CHAPTER
1

INTRODUCTION TO WINDOWS SERVER 2003

After reading this chapter and completing the exercises, you will be able to:

- Differentiate between the different editions of Windows Server 2003
- Explain Windows Server 2003 network models and server roles
- Identify concepts relating to Windows Server 2003 network management and maintenance
- Explain Windows Server 2003 Active Directory concepts

Windows Server 2003 network administration consists of two major goals. The first is to ensure that network resources such as files, folders, and printers are available to users whenever they need access. The second goal is to secure the network so that available resources are only accessible to users who have been granted the proper permissions.

To acquire the skills needed to meet your network administration goals, you need to understand a number of concepts, from the account creation process to server and resource management. A Windows Server 2003 network administrator also requires an understanding of **Active Directory (AD)** concepts and management, as well as general troubleshooting tools and techniques.

The first section of this chapter explains the main elements of the four Windows Server 2003 editions, including hardware specifications and supported features. Ultimately, the Windows Server 2003 edition best suited to a particular environment or server implementation will depend upon the performance, scalability, and reliability needs of an organization, along with the intended purpose of a particular system. In order to provide you with a better perspective on Windows networking concepts, the second section of this chapter introduces the different logical models used to group network resources, namely workgroups and domains. A look at member servers and domain controllers explains the roles of each type of server in a domain, and why an administrator might choose to configure a server in one role over another.

The third section of this chapter outlines the tasks network administrators are expected to understand and implement as part of managing and maintaining a Windows Server 2003 network. This section provides a basic outline of the concepts and procedures covered in the subsequent chapters of this book.

It is also essential to understand the basic concepts of Windows Server 2003 Active Directory and how it influences network management procedures because most network management tasks take place within domain environments. The final section of this chapter discusses Active Directory concepts and provides a solid foundation on which to build your network administration skills.To become a successful Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE), you need practical, hands-on experience with products like Microsoft Windows Server 2003. This book includes numerous hands-on activities and case studies to help ensure that you not only understand the theory behind the concepts covered but also that you feel comfortable carrying out common system administration tasks. To help simulate a real-world network environment, all of the activities in the book relate to a fictitious multinational organization calif led Dover Leasing Corporation, a property management company with a head office based in Boston. For the purpose of the activities and case projects, you have been hired by Dover Leasing Corporation as a junior network administrator responsible for looking after the day-to-day administration of an Active Directory domain within their Windows Server 2003 network. The scenarios presented are designed to help you relate the concepts that you learn to tasks typically performed by a system administrator in a corporate Windows Server 2003 environment.

WINDOWS SERVER 2003 EDITIONS

Businesses today have a wide variety of needs, making it difficult for a single operating system to include all required features. The Windows Server 2003 product line is divided into four distinct operating system editions. Each edition has similar core capabilities but is differentiated from the others by features (and limitations) that make it suitable for different server environments. This allows businesses to choose the platform that best meets their needs in terms of features, performance, and price.

The Windows Server 2003 operating system comes in the following editions, each of which are discussed in the following sections:

- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Windows Server 2003, Web Edition

Windows Server 2003, Standard Edition

Windows Server 2003, Standard Edition, is designed to meet the everyday needs of small to large businesses. It provides file and print services, secure Internet connectivity, and centralized management of network resources. Windows Server 2003, Standard Edition, provides the logical upgrade path for companies currently running its predecessor, Windows 2000 Server.

This edition of Windows Server 2003 provides basic operating system elements that enable file and printer sharing over a network, along with secure management of resources using NTFS permissions. It supports up to four processors in a symmetric multiprocessor (SMP) system, and up to 4 GB of RAM. Table 1-1 provides an overview of the system requirements and basic feature support for Windows Server 2003, Standard Edition.

Table 1-1 Windows Server 2003, Standard Edition, system requirements and feature support

Specification/Feature	Value
Minimum CPU speed	133 MHz
Recommended minimum CPU speed	550 MHz
Minimum RAM	128 MB
Recommended minimum RAM	256 MB
Maximum RAM supported	4 GB
Multiprocessor support	Up to 4 CPUs
Operating system disk space requirements	1.5 GB Free space
Clustering support	None
Itanium support	None
Active Directory support	Domain controller, Member server
Supported upgrades	Windows NT 4.0 Server (SP5), Windows NT 4.0 Terminal Server Edition (SP5), Windows 2000 Server

Itanium is the name of Intel's line of 64-bit processors aimed at higher-end application, security, and transaction processing servers. Only the Enterprise and Datacenter editions of Windows Server 2003 support these CPUs. For more information on the Itanium processor lines see *http://www.intel.com/itanium.*

Windows Server 2003, Standard Edition is designed to support the everyday business needs of small to medium organizations, or to function as a departmental server in larger environments. Key considerations for companies choosing this edition are the fact that it does not support the Itanium platform or clustering, and that it can only scale to a maximum of four processors and 4 GB of RAM.

Windows Server 2003, Enterprise Edition

Windows Server 2003, Enterprise Edition, is designed to meet the needs of organizations that support higher-end applications that demand better performance, reliability, and availability. Windows Server 2003, Enterprise Edition, supports up to eight processors in an SMP system and is available for both 32-bit x86 and 64-bit Itanium processors. In addition to these features, this platform has the following advantages:

- Supports up to 32 GB of RAM for x86 systems and up to 64 GB for Itanium systems.
- Provides **clustering** capabilities for up to eight nodes. Clustering is the ability to increase access to server resources and provide fail-safe services by linking two or more computer systems so they appear to function as though they are one.
- Supports hot-add memory in which RAM can be added to a system without shutting down the server.
- Provides Non-Uniform Memory Access (NUMA) support for SMP computers, allowing a processor to access memory designated for other processors. Applications can be written so that they take advantage of NUMA capabilities, including faster memory access.
- Supports Microsoft Metadirectory Services to facilitate networks that use multiple directory services to track and manage access to such resources as user accounts, shared folders, and shared printers.
- Provides Windows System Resource Manager (WSRM) to allow administrators to allocate and dedicate CPU and memory resources on a per-application basis.

Table 1-2 provides an overview of the system requirements and basic feature support for Windows Server 2003, Enterprise Edition.

Table 1-2 Windows Server 2003, Enterprise Edition, system requirements and feature support

Specification/Feature	Value
Minimum CPU speed	133 MHz (x86), 733 MHz (Itanium)
Recommended minimum CPU speed	733 MHz
Minimum RAM	128 MB
Recommended minimum RAM	256 MB
Maximum RAM supported	32 GB (x86), 64 GB (Itanium)
Multiprocessor support	Up to 8 CPUs
Operating system disk space requirements	1.5 GB (x86), 2.0 GB (Itanium)
Clustering support	Up to 8 nodes

Specification/Feature	Value
Itanium support	Yes
Active Directory support	Domain controller, Member server
Supported upgrades (x86 only)	Windows NT 4.0 Server (SP5), Windows NT 4.0 Terminal Server Edition (SP5), Windows NT 4.0 Enterprise Edition (SP5), Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003 Standard Edition

Windows Server 2003, Enterprise Edition, is designed to support the higher-end business needs of medium to large organizations that require support for mission-critical applications. Key considerations for companies choosing this edition are the fact that it does support the Itanium platform and 8-way clustering, can scale to a maximum of eight processors, and supports more RAM than Standard Edition.

Windows Server 2003, Datacenter Edition

Windows Server 2003, Datacenter Edition, is designed for environments with mission-critical applications, very large databases, and information access requiring the highest possible degree of availability. This platform offers support for between eight and 32 processors in an x86 SMP system (64 processors maximum on Itanium systems), along with 8-way clustering. The maximum RAM capabilities for Datacenter Edition are the most robust at 64 GB for x86 systems and 512 GB for Itanium models. Table 1-3 provides an overview of the system requirements and basic feature support for Windows Server 2003, Datacenter Edition.

Table 1-3 Windows Server 2003, Datacenter Edition, system requirements and feature support

Specification/Feature	Value
Minimum CPU speed	400 MHz (x86), 733 MHz (Itanium)
Recommended minimum CPU speed	733 MHz
Minimum RAM	512 MB
Recommended minimum RAM	1 GB
Maximum RAM supported	64 GB (x86), 512 GB (Itanium)
Multiprocessor support	Minimum 8 CPUs required, Maximum 32 CPUs supported (x86), Maximum 64 CPUs supported (Itanium)
Operating system disk space requirements	1.5 GB (x86), 2.0 GB (Itanium)
Clustering support	Up to 8 nodes
Itanium support	Yes
Active Directory support	Domain controller, Member server
Supported upgrades (x86 only)	Windows 2000 Datacenter Server

Windows Server 2003, Datacenter Edition, is the most industrial-strength platform designed for large mission-critical database and transaction processing systems. Unlike the other Windows Server 2003 editions, the Datacenter edition can only be obtained from original equipment manufacturers (OEMs).

Windows Server 2003, Web Edition

Windows Server 2003, Web Edition, is designed for hosting and deploying Web services and related applications. This platform supports up to two processors (x86 only) and a maximum of 2 GB of RAM. It is specifically optimized to run Microsoft Internet Information Services (IIS) 6.0, and provides companies that only need to deploy Web-related services with a more cost-effective solution than the other Windows Server 2003 editions. Table 1-4 provides an overview of the system requirements and basic feature support for Windows Server 2003, Web Edition.

Table 1-4 Windows Server 2003, Web Edition, system requirements and feature support

Specification/Feature	Value
Minimum CPU speed	133 MHz
Recommended minimum CPU speed	550 MHz
Minimum RAM	128 MB
Recommended minimum RAM	256 MB
Maximum RAM supported	2 GB
Multiprocessor support	Up to 2 CPUs
Operating system disk space requirements	1.5 GB
Clustering support	None
Itanium support	None
Active Directory support	Member server only
Supported upgrades	None

Small to large companies, or departments within an organization that develop and deploy Web sites are examples of the intended audience for this platform. One limitation of Windows Server 2003, Web Edition, is that it cannot be configured as a domain controller, a function that is available on all other Windows Server 2003 platforms. You'll learn more about Active Directory later in this chapter.

For a complete high-level overview of the features included in the different editions of Windows Server 2003 visit *www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx*.

Activity 1-1: Determining the Windows Server 2003 Edition Installed on a Server

Time Required: 5 minutes

Objective: Determine the edition of Windows Server 2003 installed on your server.

Description: The edition of Windows Server 2003 that is installed on a server can be determined in a number of different ways ranging from the operating system selection screen during the boot process to the graphic displayed as part of the logon dialog box. In this exercise you will use the System Properties windows to determine the edition of Windows Server 2003 installed on your server.

1. At the Welcome to Windows dialog box, press **Ctrl+Alt+Delete**.
2. At the Log On to Windows dialog box, type **Admin*XX*** in the User name text box, where *XX* is your assigned student number. In the Password text box, type **Password01**.
3. Click the **Options** button. Ensure that Domain*XX* is selected in the Log on to drop down box, where *XX* is your assigned student number. Click **OK**.
4. At the Manage Your Server window, check the **Don't display this page at logon** check box, and then close the window.
5. Click **Start**, right-click **My Computer**, and click **Properties**. Notice that the Windows Server 2003 edition installed on your server appears in the System section of the General tab, as shown in Figure 1-1.

6. Click **Cancel** to close the System Properties window.

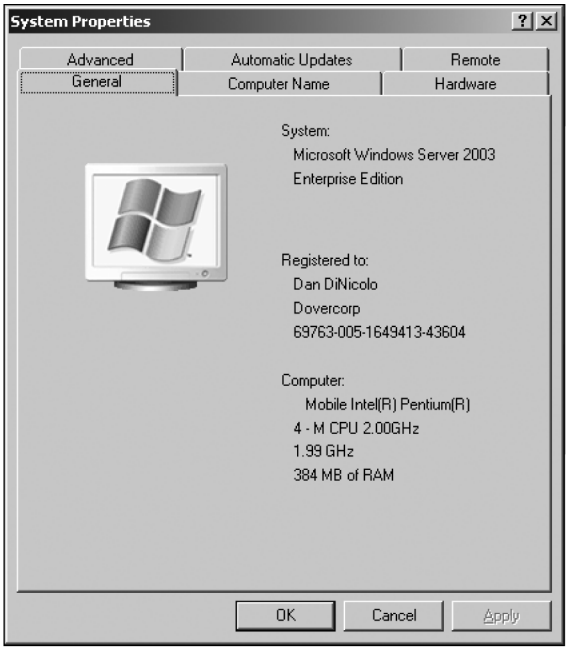

Figure 1-1 Using the General tab of the System Properties window to determine the Windows Server 2003 edition

Windows Networking Concepts Overview

As part of managing a Windows Server 2003 network environment, a network administrator needs to be familiar with both of the different security models that can be implemented as well as the roles that a server can hold. The two different security models used in Windows network environments are the workgroup model and the domain model. While almost all larger organizations use the domain model (and by extension, Active Directory), the workgroup model is often implemented in smaller environments. As part of understanding a Windows network, you should be familiar with both models, including the benefits and limitations of each.

When a Windows Server 2003 system is deployed, it can participate on the network in one of three major roles. These roles include being configured as a standalone server, member server, and domain controller. The decision as to which role a server should be configured in is a function of the network model in use (workgroup or domain), as well as the types of tasks that the server will be handling. In the following sections you'll learn more about both of the Windows networking models, as well as each Windows Server 2003 server role.

Workgroups

A Windows **workgroup** is a logical group of computers characterized by a decentralized security and administration model. Instead of implementing a server to facilitate functions like centralized authentication, systems in a workgroup rely upon a local account database known as the **Security Accounts Manager (SAM) database**. When a user logs on to their workstation in the workgroup, they are authenticated by the local SAM database on that system. One of the benefits of the workgroup model is that it is simple and does not explicitly require a server at all—users can share resources directly from their desktop systems as necessary.

While this model may initially sound appealing, it does present many limitations. First, a user needs a unique user account to be configured on each and every workstation that they will log on to, rather than a single, centralized account. This may not be difficult in a small environment with only three workstations, but would be very difficult to manage on a larger network. Second, individual users effectively manage their own systems in the workgroup model, which can lead to potential security issues. Finally, the workgroup model is not scalable to very large sizes—as such, it is only recommended for smaller networks. As a general rule, workgroups should only be used in networks with 10 or less client systems, although workgroups up to 20 systems are not uncommon.

Although the workgroup model does not explicitly require a server, a Windows Server 2003 system can still be made part of a workgroup. In the workgroup model, a server would be used for traditional purposes such as providing a centralized location for the storage of user data files or acting as an e-mail server. A Windows Server 2003 system configured as part of a workgroup does not, however, authenticate users in a centralized manner, and configuring security settings (such as file and folder permissions) is more difficult due to the lack of a single user database. When a Windows Server 2003 system is configured as a member of a workgroup, it is properly referred to as a standalone server.

Figure 1-2 illustrates the Computer Name tab of the System Properties window for a server configured as part of a workgroup. Most organizations use the default workgroup name "Workgroup," but any valid NetBIOS name can be chosen to identify the logical group.

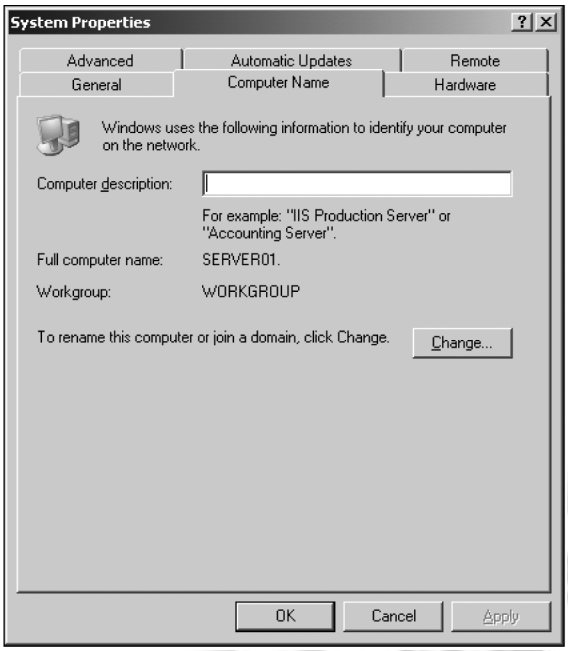

Figure 1-2 A Windows Server 2003 system configured as part of a workgroup named Workgroup

Domains

In contrast to a workgroup, a **domain** is a logical group of computers characterized by centralized authentication and administration. In the domain model, user, group, and computer accounts are stored in a centralized directory database—Active Directory, in the case of Windows Server 2003. While the directory conceptually centralizes both authentication and administration, the database itself is stored on one or more computers configured in a role known as a domain controller. In a Windows Server 2003 environment, a domain controller can be a server running Windows Server 2003, Windows 2000, or even Windows NT 4.0. In order to function as a domain controller, a server must explicitly be configured to hold this role.

The versions of Windows supported as domain controllers in a Windows Server 2003 Active Directory environment depends upon the configured functional level of both the domain and the forest. For more information on domain and forest functional levels see the Windows Server 2003 Help and Support Center.

When a user attempts to log on in a domain environment, they are authenticated by a domain controller rather than by the local SAM database of the workstation under normal circumstances. The authentication request is passed from their workstation to a domain controller where the supplied user name and password are compared to information stored in the directory database. The obvious benefit of this model is that a user requires only a

single account to be created to gain access to the network, rather than an account in the SAM database of many different workstations. By extension, this model also facilitates easier administration of the network since users and their properties can be managed centrally.

The domain model is highly recommended in any environment that consists of more than 10 users or workstations. One drawback of this model is that it requires at least one server to be configured as a domain controller, which means additional expense. Optimally, a domain environment will consist of a minimum of two domain controllers for the purpose of fault tolerance and load balancing. In this case, the second domain controller provides fault tolerance by ensuring that a domain controller is available to service requests should the other fail. Load balancing is achieved by having both domain controllers (rather than just one) handle requests, which results in better performance. Later in this chapter you'll learn more about Windows Server 2003 domains, and specifically Active Directory.

Member Servers

A **member server** is a Windows Server 2003 system that has a computer account in a domain, but is not configured as a domain controller. Member servers are typically used for a wide variety of functions including file, print, and application services. Member servers also commonly host network services such as the Domain Name Service (DNS), Routing and Remote Access Service (RRAS), and others. Each of the four Windows Server 2003 editions can be configured in the role of a member server in a domain environment.

Figure 1-3 illustrates the Computer Name tab of the System Properties window for a member server configured as part of a domain named Domain01.Dovercorp.net.

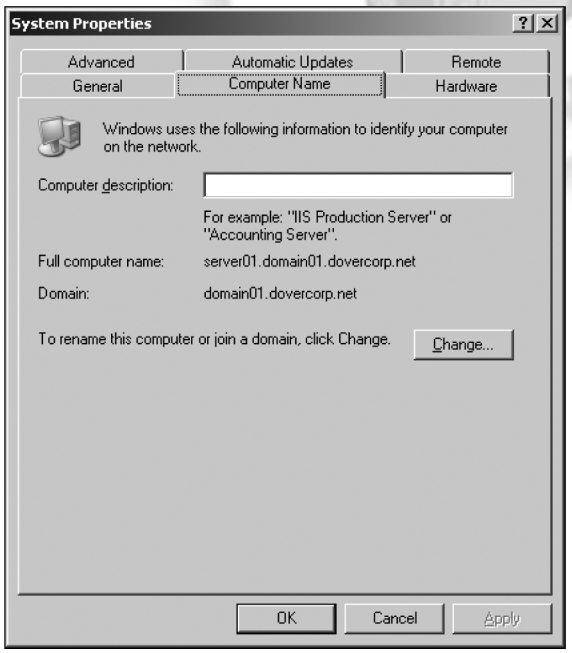

Figure 1-3 A Windows Server 2003 system configured as a member of a domain named Domain01.Dovercorp.net

Domain Controllers

While still a member of a domain, a **domain controller** is a Windows Server 2003 system explicitly configured to store a copy of the Active Directory database, and service user authentication requests or queries about domain objects. While many companies choose to dedicate servers to the role of a domain controller exclusively, other companies will use their domain controllers to also provide file, print, application, and networking services on the network. The main considerations when deciding which additional roles a domain controller should take on are the current utilization of the server, as well as whether sufficient resources (such as memory) are available to handle those roles. Of the four Windows Server 2003 editions, only Windows Server 2003, Web Edition, cannot be configured as a domain controller.

Servers are promoted to the role of a domain controller using either the Active Directory Installation Wizard (DCPROMO.EXE) or the Configure Your Server wizard. The Configure Your Server wizard is illustrated in Figure 1-4.

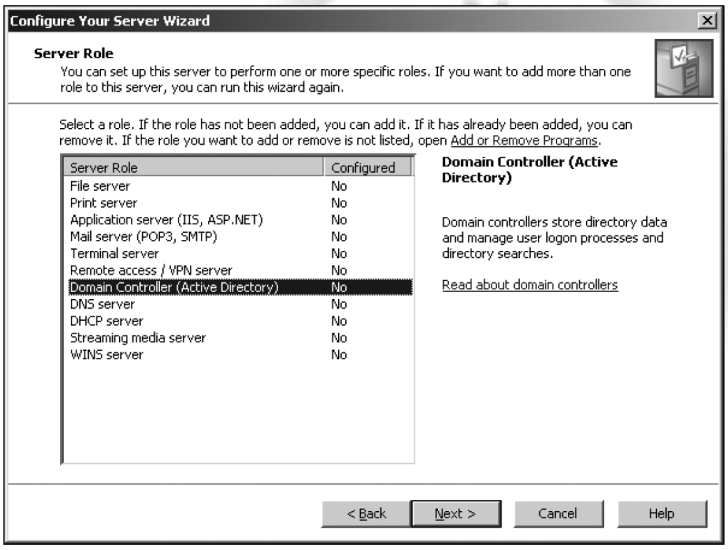

Figure 1-4 The Server Role screen of the Configure Your Server wizard

Activity 1-2: Determining the Domain or Workgroup Membership of a Windows Server 2003 System

Time Required: 5 minutes

Objective: Determine the domain or workgroup membership of a Windows Server 2003 system.

Description: Windows Server 2003 systems can be configured in different roles depending upon the Windows network environment in use and the intended purpose of the server. In this exercise you will use the System Properties window in order to determine the current role of your server as well as domain or workgroup membership settings.

1. Click **Start**, right-click on **My Computer**, and then click **Properties**.
2. Click the **Computer Name** tab. This tab displays both the full computer name of your server along with the domain that it is currently a member of.
3. Click the **Change** button. When the Computer Name Changes dialog box appears, read the message you are presented with and click **OK**. This message appears because your server is currently configured as a domain controller.
4. Notice in the lower portion of the Computer Name Changes window that the Member of section is grayed out and cannot be changed. If your system were not a domain controller, this screen would be used to add the server to a domain or workgroup. Your server is currently configured as a domain controller in domain*XX*.dovercorp.net, where *XX* is your assigned student number.
5. Click **Cancel** to close the Computer Name Changes window.
6. Click **OK** to close the System Properties window.

Computer Accounts

Computers running Windows NT, Windows 2000, Windows XP, or Windows Server 2003 are assigned computer accounts as part of joining a domain. A computer account provides a method to authenticate computers that are members of a domain, as well as audit access to network resources. While systems running Windows 95/98/ME can participate in a domain, these operating systems are not assigned computer accounts.

In an Active Directory environment, computer accounts are represented as computer objects, and can be viewed using administrative tools like Active Directory Users and Computers. In Activity 1-3, you will explore some of the basic properties associated with the computer account for your server. Later in this book you will learn more about the process of creating and managing computer accounts in an Active Directory environment.

Activity 1-3: Viewing and Configuring Computer Account Settings in Active Directory Users and Computers

Time Required: 5 minutes

Objective: Use Active Directory Users and Computers to view and configure computer account settings and properties.

Description: When a Windows Server 2003 system is configured as a member of an Active Directory domain, a computer account is created for the system in the Active Directory database. In this exercise you will use the Active Directory Users and Computers administrative tool to view the location and settings of the computer account associated with your server.

1. Click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Click on the **plus sign (+)** next to the domain*XX*.dovercorp.net (where *XX* is your assigned student number) icon to expand it.

3. Click on the **Domain Controllers** folder to view its contents. This object is an organizational unit in the domain*XX*.dovercorp.net domain.
4. Right-click the **Server*XX*** computer object shown in Figure 1-5, and click **Properties**.
5. Review the information provided on the General tab. Notice that this system currently holds the role of Domain controller. In the Description text box, type **Domain Controller for domain*XX*.dovercorp.net**, where *XX* is your assigned student number.
6. Click the **Operating System** tab. This tab displays information about the operating system installed, along with version number and service pack information. Notice, however, that Windows Server 2003 edition information is not provided. Click **OK**. You will review the remaining tabs found in the properties of a computer account in a later chapter.
7. Close Active Directory Users and Computers.

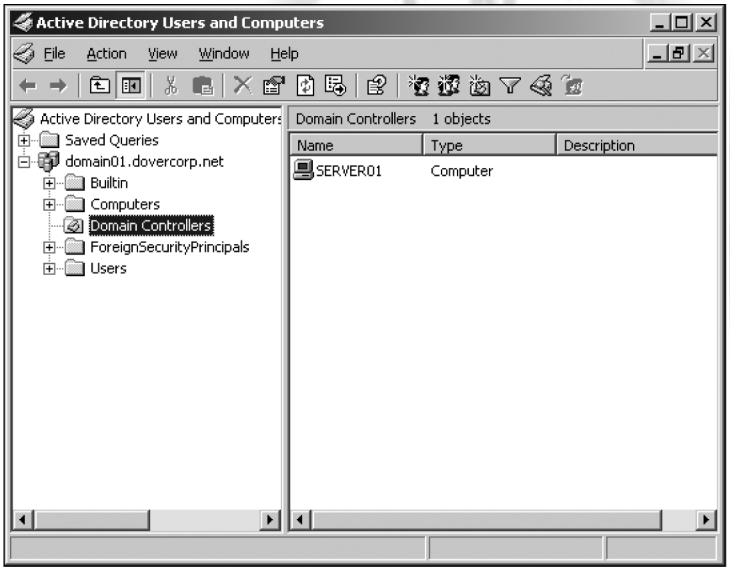

Figure 1-5 Using Active Directory Users and Computers to view a computer object

Network Management and Maintenance Overview

Although managing and maintaining a Windows Server 2003 network environment requires an administrator to be familiar with a variety of different tools, concepts, and troubleshooting procedures, most of these tasks can be broadly categorized into one of the following five major focus areas:

- Managing and maintaining physical and logical devices

- Managing users, computers, and groups
- Managing and maintaining access to resources
- Managing and maintaining a server environment
- Managing and implementing disaster recovery

The following sections outline the key tasks associated with each of these five focus areas, which make up the core concepts that a network administrator needs to be familiar with for Microsoft exam 70-290, Managing and Maintaining a Microsoft Windows Server 2003 Environment. Outside of providing a broad overview of each focus area and related tasks, each section also provides details of where these topics are covered within this book.

Managing and Maintaining Physical and Logical Devices

A large part of managing and maintaining any network environment involves ensuring that network hardware is configured and functioning correctly. In a typical environment, a network administrator will be responsible for installing and configuring server hardware devices, managing server disks, and generally ensuring that devices are performing optimally. Key tools that are used to manage server hardware and related settings include various Control Panel applets, Device Manager, and the Computer Management MMC.

A network administrator would typically be responsible for installing new server hardware, such as an additional network adapter card or perhaps a modem. Apart from the physical act of inserting the card in an expansion slot, the administrator needs to be sure that resource settings are configured correctly, the correct driver is installed, and that the installed driver is certified for Windows Server 2003.

As part of managing server disks, an administrator will need to be familiar with the different types of disks available in Windows Server 2003, and how to configure these disks with different logical volumes or partitions. Once partitions or volumes have been created, an administrator will need to manage them to ensure optimal performance using utilities like Disk Defragmenter. In cases where disk redundancy is required, an administrator will need to be familiar with the various fault tolerance techniques available in Windows Server 2003, such as **Redundant Array of Independent Disks (RAID)**.

Although a proactive approach to network management and maintenance will help to ensure that server hardware problems are minimized, there will still be times when problems occur without warning. In these situations, it is imperative that a network administrator be able to identify the problem using the various tools provided in Windows Server 2003 in order to minimize the potential impact to network users.

Managing and maintaining hardware devices and related settings is detailed in Chapter 2. Managing disks and data storage is covered in Chapter 6.

Managing Users, Computers, and Groups

One of the most common day-to-day tasks encountered by a Windows Server 2003 network administrator is the administration of user accounts. New user accounts need to be created, existing settings may need to be changed, and users will invariably forget their passwords from time to time. In large environments, the management and maintenance of user accounts can consume a great deal of time and energy for any administrator.

To help alleviate some of this burden, Windows Server 2003 Active Directory includes a variety of new tools and features that allow an administrator to automate and simplify many account-related tasks. For example, the primary user administration tool, Active Directory Users and Computers, now supports drag-and-drop functionality to make moving objects easier. Similarly, a number of new command-line utilities are available to help automate the process of adding, changing, and deleting user accounts. These powerful utilities give an administrator more flexibility in effectively managing their user environment. In a similar manner, these same tools can be used to manage the computer accounts required for Windows NT, Windows 2000, Windows XP, and Windows Server 2003 systems that will be part of a domain.

Windows Server 2003 supports a number of different group types and scopes. Groups can be created for the purpose of assigning network rights and permissions to multiple users, as well as to create distribution lists for e-mail. An administrator needs to be familiar with the different group types and scopes available in Windows Server 2003, and, subsequently, how and when each should be used. Group accounts, like user accounts, can also be managed using a variety of new command-line utilities included with Windows Server 2003.

Outside of the creation and management of users, computers, and groups, a network administrator also needs to manage the user desktop environment. In Windows Server 2003, the desktop environment is managed using user profiles. Depending upon the environment and needs of an organization, user profiles may be configured to save settings locally, enforce a standard profile for all users, or follow users to any system that they happen to log on to.

Once network objects are created and settings are configured, an administrator is still responsible for troubleshooting related problems as they arise. In some cases solving these problems may be simple, such as resetting a user's forgotten password. In others, a variety of issues may impact the user's ability to authenticate and access network resources. An administrator must be familiar with the authentication process and the different policy settings that can impact user access to the network.

Managing and maintaining user accounts, computer accounts, profile settings, and troubleshooting authentication issues are looked at in more detail in Chapter 3. The creation and management of group accounts is covered in Chapter 4.

One of the most common tasks for a network administrator involves resetting forgotten user passwords. In Activity 1-4 you will use Active Directory Users and Computers to reset the password associated with your Admin*XX* user account.

Activity 1-4: Resetting a Domain User Account Password Using Active Directory Users and Computers

Time Required: 10 minutes

Objective: Use Active Directory Users and Computers to reset a user password and force the user to change their password the next time they log on.

Description: One of the common tasks of a network administrator is to reset forgotten user passwords. While an administrator can explicitly control the passwords that users will need to provide during the logon process, this is not a common configuration. Instead, when a user forgets their password, an administrator will typically reset the account password to a temporary value, supply this password to the user, and then force them to change it to a new value during the logon process. In this exercise you will use Active Directory Users and Computers to reset the password associated with your Admin*XX* account, and then create a new personal password during the logon process.

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Click the **Users** folder to view its contents. The Users folder is a built-in container in Windows Server 2003 Active Directory environments.
3. Right-click the **Admin*XX*** user object, where *XX* is your assigned student number. From the shortcut menu, click **Reset Password**.
4. In the Reset Password dialog box displayed in Figure 1-6, type **Password02** in the New password text box and **Password02** in the Confirm password text box.
5. Check the **User must change password at next logon** check box. This will force you to change your password immediately the next time you log on. Click **OK**.
6. When the Active Directory dialog box appears, click **OK**.
7. Close Active Directory Users and Computers.
8. Click **Start**, and then click **Log Off**. In the Log Off Windows dialog box, click the **Log Off** button.
9. Log on using your **Admin*XX*** account and the password **Password02**. At the Logon Message dialog box, click **OK**.
10. In the Change Password dialog box, type a new password in the New Password textbox and then re-type the new password in the Confirm New Password check box. Click **OK**. If the password you chose does not meet the complexity requirements read the dialog box that appears, click **OK**, and then enter a sufficiently complex password.

11. At the Change Password dialog box, click **OK**.

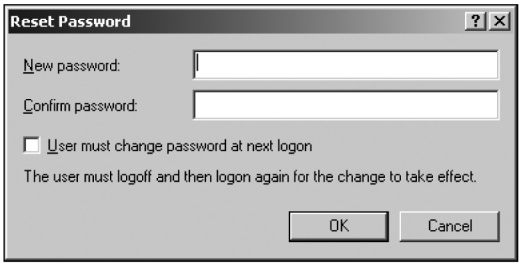

Figure 1-6 The Reset Password dialog box in Active Directory Users and Computers

Managing and Maintaining Access to Resources

The primary reason for implementing a network is to allow users to share resources. Examples of common network resources that users need access to include files saved on network servers and shared network printers. An administrator not only needs to ensure that resources are accessible to users, but also that they are properly secured.

In Windows Server 2003, resources are made available to network users via a technique known as sharing. When a folder or printer is shared over the network it becomes possible for users to connect to and remotely access the resource. The two most common methods of sharing resources are using the Windows Explorer interface and the Computer Management administrative tool. Other methods are also possible including using the command line.

Although sharing resources is the primary reason for implementing a network, it is imperative that resources are properly secured. While it might be fine for all users to access certain network folders or printers, others will need to be restricted to certain users or groups. Windows Server 2003 provides two main methods of securing resources, shared folder permissions and NTFS permissions. Shared folder permissions are only applicable when a user tries to access a resource over a network, while NTFS permissions apply both locally and remotely.

An administrator needs to understand the difference between each type of permission and the effects of combining them in order to properly plan permissions. If these concepts are not correctly understood and accounted for, the security of the network is put at risk, and unauthorized users may be able to access resources they shouldn't be able to.

Windows Server 2003 also includes a service known as **Terminal Services**. Terminal Services allows a user to connect to a central server and access applications as though working from the user desktop. This is a popular method of granting users access to certain applications without the need to deploy those applications to all desktops. Along the same lines, Terminal Services can also be used to give users running different operating systems (such as Windows 98 or Windows NT) the ability to use applications that were designed

for Windows Server 2003. Once the decision to use Terminal Services has been made, a network administrator not only needs to ensure that a client can access the environment, but also that the environment is properly secured.

Managing the access to files and configuring security permissions is looked at in more detail in Chapter 5. Terminal Services and related settings are covered in Chapter 10.

Managing and Maintaining a Server Environment

A wide variety of tasks are involved in the general management and maintenance of a Windows Server 2003 server environment. Tasks included in this focus area range from managing server licensing to deploying software updates to managing Web servers. As part of the day-to-day operations of a network, a network administrator needs to be familiar with a wide variety of software tools and concepts aimed not only at management, but also the monitoring of resources.

Two of the most popular tools used to monitor and troubleshoot a server environment are Event Viewer and System Monitor. Event Viewer handles the primary event logging functions on a Windows Server 2003 system, creating entries when any event of significance occurs. When an error occurs, Event Viewer should be the main tool accessed by a network administrator to gather more information. In cases where the overall performance of a server is in question, the System Monitor tool allows an administrator to gather current performance information that can be compared against the baseline of normal performance. Both tools are key utilities in helping an administrator to identify problem areas or performance issues.

Timely application of software patches and security updates is another key maintenance task for the network administrator. Microsoft typically releases patches for known exploits or issues shortly after they are identified, and then later includes these updates in a Service Pack release. Because managing individual updates for hundreds of computers is time-consuming and difficult, Microsoft has released a tool known as **Software Update Services (SUS)** for managing updates in a centralized manner. Administrators of Windows Server 2003 networks should be familiar with this tool and the capabilities that it provides.

Managing printing is yet another key component of a Windows Server 2003 network. Outside of physically connecting and then sharing printers, an administrator needs to ensure that printers are properly secured, and troubleshoot print queue issues as they arise.

While users should be encouraged to save their data files to a network server, an administrator also needs to prevent misuse of this space. For example, users may begin using their server storage space for non-critical files, such as MP3s. Ultimately such misuse of corporate resources leads to higher costs since additional disk space must consequently be acquired. In order to help control these types of issues, an administrator should be familiar with the disk quota feature of Windows Server 2003, which allows an administrator to control the amount of disk space allocated and available to each user.

Windows Server 2003 also includes Web server software in the form of Internet Information Services (IIS) 6.0. Although not installed by default, a Windows Server 2003 network administrator should be familiar with installing the service, and then subsequently ensuring that it is properly secured.

In order to simplify the administration of Windows Server 2003 servers, a variety of remote administration tools are included. One of these tools, the **Microsoft Management Console (MMC)**, provides an administration framework that allows different tools (known as snap-ins) to be added in custom configurations for different management and maintenance tasks. Almost all MMC snap-ins can be focused locally or remotely, allowing an administrator to manage settings on both local and remote servers from a central location. Another very useful remote management tool included with Windows Server 2003 is Remote Desktop, which allows an administrator to remotely connect to a server and manage it as though sitting in front of it. Both tools are key components of any Windows Server 2003 remote administration strategy.

Advanced file system management concepts, including the configuration of disk quotas, are looked at in Chapter 7. Implementing and managing printing are detailed in Chapter 8. Software Update Services (SUS) and the remote administration of servers are covered in Chapter 10. Monitoring and managing server performance using tools like Event Viewer and System Monitor is looked at in more detail in Chapter 11. The administration and configuration of Web resources is covered in Chapter 13.

In Activity 1-5 you will create a custom Microsoft Management Console.

Activity 1-5: Creating a Custom Microsoft Management Console

Time Required: 10 minutes

Objective: Create a custom MMC.

Description: The MMC is the common environment in which all of the Windows Server 2003 administrative tools run. Although these tools are individually available from the Administrative Tools section of the Start menu, administrative tasks can be simplified by grouping commonly used tools into a single customized MMC. The IT manager at Dover Leasing has asked you to create and save a custom MMC to access both Event Viewer and Device Manager. In this activity, you will create a custom MMC and save it to your desktop for more convenient access.

1. Click **Start**, click **Run**, and then type **mmc** in the Open text box. Click **OK**. Figure 1-7 shows an empty MMC window.

2. Click the **File** menu, and click **Add/Remove Snap-in**. Figure 1-8 shows an open Add/Remove Snap-in dialog box.

Figure 1-7 An empty MMC

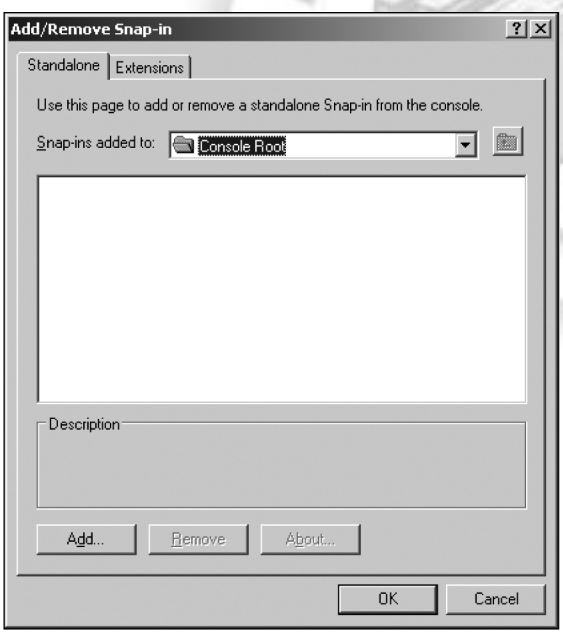

Figure 1-8 The Add/Remove Snap-in dialog box

3. Click the **Add** button to open the Add Standalone Snap-in dialog box listing the available snap-ins, as shown in Figure 1-9.

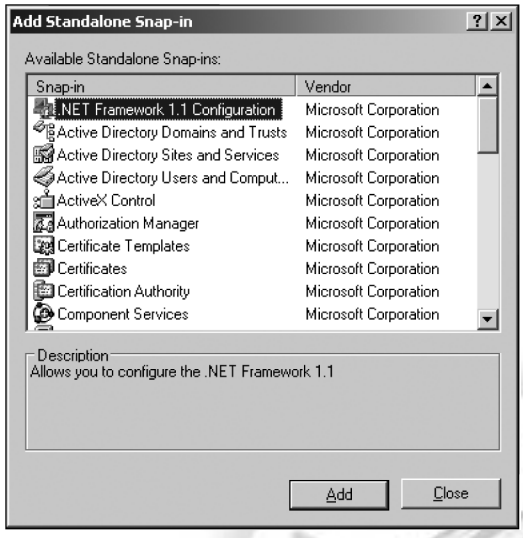

Figure 1-9 The Add Standalone Snap-in dialog box

4. From the list of available snap-ins, click **Event Viewer** and click **Add**. When the Select Computer dialog box opens, make sure that the **Local computer** radio button is selected, as shown in Figure 1-10, and click **Finish**.

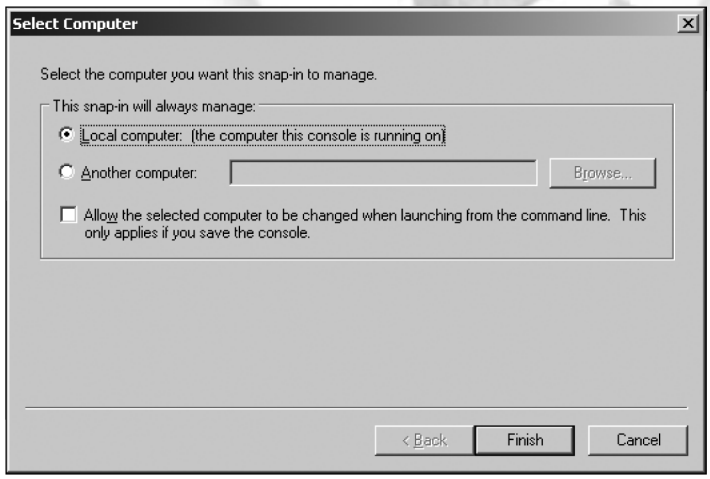

Figure 1-10 Selecting the snap-in focus

5. Click **Device Manager** on the list of available snap-ins and click **Add**. In the Device Manager dialog box, ensure that the **Local computer** radio button is selected and click **Finish**.

6. Click **Close** in the Add Standalone Snap-in dialog box.
7. Click **OK** in the Add/Remove Snap-in dialog box.
8. To save the console, click the **File** menu, and click **Save As**. In the Save in drop-down box, select your desktop, type the file name **My Console** in the File name text box, and click **Save**. Figure 1-11 shows a finished console.
9. Close the My Console window. If prompted to save changes, click **Yes**.
10. Double-click the **My Console** file on your desktop to open the custom console. Notice that it includes both the Event Viewer and Device Manager snap-ins. Close the **MMC**.

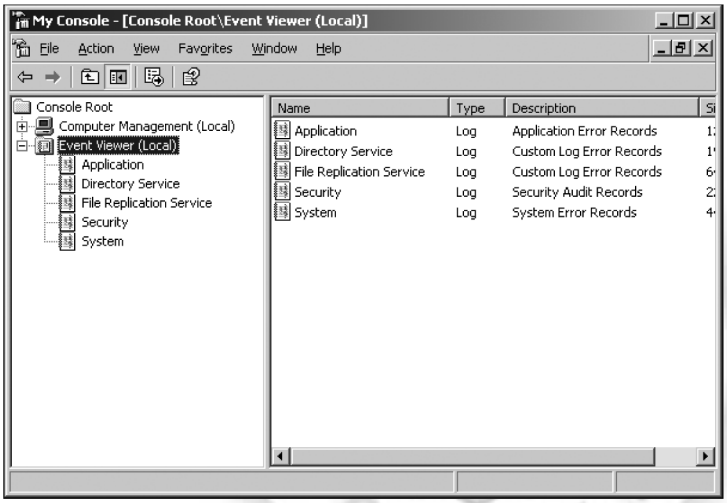

Figure 1-11 A customized MMC

Managing and Implementing Disaster Recovery

The final major focus area for a Windows Server 2003 network administrator is implementing and managing disaster recovery. This focus area concentrates on tasks that ensure both data and system settings are properly backed up and then available in cases like the failure of a server or the accidental deletion of files.

The backup tool provided with Windows Server 2003 is Windows Backup. This tool includes not only a graphical interface where the files to be backed up or restored can be selected, but also a wizard that can be used to simplify the same tasks. A network administrator should be familiar with the different types of backups available using this tool, along with how to schedule backup operations to occur automatically.

The Windows Backup tool can also be used to back up critical system information by selecting the System State option. System State information includes a variety of operating system components, including the Registry and critical system files. An administrator should be familiar with both backing up and restoring System State information using the Windows Backup tool.

Windows Server 2003 also includes a new feature known as Automated System Recovery. This feature, which is accessible from the Windows Backup utility, allows an administrator to create a floppy disk to which critical configuration information will be copied, allowing a server operating system to be restored using a combination of the disk and the Windows Server 2003 installation media. This provides a fast and effective way for an administrator to restore the operating system to a more current configuration rather than reinstalling from scratch.

Finally, another new and important feature in Windows Server 2003 is Shadow Copies of Shared Folders. Shadow Copies of Shared Folders is a feature that maintains previous versions of files on a server in a manner accessible to individual users. In the event that the current copy of a file has been deleted or overwritten, Shadow Copies of Shared Folders allows a user to restore a previous version of the file without having to contact an administrator. Ultimately, this feature can save an administrator a great deal of time and effort traditionally expended restoring individual user files from backup.


NOTE

Concepts relating to implementing and managing disaster recovery are looked at in more detail in Chapter 12.

Introduction to Windows Server 2003 Active Directory

Active Directory is the native directory service included with Windows Server 2003 operating systems. Active Directory provides the following services and features to the network environment:

- A central point for storing, organizing, managing, and controlling network objects, such as users, computers, and groups
- A single point of administration of objects, such as users, groups, computers, and Active Directory-published resources, such as printers or shared folders
- Logon and authentication services for users
- Delegation of administration to allow for decentralized administration of Active Directory objects, such as users and groups

The Active Directory database is stored on any Windows Server 2003 server that has been promoted to the role of domain controller. Each domain controller on the network has a writeable copy of the directory database. This means that you can make Active Directory changes to any domain controller within your network, and those changes are replicated

to all of the other domain controllers. This process is called **multimaster replication**, and provides a form of fault-tolerance. If a single server fails, Active Directory does not fail because replicated copies of the database are available from other servers within the network.

Active Directory uses the **Domain Name Service (DNS)** to maintain domain-naming structures and locate network resources. What this means to a network designer is that all Active Directory names must follow standard DNS naming conventions. An example of a standard DNS naming convention would be *Dovercorp.net*. A child domain of *Dovercorp.net* would add its name as a prefix, such as *Europe.Dovercorp.net*.

Active Directory Objects

Active Directory stores a variety of objects within the directory database. An **object** represents network resources such as users, groups, computers, and printers. When an object is created in Active Directory, various attributes are assigned to it to provide information about the object. For example, Figure 1-12 illustrates creating a new user object and the ability to add various attributes, such as First name, Last name, and User logon name.

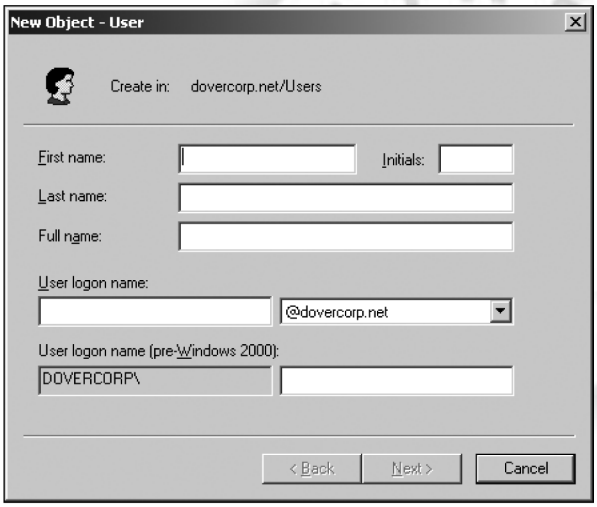

Figure 1-12 Creating a new user object

If you need to locate information about an object from Active Directory, you can perform a search of specific attributes relating to the object. For example, Figure 1-13 shows how you can find the e-mail address of a user object by searching for the specific user name in Active Directory and then viewing the attributes for the object.

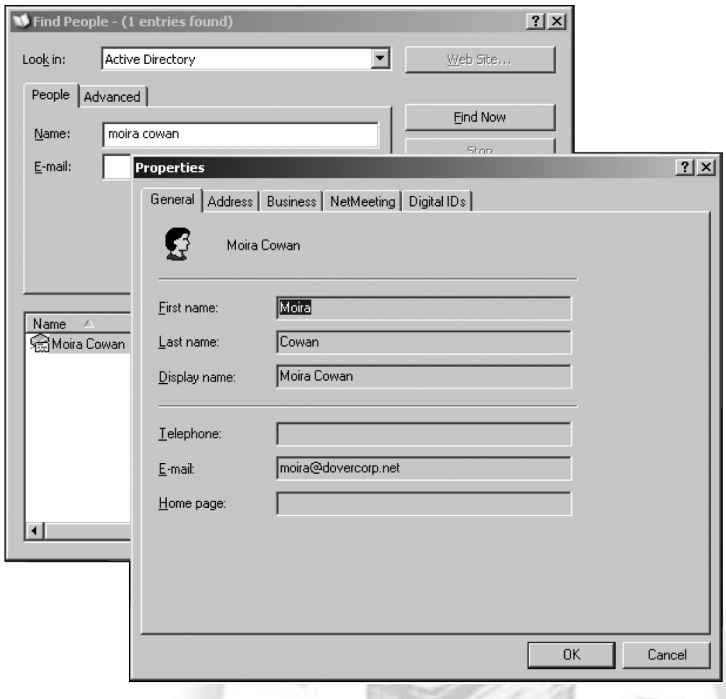

Figure 1-13 Viewing the e-mail address for a user object

Active Directory Schema

All of the objects and attributes that are available in Active Directory are defined in the **Active Directory schema**. In Windows Server 2003, the schema defines the objects for the entire Active Directory structure. This means that there is only one schema for a given Active Directory implementation, and it is replicated among all domain controllers within the network.

The Active Directory schema consists of two main definitions: **object classes** and **attributes**. Object classes define the types of objects that can be created within Active Directory, such as user objects and printer objects. All object classes consist of various attributes that describe the object itself. For example, the user and printer object classes may both have an attribute called description, which is used to describe the use of the object. Attributes are created and stored separately in the schema and can be used with multiple object classes to maintain consistency.

The Active Directory database stores and replicates the schema partition to all domain controllers in an Active Directory environment. Storing the schema within the Active Directory database provides the ability to dynamically update and extend the schema, as well as instant access to information for user applications that need to read the schema properties.

Active Directory Logical Structure and Components

Active Directory is made of several components that provide a way to design and administer the hierarchical, logical structure of the network. The logical components that make up an Active Directory structure include:

- Domains and organizational units
- Trees and forests
- A global catalog

To ensure efficient maintenance and troubleshooting within Active Directory, it is essential that you understand these logical components. The next sections discuss each component in greater detail.

Domains and Organizational Units

A Windows Server 2003 domain is a logically structured organization of objects, such as users, computers, groups, and printers that are part of a network and share a common directory database. Each domain has a unique name and is organized in levels and administered as a unit with common rules and procedures. Windows Server 2003 domains provide a number of administrative benefits including the ability to configure unique security settings, decentralize administration (if necessary), and control replication traffic. By default, members of the Administrators group are only allowed to manage the objects within their own domain. All domain controllers within a single domain store a copy of the Active Directory database, and domain-specific information is only replicated between the domain controllers of the same domain.

An **organizational unit (OU)** is a logical container used to organize objects within a single domain. Objects such as users, groups, computers, and other OUs can be stored in an OU container. For example, you may want to organize your users based upon the department in which they work. You might create a Sales OU to store all of your sales department users and objects and a Marketing OU to store all of your marketing department users and objects. Not only does this make it easier to locate and manage Active Directory objects, but it also allows you to apply **Group Policy** settings to define more advanced features such as software deployment or desktop restrictions based upon department, job function, or perhaps geographic location. Figure 1-14 illustrates an example of a domain with several OUs.

Another main advantage of using an OU structure is the ability to delegate administrative control over OUs. For example, you may want to give a set of users the right to add or remove new users within the Sales OU. You do not have to provide the group with full administrative rights to accomplish this task because Active Directory allows you to delegate very specific tasks, if necessary.

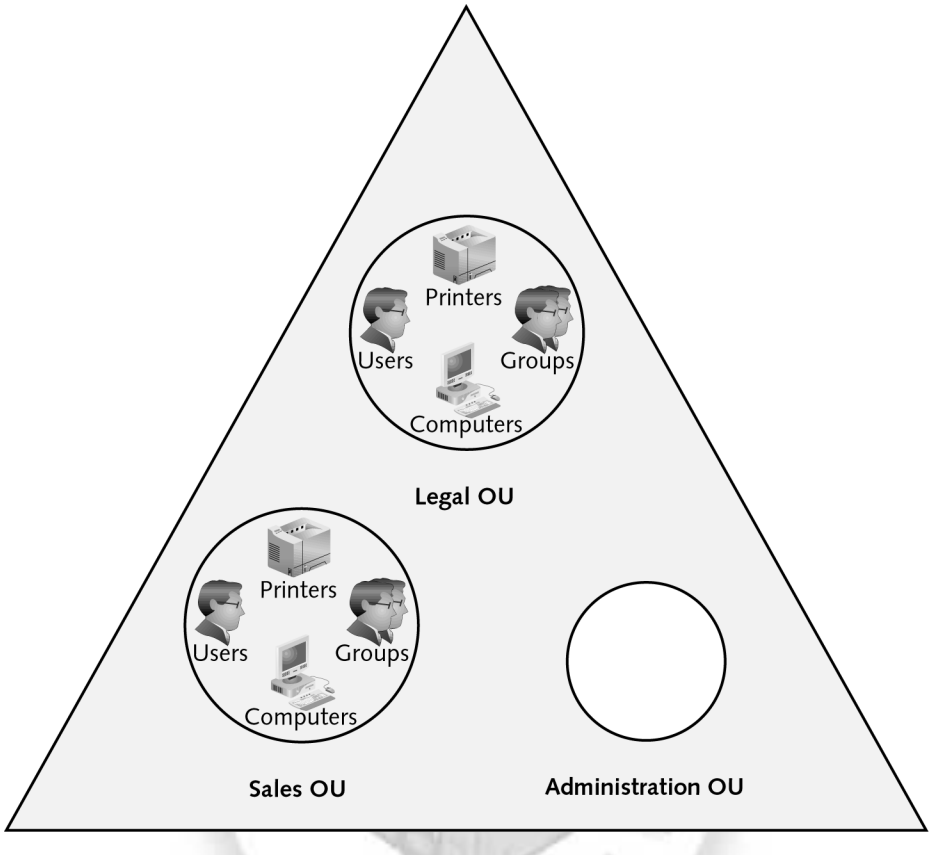

Figure 1-14 An Active Directory domain and OU structure

Trees and Forests

When designing a Windows Server 2003 network infrastructure, there may be times when you are required to create multiple domains within an organization. Reasons for doing this include the following:

- Divisions within the company may be administered on a geographic basis. To make administration easier, a separate domain is created for each division.
- Different password policies are needed between divisions within an organization.
- An extraordinarily large number of objects need to be defined.
- Replication performance needs to be improved.

The first Active Directory domain created in an organization is called the **forest root domain**. When multiple domains are needed, they are connected to the forest root to form either a single **tree** or multiple trees, depending upon the design of the domain name structure. A tree is a hierarchical collection of domains that share a contiguous DNS namespace. For example, Dover Leasing has its head office in Boston with a forest root domain called *Dovercorp.net*. Dover has two divisions, one located in London and the other located in Hong Kong. Because of geographic and administrative differences, you might decide to create a distinct domain for each division. Two child domains can be created off of the forest root domain. The London domain can be named *Europe.Dovercorp.net*, which follows the contiguous DNS namespace design. Similarly, the Hong Kong domain can be called *Asia.Dovercorp.net*. Figure 1-15 illustrates an example of this structure.

Whenever a child domain is created, a two-way, transitive trust relationship is automatically created between the child and parent domains. A **transitive trust** means that all other trusted domains implicitly trust one another. For example, because *Europe.Dovercorp.net* trusts the *Dovercorp.net* forest root domain, Europe also implicitly trusts the *Asia.Dovercorp.net* domain via the *Dovercorp.net* domain. These two-way, transitive trusts allow for resource access anywhere throughout the Active Directory structure. Windows Server 2003 also allows explicit trusts to be created between domains in the same forest, as well as between forests if necessary.

A **forest** is a collection of trees that do not share a contiguous DNS naming structure. For example, Dover Leasing purchases a large international company called Seven Acres Property Management. It may not make sense to make the Seven Acres domain a child of *Dovercorp.net* because of the renaming required to maintain a contiguous naming convention based on *Dovercorp.net*. Instead, you could create a new tree and allow Seven Acres to start its own contiguous naming hierarchy. Both trees make up an Active Directory forest. See Figure 1-16 for an illustration. Although the term "forest" implies a number of trees, an Active Directory forest might consist of only a single domain.

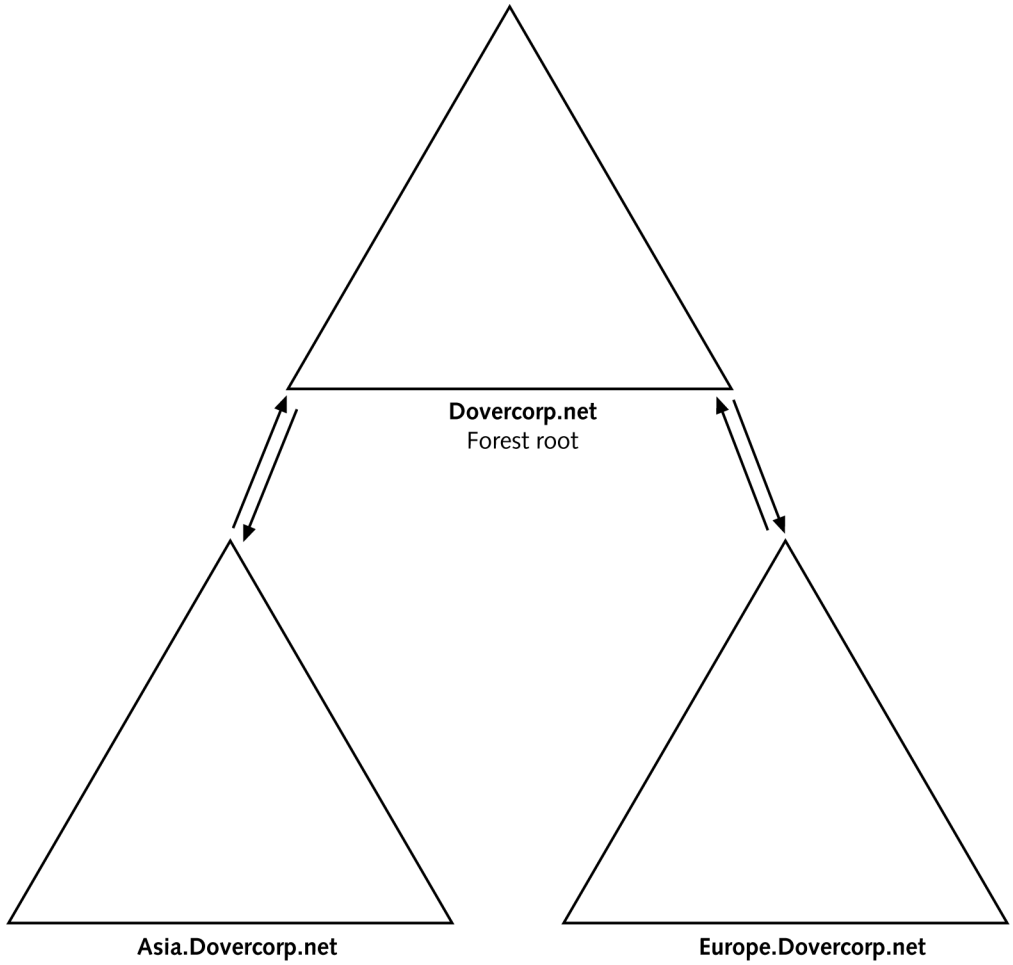

Figure 1-15 The Dovercorp.net domain tree

.

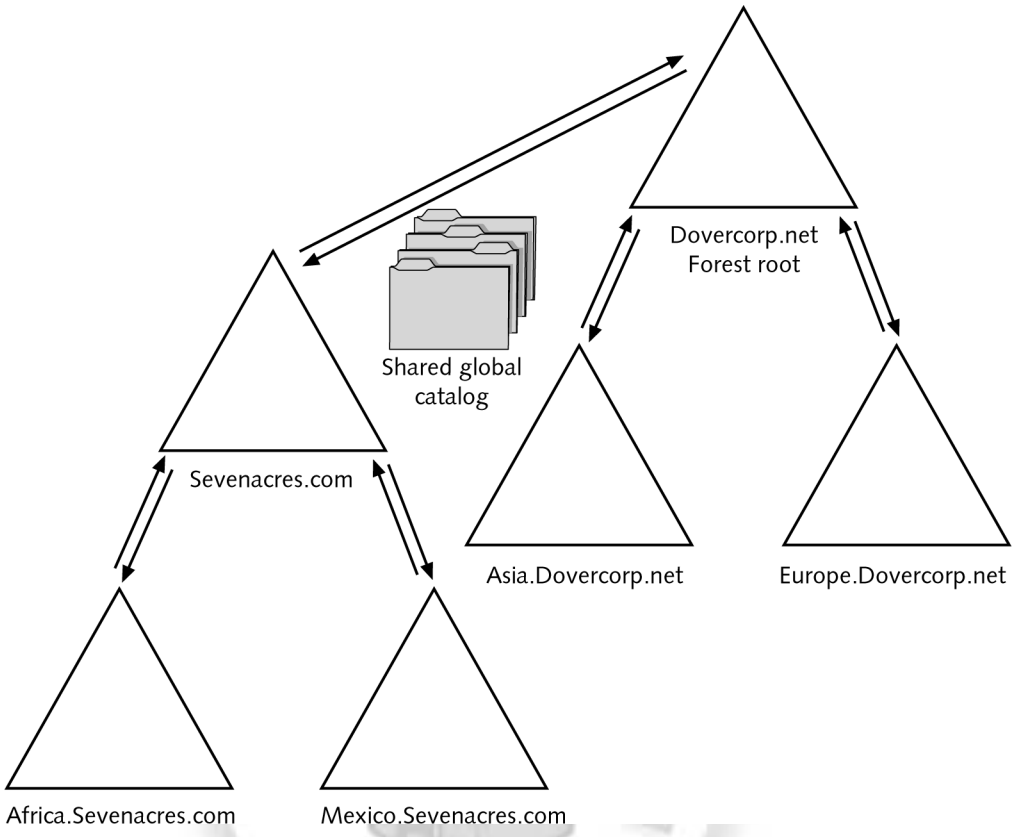

Figure 1-16 Creating an Active Directory forest

Even though the trees within a forest do not share a common namespace, they do share a single Active Directory schema, which ensures that all object classes and attributes are consistent throughout the entire structure. A special group called Enterprise Admins is also created, which allows members to manage objects throughout the entire forest. The Enterprise Admins group is created within the initial forest root domain and has a scope throughout the entire forest. Another component that is shared throughout the forest is a **global catalog**.

Global Catalog

A global catalog is an index and partial replica of the objects and attributes most frequently used throughout the entire Active Directory structure. Some of the common attributes that are stored in a global catalog include a user's first and last names, logon name, and e-mail address. A global catalog is replicated to any server within the forest that is configured to be a global catalog server.

A global catalog is used primarily for four main functions:

- To enable users to find Active Directory information from anywhere in the forest.

- To provide universal group membership information to facilitate logging on to the network. During the logon process in a multiple-domain environment, a global catalog server is contacted to provide universal group membership information.
- To supply authentication services when a user from another domain logs on using a **User Principal Name (UPN)**. (A UPN is a representation of a user's logon credentials in the form user@domain.com. When a UPN is used, a domain name does not need to be explicitly specified in the Log on to drop-down box.)
- To respond to directory lookup requests from Exchange 2000 and other applications. Global catalog servers also host the Exchange 2000 Global Address List (GAL).

The first domain controller in the forest root domain automatically becomes a global catalog server. To provide redundancy, additional domain controllers can easily be configured to also be global catalog servers. Multiple global catalogs can improve user query and logon authentication performance, especially in Active Directory environments that include geographically distant sites connected by wide area network (WAN) links. Microsoft recommends that each Active Directory site be configured with at least one domain controller acting as a global catalog server.

In cases where placing a global catalog in a specific site is not practical (possibly due to slow WAN links between locations], Windows Server 2003 Active Directory provides a new feature known as universal group caching. Universal group caching allows the domain controllers within a particular site to query a global catalog server in another location for a user's universal group membership information, and then cache that information locally for use in subsequent logons.

Active Directory Communications Standards

As mentioned previously, Active Directory uses the DNS naming standard for hostname resolution and for providing information on the location of network services and resources. For example, if you need to locate a server called *database.Dovercorp.net*, your workstation first queries a DNS server to resolve the IP address of the database server. Once the IP address is known, a direct communication session can take place.

The same process occurs when you need to log on to the domain. Your workstation queries DNS to find a domain controller to perform authentication. Once the location of a domain controller is known, then the authentication process can take place, thus allowing a user access to network resources.

When users need to access Active Directory, the **Lightweight Directory Access Protocol (LDAP)** is used to query or update the Active Directory database directly. Just as a DNS name contains a specific naming convention (e.g., *Dovercorp.net*), LDAP also follows a specific naming convention. LDAP naming paths are used when referring to objects stored within the Active Directory. Two main components of the naming paths include:

- *Distinguished name*—Every object in Active Directory has a unique **distinguished name (DN)**. For example, the *Dovercorp.net* domain component (DC) has a user object with a common name (CN) of Moira Cowan that is stored within the

Marketing OU. The distinguished name for the object would be CN=Moira Cowan, OU=Marketing, DC=Dovercorp, DC=Net.

- *Relative distinguished name*—A portion of the distinguished name that uniquely identifies the object within the container is referred to as the **relative distinguished name (RDN)**. For example, the distinguished name OU=Marketing, DC=Dovercorp, DC=Net would have a relative distinguished name of OU=Marketing. For the distinguished name CN=Moira Cowan, OU=Marketing, DC=Dovercorp, DC=Net, the relative distinguished name would be CN=Moira Cowan.

Active Directory Physical Structure

The Active Directory physical structure relates to the actual connectivity of the physical network itself. Because the Active Directory database is stored on multiple servers, you need to make sure that any modification to the database is replicated as quickly as possible between domain controllers. You must also design your topology so that replication does not saturate the available network bandwidth. One replication problem that you may encounter is when domain controllers are separated over a slow WAN connection. In this scenario, you likely want to control the frequency and the time that replication takes place.

In addition to replication, you may also want to control logon traffic. Referring back to the previous scenario, you generally would not want any user authentication requests to have to cross over slow WAN links during the logon process. Optimally, users should authenticate to a domain controller on their side of the WAN connection.

Keep in mind that the physical structure of Active Directory is totally separate from the logical structure. The logical structure is used to organize your network resources, whereas the physical structure is used to control network traffic.

You can control Active Directory replication and authentication traffic by configuring sites and site links. An Active Directory **site** is a combination of one or more Internet Protocol (IP) subnets connected by a high-speed connection. It is assumed that domain controllers that belong to the same site all have a common network connection. It is also assumed that any connection between sites that are not reliable at all times must have replication controlled through replication schedules and frequency intervals.

A **site link** is a configurable object that represents a connection between sites. Site links created using the Active Directory Sites and Services snap-in are the core of Active Directory replication. The site links can be adjusted for replication availability, bandwidth costs, and replication frequency. Windows Server 2003 uses this information to generate the replication topology for the sites, including the schedule for replication. Figure 1-17 shows an example of a site structure within a domain. Each site contains domain controllers that share a high-speed connection. Because of a slower WAN connection between Boston, Hong Kong, and London, sites and site links have been defined to better control replication and logon traffic.

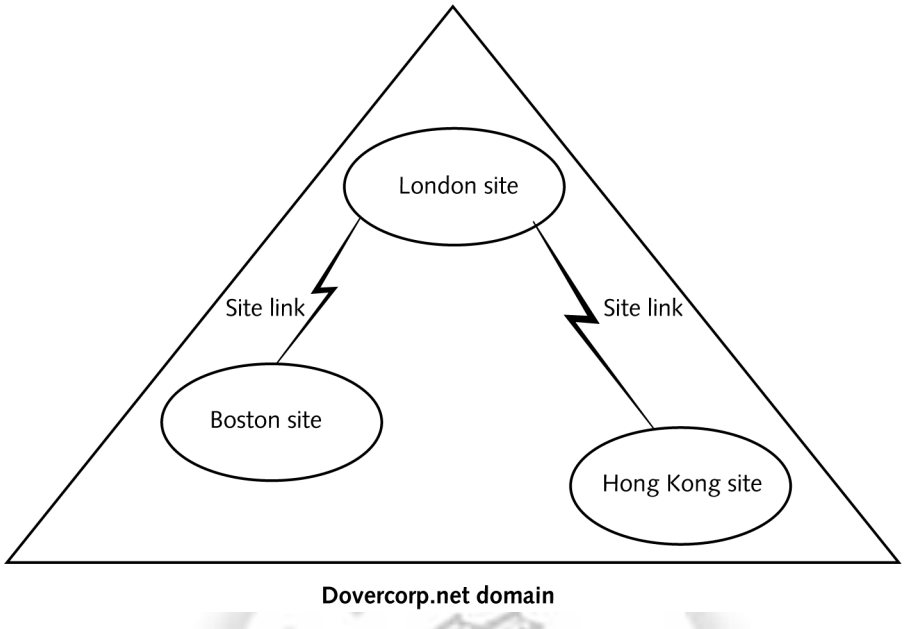

Figure 1-17 The site structure of Dovercorp.net

Replication within a site takes place based on a change notification process. If any change is made within Active Directory, the server waits 15 seconds and then announces the changes to another domain controller. In cases where a domain controller has multiple replication partners within a site, changes are sent out to additional domain controllers at three-second intervals. Replication between sites is initially set at every three hours by default, but can easily be changed by editing the properties of the site link object.

Chapter Summary

- Windows Server 2003 is available in four different editions—Standard Edition, Enterprise Edition, Datacenter Edition, and Web Edition. The edition chosen for a particular environment or server implementation depends upon the individual performance, scalability, and reliability needs of the business or organization.
- Windows networks use one of two models to logically group computers. A workgroup is a model characterized by decentralized authentication and administration, and is typically used on smaller networks. A domain provides centralized authentication and administration, and is more common in larger environments.
- Managing and maintaining a Windows Server 2003 environment consists of five major focus areas: managing physical and logical devices; managing users, computers, and groups; managing and maintaining access to resources; managing and maintaining a server environment; and managing and implementing disaster recovery.
- Active Directory is the native directory service for Windows Server 2003 operating systems. Active Directory provides a variety of services to a network environment including centralized management and administration, authentication services, and more.

- The logical components of Active Directory include domains, organizational units, trees, forests, and the global catalog. The physical components of Active Directory include domain controllers and sites.

KEY TERMS

Active Directory (AD) — The directory service included with Windows Server 2003 that provides a single point of administration, authentication, and storage for user, group, and computer objects.

Active Directory schema — Contains the definition of all object classes and attributes used in the Active Directory database.

attributes — Used to define the characteristics of an object class within Active Directory.

clustering — The ability to increase access to server resources and provide fail-safe services by linking two or more computer systems so they appear to function as though they are one. Clustering is only supported in Windows Server 2003 Enterprise and Datacenter editions.

distinguished name (DN) — An LDAP component used to uniquely identify an object throughout the entire LDAP hierarchy by referring to the relative distinguished name, domain name, and the container holding the object.

domain — A logically structured organization of objects, such as users, computers, groups, and printers, that are part of a network and share a common directory database. Domains are defined by an administrator and administered as a unit with common rules and procedures.

domain controller — A Windows Server 2003 system explicitly configured to store a copy of the Active Directory database, and service user authentication requests or queries about domain objects.

forest — A collection of Active Directory trees that do not necessarily share a contiguous DNS naming convention but do share a common global catalog and schema.

forest root domain — The first domain created within the Active Directory structure.

global catalog — An index of the objects and attributes used throughout the Active Directory structure. It contains a partial replica of every Windows Server 2003 domain within Active Directory, enabling users to find any object in the directory.

Group Policy — The Windows Server 2003 feature that allows for policy creation that affects domain users and computers. Policies can be anything from desktop settings to application assignments to security settings and more.

Lightweight Directory Access Protocol (LDAP) — An access protocol that defines how users can access or update directory service objects.

member server — A Windows Server 2003 system that has a computer account in a domain, but is not configured as a domain controller.

Microsoft Management Console (MMC) — A customizable management interface that can contain a number of management tools to provide a single, unified application for network administration.

multimaster replication — A replication model in which any domain controller accepts and replicates directory changes to any other domain controller. This differs from other replication models in which one computer stores the single modifiable copy of the directory and other computers store back-up copies.

object — A collection of attributes that represent items within Active Directory, such as users, groups, computers, and printers.

object classes — Define which types of objects can be created within Active Directory, such as users, groups, and printers.

Organizational unit (OU) — An Active Directory logical container used to organize objects within a single domain. Objects such as users, groups, computers, and other OUs can be stored in an OU container.

Redundant Array of Independent Disks (RAID) — A collection of hard disks that act as a single unit for the purpose of providing fault tolerance or increasing performance.

relative distinguished name (RDN) — An LDAP component used to identify an object within the object's container.

Security Accounts Manager (SAM) database — The local security and account database on a Windows Server 2003 standalone or member server.

site — A combination of one or more Internet Protocol (IP) subnets connected by a high-speed connection.

site link — A low-bandwidth or unreliable/occasional connection between sites. Site links can be adjusted for replication availability, bandwidth costs, and replication frequency. They enable control over replication and logon traffic.

Software Update Services (SUS) — Microsoft software that allows security patches and updates to be deployed from a centralized server.

Terminal Services — A Windows Server 2003 service that allows a user to connect to and run applications on a server as if sitting at the server console.

transitive trust — The ability for domains or forests to trust one another, even though they do not have a direct explicit trust between them.

User Principal Name (UPN) — A user-account naming convention that includes both the user name and domain name in the format user@domain.com.

workgroup — A logical group of computers characterized by a decentralized security and administration model.

REVIEW QUESTIONS

1. What is the name of the first domain installed within the Active Directory database?
   a. Master root domain
   b. Forest root domain
   c. Main root domain
   d. Tree root domain

2. Assuming a user name of John Doe with a user account located in the Sales OU of the domain *Dovercorp.net*, what would be the object's distinguished name?
   a. OU=Sales, CN=John Doe
   b. CN=John Doe
   c. CN=John Doe, OU=Sales, DC=Dovercorp, DC=Net
   d. DC=Net, DC=Dovercorp, OU=Sales, CN=John Doe

3. In Windows Server 2003, a two-way, transitive trust relationship is maintained between which of the following?
   a. Child and parent forests
   b. Child and parent groups
   c. Child and parent domains
   d. None of the above

4. What is the absolute minimum RAM requirement for Windows Server 2003, Standard Edition?
   a. 64 MB
   b. 128 MB
   c. 256 MB
   d. 512 MB

5. Which of the following are not supported features or configurations for a Windows Server 2003, Web Edition system? (Choose all that apply.)
   a. Standalone server
   b. Domain controller
   c. Member server

6. Which edition of Windows Server 2003 cannot be configured as an Active Directory domain controller?
   a. Windows Server 2003, Web Edition
   b. Windows Server 2003, Standard Edition
   c. Windows Server 2003, Enterprise Edition
   d. Windows Server 2003, Datacenter Edition

7. How often does Active Directory replication between sites take place by default?
   a. Every hour
   b. Every 2 hours
   c. Every 3 hours
   d. Never

8. What is the recommended minimum CPU speed for Windows Server 2003, Enterprise Edition?
   a. 550 MHz
   b. 1 GHz
   c. 733 MHz
   d. 133 MHz

9. How many seconds after a change notification process is triggered does replication between domain controllers occur?
   a. 10
   b. 20
   c. 15
   d. 5

10. The global address list (GAL) for Exchange 2000 e-mail systems is stored on which of the following systems?
    a. All domain controllers
    b. All member servers
    c. All desktop systems
    d. Global catalog server

11. Which group has administrative privileges in all forest domains by default but exists within the forest root domain only?
    a. Administrators
    b. Enterprise Admins
    c. Domain Admins
    d. Forest Admins

12. Which of the following domain controllers will become global catalog servers by default?
    a. First domain controller in all domains
    b. All domain controllers in the forest root domain
    c. First domain controller in the forest root domain
    d. None

13. If a customer network needs to support Windows Server 2003 systems configured in a 4-node cluster, which edition(s) of Windows Server 2003 could be used?
    a. Windows Server 2003, Web Edition
    b. Windows Server 2003, Standard Edition
    c. Windows Server 2003, Enterprise Edition
    d. Windows Server 2003, Datacenter Edition

14. Which of the following operating systems can be upgraded to Windows Server 2003, Standard Edition?
    a. Windows 2000 Server
    b. Windows 2000 Advanced Server
    c. Windows NT Server 4.0 (SP5)
    d. Windows 2000 Datacenter Server

15. Which of the following operating systems can be upgraded to Windows Server 2003, Web Edition?
    a. Windows 2000 Server
    b. Windows NT Server 4.0 (SP5)
    c. Windows 2000 Advanced Server
    d. None of the above

16. Which of the following Windows Server 2003 editions are capable of running on Itanium-based systems?

    a. Windows Server 2003, Web Edition

    b. Windows Server 2003, Standard Edition

    c. Windows Server 2003, Enterprise Edition

    d. Windows Server 2003, Datacenter Edition

17. What is the maximum number of CPUs supported in an SMP configuration on a Windows Server 2003, Datacenter Edition, system running on the x86 platform?

    a. 64

    b. 32

    c. 8

    d. 16

18. Which of the following operating systems can be upgraded to Windows Server 2003, Enterprise Edition?

    a. Windows 2000 Server

    b. Windows Server 2003, Standard Edition

    c. Windows NT Server 4.0 (SP5)

    d. Windows 2000 Advanced Server

19. Which of the following logical Active Directory components is created mainly for the delegation of administrative authority and the implementation of group policy settings?

    a. Tree

    b. Domain

    c. Forest

    d. Organizational unit

20. Which of the following statements best describes an Active Directory forest?

    a. A collection of domains that share a common schema

    b. A collection of organizational units

    c. A collection of trees with different schemas

    d. A collection of users with common settings

CASE PROJECTS

Case Project 1-1

Dover Leasing Corporation has recently implemented Windows Server 2003 and Active Directory. Dover's network consists of three main locations with offices in Boston, Hong Kong, and London. The Boston location is the head office and connects to London via a dedicated T1 WAN link, whereas the Hong Kong location connects to London via a 256-Kbps Frame Relay link. Dover had recently considered opening a new office in San Francisco, which would connect via WAN links to both the Boston and Hong Kong offices. Different password policies need to be implemented in the Boston, Hong Kong, and London locations. Ultimately, the San Francisco office will become the administrative responsibility of IT staff in Boston. Based on what you know of Windows Server 2003 thus far and the information provided above, the IT manager has asked you to assess Dover Leasing's Active Directory design by answering the following questions:

1. Which of the factors listed in the scenario would influence the logical design of Dover Leasing's Active Directory implementation?
2. What type of domain structure would you suggest for Dover Leasing?
3. Based on Dover Leasing's current and future locations, what would be the best naming strategy for their Active Directory domain structure?
4. How many sites would likely be configured as part of Dover Leasing's Active Directory implementation once the San Francisco office opens, and how many site links would be required?
5. Once the San Francisco office is opened, how many global catalog servers should be implemented on the network to ensure adequate performance?

Case Project 1-2

Dover Leasing is currently planning the deployment of three new Windows Server 2003 systems in its head office location. The company plans to deploy one server as a dedicated Web server running IIS 6.0. The second server will be used for file and print services, and will be deployed on an SMP system with 4 CPUs and 8 GB of RAM. The last system will be used as a database server, and will be deployed in conjunction with an existing server as part of a 2-way cluster. Based on these configurations, the IT manager at Dover Leasing has asked you to identify the most appropriate Windows Server 2003 edition for each system.

1. Which Windows Server 2003 edition would be most appropriate for the server that will run IIS? Why?
2. Which Windows Server 2003 edition would be most appropriate for the file and print server? Why?
3. Which Windows Server 2003 edition would be most appropriate for the database server? Why?