group or organizational unit folders within the domain, but you cannot move them to other domains.

The default groups placed into the Built-in folder for Active Directory Users and Computers are:

- Account Operators
- Administrators
- Backup Operators
- Guests
- Print Operators
- Replicators
- Server Operators
- Users

These built-in groups have domain local scope and are primarily used to assign default sets of permissions to users who will have some administrative control in that domain. For example, the Administrators group in a domain has a broad set of administrative authority over all accounts and resources in the domain.

In addition to the groups in the Built-in and Users folders, Windows 2000 Server includes three special identities. For convenience, these identities, too, are generally called groups. These special groups do not have specific memberships that you can modify, but they can represent different users at different times, depending on the circumstances. The three special groups are:

Everyone. Represents all current network users, including guests and users from other domains. Whenever users log on to the network, they are automatically added to the Everyone group.

Network. Represents users currently accessing a given resource over the network (as opposed to users who access a resource by logging on locally at the computer where the resource is located). Whenever users access a given resource over the network, they are automatically added to the Network group.

Interactive. Represents all users currently logged on to a particular computer and accessing a given resource located on that computer (as opposed to users who access the resource over the network). Whenever users access a given resource on the computer to which they are currently logged on, they are automatically added to the Interactive group.

Although the special identities can be assigned rights and permission to resources, as stated, you cannot modify or view the memberships of these special identities. You do not see them when you administer groups, and you cannot place the special identities into groups. Group scopes do not apply to special identities. Users are automatically assigned to these special identities whenever they log on to or access a particular resource.

By using *nesting*, you can add a group as a member of another group. You can nest groups to consolidate group management by increasing the affected member accounts and to reduce replication traffic caused by replication of group membership changes. Your nesting options depend on whether the domain is *native-mode* (composed of Windows 2000 systems) or *mixed-mode* (composed of both Windows NT and Windows 2000 systems). Groups in native-mode domains or distribution groups in mixed-mode domains have their membership determined as follows:

- Groups with universal scope can have as their members the following: user accounts, computer accounts, other groups with universal scope, and groups with global scope from any domain.
- Groups with global scope can have as their members the following: accounts from the same domain and other groups with global scope from the same domain.
- Groups with domain local scope can have as their members the following: user and/or computer accounts, groups with universal scope, and groups with global scope, all from any domain. They can also have as members other groups with domain local scope from within the same domain.

Security groups in a mixed-mode domain are restricted to the following types of membership:

- Groups with global scope can have as members only user and/or computer accounts.
- Groups with domain local scope can have as their members other groups with global scope and accounts.

Security groups with universal scope cannot be created in mixed-mode domains, because universal scope is supported only in Windows 2000 native-mode domains.

To create a group to assign permissions to all the computer accounts in that group, and to filter Group Policy settings on all accounts in that group by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. Right-click the folder in which you want to add the group, point to New, and then click Group.

Step 3. Type the name of the new group. By default, the name you type is also entered as the pre-Windows 2000 name of the new group (see Figure 1.20).

Step 4. Click the Group scope and the Group type you want.

Step 5. Click OK.

If the domain in which you are creating the group is in the mixed-mode, you can only select security groups with domain local or global scopes.

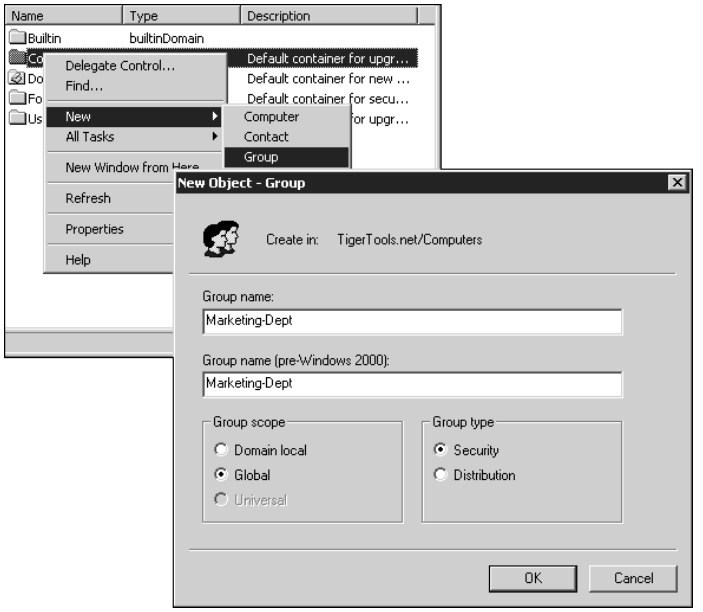

Figure 1.20 Adding a group.

Step 6. (optional) To add a member to the group, right-click the new group name, click Properties, then click the Members tab followed by Add. Finally, click the users and computers to be added, then click Add again.

To move, delete, or rename a group by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. Click the folder that contains the group.

Step 3. In the details panel, right-click the group and select the appropriate course of action.

Managing Organizational Units

According to Microsoft, a particularly useful type of directory object contained within domains is the *organizational unit*. Organizational units are Active Directory containers into which you can place users, groups, computers, and other organizational units.

NOTE An organizational unit may not contain objects from other domains.

An organizational unit is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority. By using organizational units, you can create containers within a domain that represent the hierarchical, logical structures within your organization. Doing so enables you to manage the configuration and use of accounts and resources based on your organizational model. A hierarchy of containers can be extended as necessary to model your organization's hierarchy within a domain. Using organizational units will help you minimize the number of domains required for your network.

You can also use organizational units to create an administrative model that can be scaled to any size. A user can be granted administrative authority for all organizational units in a domain or for a single organizational unit. An administrator of an organizational unit does not need to have administrative authority for any other organizational units in the domain.

To add an organizational unit by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. Right-click the domain node or the folder in which you want to add the organizational unit, point to New, and then click Organizational Unit.

Step 3. Type the name of the organizational unit (see Figure 1.21).

Step 4. Click OK.

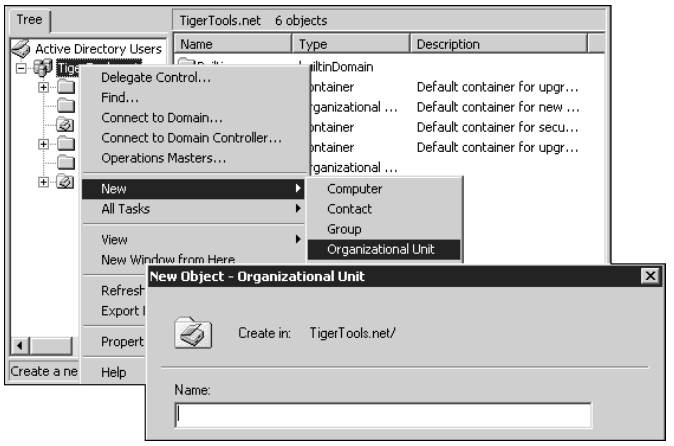

Figure 1.21 Adding an organizational unit.

To modify an organizational unit's properties, in the details panel follow these steps:

Step 1. Right-click the organizational unit and click Properties (see Figure 1.22).

Step 2. Customize the unit's properties, and when you're done, click OK.

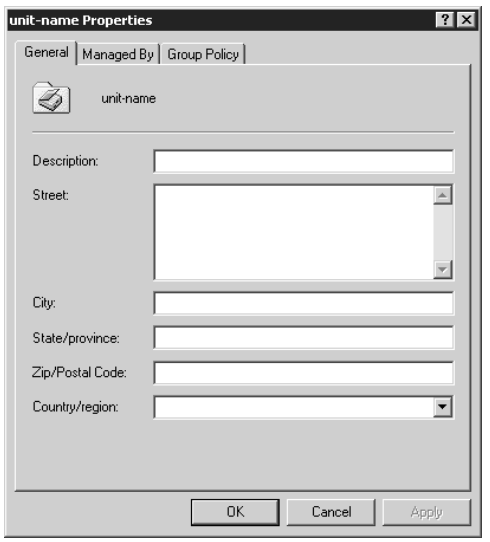

Figure 1.22 Modifying the properties of an organizational unit.

To delegate control of an organizational unit by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. In the details panel, right-click the organizational unit and click Delegate control to start the Delegation of Control wizard. Follow the instructions in the Delegation of Control wizard as previously described in the "Managing Domain Controllers" section.

To move, delete, or rename an organizational unit by using the Active Directory admin utility, follow these steps:

Step 1. In the Console Tree, double-click the domain node.

Step 2. Click the folder that contains the group.

Step 3. In the details panel, right-click the organizational unit and select the appropriate course of action.

Managing Domains and Trusts

Microsoft explicitly states that in Active Directory, each user account has a UPN that is based on the Internet Engineering Task Force (IETF) RFC 822, "Standard for the Format of ARPA Internet Text Messages." The UPN has two parts: the prefix (a user logon name) and the suffix (a domain name). These parts are joined by the `@` symbol to form the complete UPN.

For existing Windows NT accounts, the first part of the UPN, the user logon name, is by default the same as the name used to log on to a Windows NT 4.0 domain. For new Windows 2000 user accounts, the user logon name must be created and assigned by an administrator.

The second part of the UPN, the UPN suffix, identifies the domain in which the user account is located. This second part can be the DNS domain name or an alternative name created by an administrator and used just for logon purposes. This logon name does not need to be a valid DNS name.

In Active Directory, the default UPN suffix is the DNS name of the root domain in the domain tree. In most cases, this is the domain name registered as the enterprise domain on the Internet. Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest.

For example, if your organization uses a deep domain tree, organized by department and region, domain names can become quite long. The default UPN for a user in that domain might be sales.westcoast.microsoft.com. The logon name for a user in that domain would be `user@sales.westcoast.microsoft.com`. Creating a UPN suffix of `microsoft` would allow that same user to log on with the much simpler logon name of `user@microsoft.com`.

You can add or remove UPN suffixes by using the Active Directory Domains and Trusts utility. To add UPN suffixes, follow these steps:

Step 1. From Start/Programs/Administrative Tools, click Active Directory Domains and Trusts.

Step 2. In the Console Tree, right-click Active Directory Domains and Trusts; then click Properties.

Step 3. Click on the UPN Suffixes tab, type an alternative UPN suffix for the domain, and then click Add (see Figure 1.23). Repeat this step to add additional alternative UPN suffixes.

Step 4. Click Apply and OK.

A *domain trust* is a relationship established between two domains that enables users in one domain to be authenticated by a domain controller in another domain. All domain trust relationships have only two domains in the relationship: the trusting domain and the trusted domain.

In earlier versions of Windows, trusts were limited to the two domains involved in the trust, and the trust relationship was one-way. In Windows 2000, all trusts are transitive and two-way. Both domains in a trust relationship automatically trust each other.

As an example, given domains A, B, and C, if domain A trusts domain B and if domain B trusts domain C, users from domain C (when granted the proper permissions) can access resources in domain A. The fact that a user is authenticated by a domain controller does not imply any access to resources in that domain. Rather, it is determined solely by the rights and permissions granted to the user account by the domain administrator for the trusting domain.

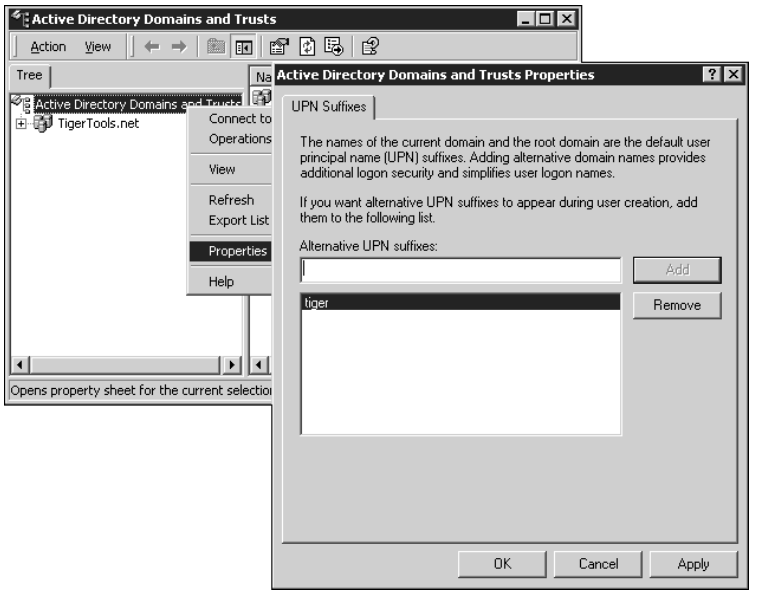

Figure 1.23 Adding UPN suffixes.

Explicit trusts are trust relationships that you create yourself, as opposed to trusts created automatically during installation of a domain controller. You create and manage explicit trusts using the Active Directory Domains and Trusts utility. There are two kinds of explicit trusts: *external* and *shortcut*. External trusts enable user authentication to a domain outside of a forest.

External trusts establish trust relationships to domains outside the forest. The benefit of creating external trusts is to enable user authentication to a domain not encompassed by the trust paths of a forest. All external trusts are one-way nontransitive trusts. You can combine 2 one-way trusts to create a two-way trust relationship.

Before an account can be granted access to resources by a domain controller of another domain, Windows 2000 must determine whether the domain containing the desired resources (the *target domain*) has a trust relationship with the domain in which the account is located (the *source domain*). To make this determination for two domains in a forest, Windows 2000 computes a *trust path* between the domain controllers for these source and target domains. A trust path is the series of domain trust relationships that must be traversed by Windows 2000 security to pass authentication requests between any two domains. Computing and traversing a trust path between domain trees in a complex forest can take time, although the amount of time can be reduced with shortcut trusts.

Shortcut trusts are two-way transitive trusts that enable you to shorten the path in a complex forest. You explicitly create shortcut trusts between Windows 2000 domains in the same forest. A shortcut trust is a performance optimization that shortens the trust path for Windows 2000 security to take for authentication purposes. The most effective use of shortcut trusts is between two domain trees in a forest. You can also create multiple shortcut trusts between domains in a forest, if necessary.

To create an explicit trust, you must know the domain names and a user account with permission to create trusts in each domain. Each trust is assigned a password that must be known to the administrators of both domains in the relationship. To create an explicit domain trust by using the Active Directory admin utility, follow these steps:

Step 1. From Start/Programs/Administrative Tools, click Active Directory Domains and Trusts.

Step 2. In the Console Tree, right-click the domain node for the domain you want to administer; then click Properties.

Step 3. Click the Trusts tab (see Figure 1.24).

Step 4. Depending on your requirements, in either Domains trusted by this domain or Domains that trust this domain, click Add. If the domain to be added is a Windows 2000 domain, type the full DNS name of the domain; if the domain is running an earlier version of Windows, type the domain name.

Step 5. Type the password for this trust, confirm the password, and click OK.

Repeat this procedure on the domain that forms the second half of the explicit trust relationship. And, note, the password must be accepted in both the trusting and trusted domains.

To verify/revoke a trust, click the trust to be verified, click Edit, and then click Verify/Reset.

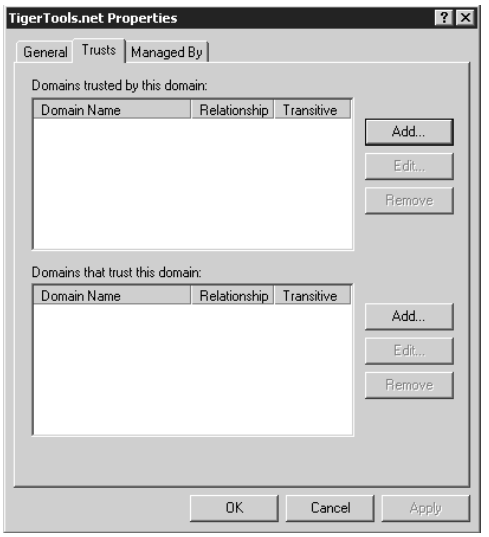

Figure 1.24 Creating an explicit domain trust.

TCP/IP Customization

The Networking Configuration wizard, accessible from Start/Programs/Administrative Tools/Configure Your Server, allows for the configuration of most of the services we're exploring in this chapter. Typically, during the standard Windows 2000 Server installation, simple TCP/IP services—including NIC configurations using a Dynamic Host Configuration Protocol (DHCP) client—are installed. In this section, you'll learn how to customize that configuration to conform to your own network operating standards.

To begin, from Start/Settings/Control Panel/Network and Dial-up Connections, double-click Local Area Connection (see Figure 1.25) to access the Local Area Connection Status box. You'll notice immediately the general packet-activity status (helpful when troubleshooting connectivity) and that you have the capability to halt communications by clicking Disable.

Next to the Disable button is the Properties button, which we'll use to customize TCP/IP configuration. Click on Properties to open the Local Area Network Connection Properties window shown in Figure 1.26. To configure TCP/IP for static addressing, on the General tab (for a local area connection) or the Networking tab (for all other

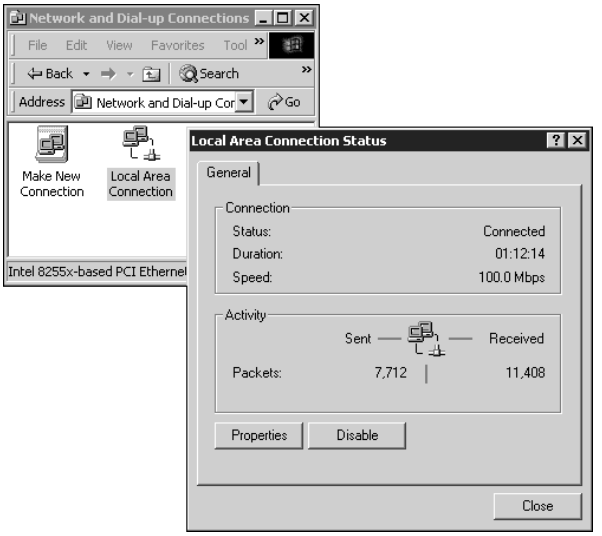

Figure 1.25 Simple TCP/IP management utility.

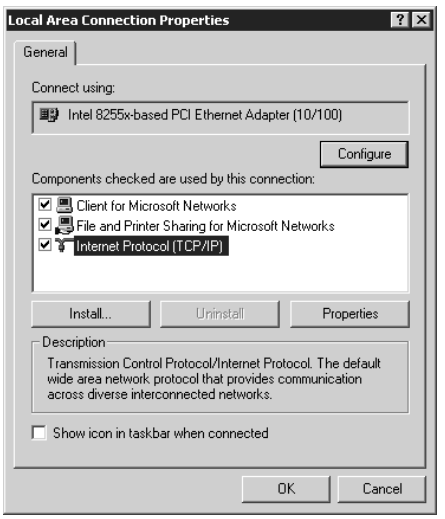

Figure 1.26 Local Area Connection Properties window.

connections), click to select Internet Protocol (TCP/IP) and then click Properties. That will lead you to the screen shown in Figure 1.27. From there do the following:

Step 1. In the IP Properties screen, click Use the following IP address: and do one of the following:

- For a local area connection, type the IP address, subnet mask, and default gateway addresses in the appropriate fields.
- For all other connections, type the IP address in that field.

Step 2. Click Use the following DNS server addresses: In Preferred DNS server and Alternate DNS server, type the primary and secondary DNS server addresses.

Step 3. To configure advanced settings, click Advanced to reach the Advanced TCP/IP Settings screen shown in Figure 1.28. Then do one or more of the following:

- To configure additional IP addresses, in the IP Settings tab window, in the IP addresses box, click Add. In the IP Address and Subnet mask columns, type an IP address and subnet mask; then click Add. Repeat this step for each IP address you want to add. Click OK when you're done.
- To configure additional default gateways, in the IP Settings tab window, in the Default gateways box, click Add. In the Gateway and Metric columns, type the IP address of the default gateway and the metric; then click Add. (As a memory jogger, a gateway is the device (i.e., router) that links two networks together; the metric is the number of gateways traversed before the specified gateway is reached.) Repeat this step for each default gateway you want to add. Click OK when you're done.
- To configure a custom metric for this connection, type a metric value in Interface metric.

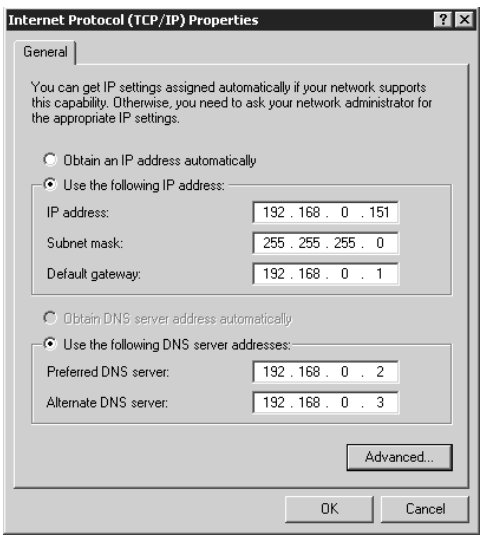

Figure 1.27 Configuring static IP addressing.

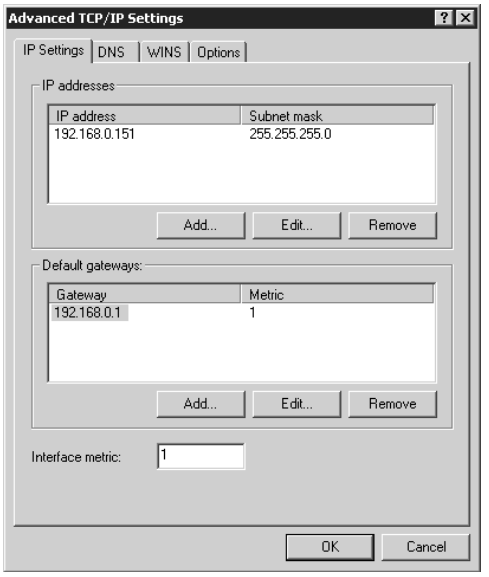

Figure 1.28 Configuring advanced TCP/IP settings.

Step 4. Optionally, you can configure TCP/IP to use WINS. To do that, click the WINS tab to access the screen shown in Figure 1.29; then click Add. In TCP/IP WINS server, type the IP address of the WINS server; then click Add. Repeat this step for each WINS server IP address you want to add. Click OK when you're done.

- To enable the use of the LMHOSTS file to resolve remote NetBIOS names, select the Enable LMHOSTS lookup checkbox. This option is enabled by default.
- To specify the location of the file that you want to import into the LMHOSTS file, click Import LMHOSTS and select the file in the Open dialog box.
- To modify the behavior of NetBIOS over TCP/IP behavior by enabling the use of NetBIOS over TCP/IP, click Enable NetBIOS over TCP/IP.
- To modify the behavior of NetBIOS over TCP/IP behavior by disabling the use of NetBIOS over TCP/IP, click Disable NetBIOS over TCP/IP.
- To have the DHCP server determine the NetBIOS behavior, click Use NetBIOS setting from the DHCP server.

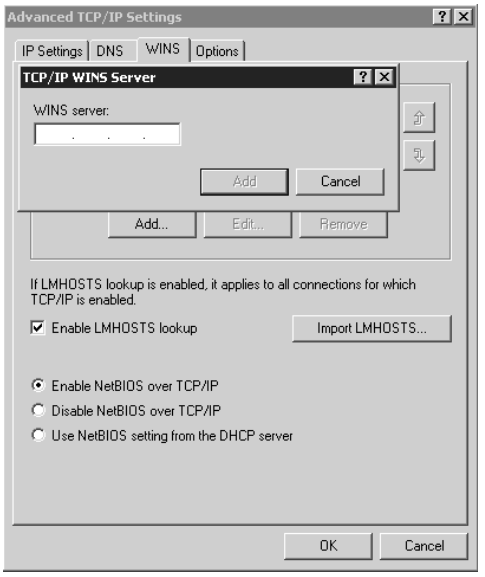

Figure 1.29 Configuring WINS.

Step 5. Optionally, you can configure TCP/IP to use an Internet Protocol Security (IPSec) policy. IPSec is an easy-to-use yet aggressive protection mechanism against private network and Internet attacks. It is a suite of cryptography-based protection services and security protocols with end-to-end security. IPSec is also capable of protecting communications between workgroups, LAN computers, domain clients and servers, branch offices that may be physically remote, extranets, roving clients, and remote administration of computers. To add IPSec, click on the Options tab, click IP security, and then click Properties to reach the IP Security window (see Figure 1.30). To enable IP security, click Use this IP security policy; then click on the name of a policy. To disable IP security, click Do not use IPSEC. Click OK when you're done.

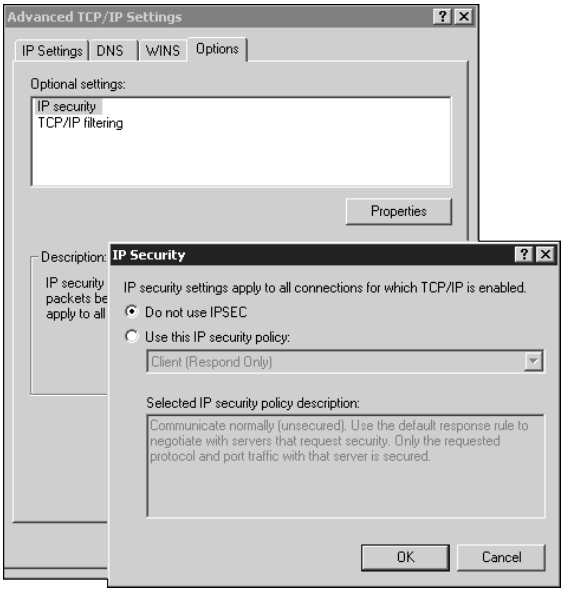

Figure 1.30 Configuring IPSec.

Step 6. TCP/IP filtering is a security measure that specifies the types of incoming traffic that are to be passed to the TCP/IP protocol suite for processing. You can opt to configure TCP/IP to use TCP/IP filtering. To do so, in the Options tab window click TCP/IP filtering and then Properties (see Figure 1.31).

- To enable TCP/IP filtering for all adapters, select the Enable TCP/IP Filtering (All adapters) checkbox.
- To disable TCP/IP filtering for all adapters, clear the Enable TCP/IP Filtering (All adapters) checkbox.

Based on your requirements for TCP/IP filtering, configure TCP ports, UDP ports, or IP protocols for the allowed traffic. Click OK when you're done.

Step 7. Click OK again; then click Close to finish.

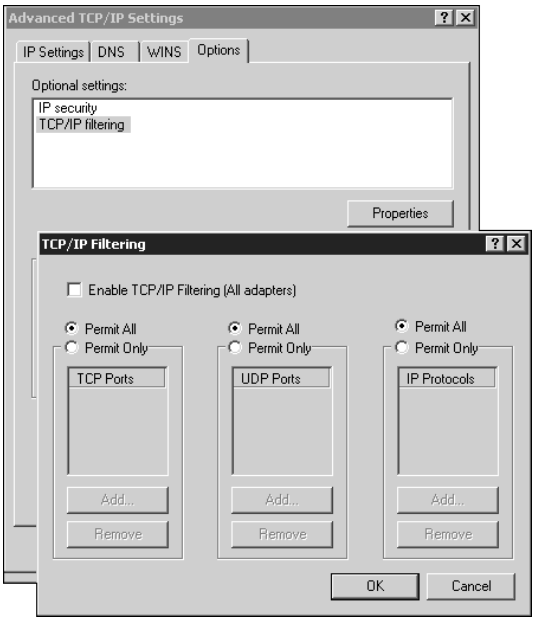

Figure 1.31 Configuring TCP/IP filtering.

Domain Name Service

As defined earlier, DNS is a system for naming computers and network services. For example, most users prefer an easy-to-remember name such as example.microsoft.com to locate a computer—say, a mail or Web server on a network. However, computers communicate over a network by using numeric addresses, which are more difficult for users to remember. In short, name services such as DNS provide a way to map the user-friendly name for a computer or service to its numeric address. If you have ever used a Web browser, you used DNS.

Windows 2000 provides a number of utilities for administering, monitoring, and troubleshooting both DNS servers and clients. These utilities include:

- The DNS console, which is part of Administrative Tools.
- Command-line utilities, such as nslookup, which can be used to troubleshoot DNS problems.
- Logging features, such as the DNS server log, which can be viewed by using Event Viewer. File-based logs can also be used temporarily as an advanced debugging option to log and trace selected service events.
- Performance-monitoring utilities, such as statistical counters to measure and monitor DNS server activity with System Monitor.

DNS Console

The primary tool that you use to manage Windows 2000 DNS servers is the DNS console, which is provided in the Administrative Tools folder in Control Panel. The DNS console appears as a Microsoft Management Console (MMC) snap-in, to further integrate DNS administration to your total network management.

The DNS console provides new ways to perform familiar DNS administrative tasks previously handled in Windows NT Server 4.0 using DNS Manager. For Windows 2000 Server, the DNS console appears after a DNS server is installed. To use the DNS console from another nonserver computer, such as one running Windows 2000 Professional, you must install the Administrative Tools pack.

Command-Line Utilities

Windows 2000 provides several command-line utilities. You can use them to manage and troubleshoot DNS servers and clients. The following list describes each of these utilities, which can be run either by typing them at a command prompt or by entering them in batch files for scripted use.

nslookup. Used for performing query testing of the DNS domain namespace.

dnscmd. A command-line interface used for managing DNS servers. It is useful in scripting batch files to help automate routine DNS management tasks or for performing simple, unattended setup and configuration of new DNS servers on your network.

ipconfig. Used for viewing and modifying IP configuration details used by the computer. For Windows 2000, additional command-line options are included with this utility to provide help in troubleshooting and supporting DNS clients.

DNS Management Console

Here, we'll use the DNS console to accomplish the following basic administrative server tasks:

- Connecting to and managing a local DNS server on the same computer or on remote DNS servers on other computers.
- Adding and removing forward and reverse lookup zones as needed.
- Adding, removing, and updating resource records (RRs) in zones.
- Modifying security for specific zones or RRs.

In addition, you'll learn to use the DNS console to perform the following tasks:

- Performing maintenance on the server. You can start, stop, pause, or resume the server, or you can manually update server data files.
- Monitoring the contents of the server cache and, as needed, clearing it.
- Tuning advanced server options.
- Configuring and performing aging and scavenging of stale RRs stored by the server.

To open the DNS management console, click Start/Programs/Administrative Tools/DNS (see Figure 1.32).

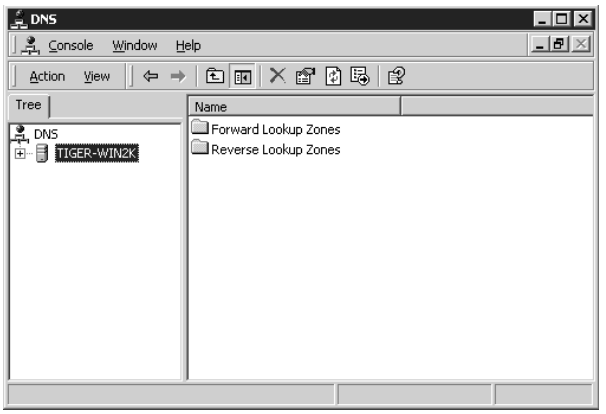

Figure 1.32 The DNS management console.

To start, stop, pause, resume, or restart a DNS server from the console, in the Console Tree click the applicable DNS server, and on the Action menu point to All Tasks and click one of the following:

- To start the service, click Start.
- To stop the service, click Stop.
- To interrupt the service, click Pause.
- To stop and then automatically restart the service, click Restart.

After you pause or stop the service, on the Action menu, in All Tasks, you can click Resume to immediately continue service. You can also perform most of these tasks at a command prompt by using the following commands:

```
net start dns
net stop dns
net pause dns
net continue dns
```

Adding Forward and Reverse Lookup Zones

DNS allows a namespace to be divided into *zones*, which store name information about one or more DNS domains. Each zone in which a DNS domain name is becomes the authoritative source for information about that domain.

A zone starts as a storage database for a single DNS domain name. Other domains added below the domain used to create the zone can either be part of the same zone or belong to another zone. Once a subdomain is added, it can then either be managed and included as part of the original zone records or be delegated to another zone created to support the subdomain.

For example, if the microsoft.com zone does not use delegation for a subdomain, any data for the subdomain will remain part of the microsoft.com zone. Thus, the subdomain dev.microsoft.com is not delegated away but is managed by the microsoft.com zone.

Because zones play an important role in DNS, they are intended to be available from more than one DNS server on the network to provide availability and fault tolerance when they resolve name queries. Otherwise, if a single server is used and that server is not responding, queries for names in the zone can fail. For additional servers to host a zone, zone transfers are required to replicate and synchronize all copies of the zone used at each server configured to host the zone.

When a new DNS server is added to the network and is configured as a new secondary server for an existing zone, it will perform a full initial transfer of the zone to obtain and replicate a full copy of the zone's RRs. For most earlier DNS server implementations, this same method of full transfer for a zone is also used when the zone requires updating after changes are made to it. For Windows 2000 Server, the DNS service supports *incremental zone transfer* (IXFR), a revised DNS zone transfer process for intermediate changes.

NOTE IXFRs are described in RFC 1995, an additional DNS standard for replicating DNS zones. RFC 1995 provides a more efficient method of propagating zone changes and updates when IXFRs are supported by a DNS server acting as the source for a zone, as well as by any servers that copy the zone from it.

In earlier DNS implementations, any request for an update of zone data required a full transfer of the entire zone database by way of an *all zone transfer* (AXFR) query or an IXFR query. The IXFR allows the secondary server to pull only those zone changes that it needs to synchronize its copy of the zone with its source, either a primary or secondary copy of the zone maintained by another DNS server.

With IXFRs, differences between the source and replicated versions of the zone are first determined. If the zones are identified to be the same version—as indicated by the serial number field in the start-of-authority (SOA) RR of each zone—no transfer will be made.

If the serial number for the zone at the source is greater than at the requesting secondary server, a transfer is made of only those changes to RRs for each incremental version of the zone. For an IXFR query to succeed and for changes to be sent, the source DNS server for the zone must keep a history of incremental zone changes to use when it answers these queries. The incremental transfer process requires substantially less traffic on a network, and zone transfers are completed much faster.

A zone transfer might occur during any of the following scenarios:

- When the refresh interval expires for the zone
- When a secondary server is notified of zone changes by its master server
- When the DNS server service is started at a secondary server for the zone
- When the DNS console is used at a secondary server for the zone to manually initiate a transfer from its master server

Zone transfers are always initiated at the secondary server for a zone and sent to their configured master servers, which act as their source for the zone. Master servers can be any other DNS server that loads the zone, such asthe primary server for the zone or another secondary server. When the master server receives the request for the zone, it can reply with either an IXFR or an AXFR of the zone to the secondary server.

During new configuration, the destination server sends anAXFR request to the master DNS server configured as its source for the zone. The master (source) server responds and fully transfers the zone to the secondary (destination) server.

The zone is delivered to the destination server requesting the transfer with its version established by use of a serial number field in the properties for the SOA RR. The SOA RR also contains a stated refresh interval (900 sec, or 15 min, by default) to indicate when the destination server should next request to renew the zone with the source server.

When the refresh interval expires, an SOA query will be used by the destination server to request renewal of the zone from the source server. The source server answers the query for its SOA record. This response contains the serial number for the zone in its current state at the source server.

The destination server checks the serial number of the SOA record in the response and determines how to renew the zone. If the value of the serial number in the SOA response is equal to its current local serial number, the destination server concludes that the zone is the same at both servers and that a zone transfer is not needed. The destination server then renews the zone by resetting its refresh interval based on the value of this field in the SOA response from its source server.

If the value of the serial number in the SOA response is higher than its current local serial number, it will conclude that the zone has been updated and that a transfer is needed. If the destination server concludes that the zone has changed, it will send to the source server an IXFR query containing its current local value for the serial number in the SOA record for the zone. The source server responds with either an incremental or a full transfer of the zone. If the source server supports incremental transfer by maintaining a history of recent incremental zone changes for modified RRs, it can answer with an IXFR of the zone. If the source server does not support IXFR or does not have a history of zone changes, it can answer with an AXFR of the zone instead.

IXFR through IXFR query is supported for Windows 2000 Server. For earlier versions of the DNS service running on Windows NT Server 4.0, as well as for many other DNS server implementations, IXFR is not available; in these versions, only full-zone (i.e., AXFR) queries and transfers are used to replicate zones.

Windows DNS servers support DNS Notify, an update to the original DNS protocol specification that permits a means of initiating notification to secondary servers when zone changes occur (RFC 1996). DNS notification implements a push mechanism for notifying a select set of secondary servers for a zone when the zone is updated. Servers that are notified can then initiate zone transfers, as just described, to pull zone changes from their master servers and update their local replicas of the zone.

For secondaries to be notified by the DNS server acting as their configured source for a zone, each secondary server must first have its IP address in the notify list of the

source server. When the DNS console is used to manage zones loaded at Windows 2000 DNS servers, this list is maintained in the Notify dialog box, which is accessible from the Zone Transfer tab located in Zone Properties.

In addition to notifying the listed servers, the DNS console permits you to use the contents of the notify list as a means of restricting zone transfer access to only those secondary servers specified in the list. These restrictions can help prevent an undesired attempt by an unknown or unapproved DNS server to pull, or request, zone updates. The following is a brief summary of the typical DNS notification process for zone updates:

Step 1. The local zone at a DNS server acting as a master server, a source for the zone to other servers, is updated. When the zone is updated at the master or source server, the serial number field in the SOA RR will also be updated, indicating a new local version of the zone.

Step 2. The master server sends a DNS notify message to other servers that are part of its configured notify list.

Step 3. All secondary servers that receive the notify message can then respond by initiating a zone transfer request back to the notifying master server.

The normal zone transfer process can then continue, as described previously.

To add a forward lookup zone, from the DNS management console, in the Console Tree, click Forward Lookup Zones. On the Action menu, click New Zone to start the wizard. You can also right-click on Forward Lookup Zones and then click New Zone.

Step 1. Click Next to begin.

Step 2. Select the type of zone: Active Directory-integrated, Standard primary, or Standard secondary. For this example, choose Standard primary; then click Next.

Step 3. Enter the name of the zone; then click Next.

Step 4. Select whether to create a new zone file or use one previously created, click Next, and then click Finish.

To add a reverse lookup zone, from the DNS management console, in the Console Tree, click Reverse Lookup Zones; on the Action menu, click New Zone to start the wizard. You can also right-click on Reverse Lookup Zones and then click New Zone.

Step 1. Click Next to begin.

Step 2. Select the type of zone from Active Directory-integrated, Standard primary, or Standard secondary. As with the forward lookup zone, choose Standard primary and then click Next.

Step 3. To identify the zone, enter the network ID or the name of the zone; then click Next.

Step 4. Select whether to create a new zone file or use one previously created. Click Next; then click Finish.

Adding and Updating RRs in Zones

After you create a zone, additional RRs need to be added to it. The most common RRs you'll add are the following:

Host (A). For mapping a DNS domain name to an IP address used by a computer.

Alias (CNAME). For mapping an alias DNS domain name to another primary or canonical name.

Mail Exchanger (MX). For mapping a DNS domain name to the name of a computer that exchanges or forwards mail.

Pointer (PTR). For mapping a reverse DNS domain name based on the IP address of a computer that points to the forward DNS domain name of that computer.

Service location (SRV). For mapping a DNS domain name to a specified list of DNS host computers that offer a specific type of service, such as Active Directory domain controllers.

To add an RR—in this case, a host (A) RR to a zone—from the DNS console, in the Console Tree click the applicable forward lookup zone.

Step 1. On the Action menu, click New Host.

Step 2. In the Name text box, type the DNS computer name for the new host.

Step 3. In the IP address text box, type the IP address for the new host (see Figure 1.33). As an option, select the Create associated pointer (PTR) record checkbox to create an additional pointer record in a reverse zone for this host, based on the information you entered in the Name and IP address boxes.

Step 4. Click Add Host to add the new host record to the zone.

Step 5. Repeat the process or click Done to finish.

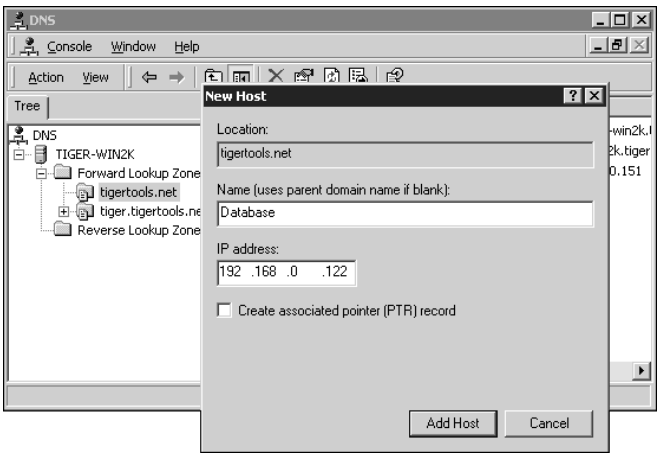

Figure 1.33 Creating a zone record.