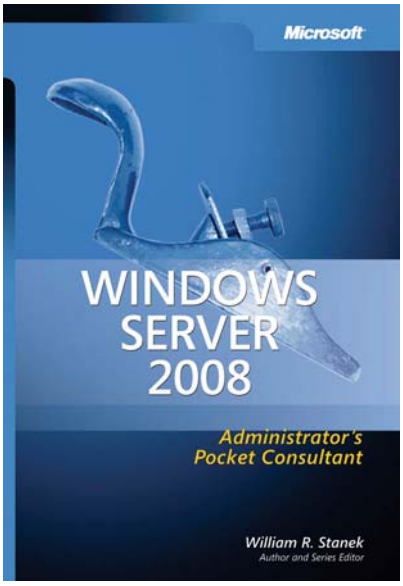

Windows Server® 2008 Administrator's Pocket Consultant

William R. Stanek

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/11449.aspx

978-0-7356-2437-5

Table of Contents

Chapter 7
Using Active Directory

Active Directory Domain Services is an extensible and scalable directory service that you can use to manage network resources efficiently. As an administrator, you'll need to be very familiar with how Active Directory technology works, and that's exactly what this chapter is about. If you haven't worked with Active Directory technology before, one thing you'll notice immediately is that the technology is fairly advanced and has many features. To help manage this complex technology, I'll start with an overview of Active Directory and then explore its components.

Introducing Active Directory

Ever since the introduction of Windows 2000, Active Directory has been the heart of Windows-based domains. Just about every administrative task you'll perform will affect Active Directory in some way. Active Directory technology is based on standard Internet protocols and has a design that helps you clearly define your network's structure.

Active Directory and DNS

Active Directory uses Domain Name System (DNS). DNS is a standard Internet service that organizes groups of computers into domains. Unlike Windows NT 4 domains, which have a flat structure, DNS domains are organized into a hierarchical structure. The DNS domain hierarchy is defined on an Internet-wide basis, and the different levels within the hierarchy identify computers, organizational domains, and top-level domains. DNS is also used to map host names, such as zeta.microsoft.com, to numeric Transmission Control Protocol/Internet Protocol (TCP/IP) addresses, such as 192.168.19.2. Through DNS, an Active Directory domain hierarchy can also be defined on an Internet-wide basis or the domain hierarchy can be separate and private.

When you refer to computer resources in this type of domain, you use the fully qualified domain name (FQDN), such as zeta.microsoft.com. Here, *zeta* represents the name of an individual computer, *microsoft* represents the organizational domain, and *com* is the top-level domain. Top-level domains (TLDs) are at the base of the DNS hierarchy. TLDs are organized geographically, by using two-letter country codes, such as *CA* for Canada; by organization type, such as *com* for commercial organizations; and by function, such as *mil* for U.S. military installations.

Normal domains, such as microsoft.com, are also referred to as *parent domains*. They have this name because they're the parents of an organizational structure. You can divide parent domains into subdomains, which you can then use for different offices, divisions, or geographic locations. For example, the fully qualified domain name for a computer at Microsoft's Seattle office could be designated as jacob.seattle.microsoft.com. Here, *jacob* is the computer name, *seattle* is the subdomain, and *microsoft.com* is the parent domain. Another term for a subdomain is a *child domain*.

As you can see, DNS is an integral part of Active Directory technology—so much so, in fact, that you must configure DNS on the network before you can install Active Directory. Working with DNS is covered in Chapter 20, "Optimizing DNS."

With Windows Server 2008, you install Active Directory in a two-part process. First, you add the Active Directory Domain Services role to the server using the Add Role Wizard. Then, you run the Active Directory Installation Wizard (click Start, type **dcpromo** in the Search field, and then press Enter). If DNS isn't installed already, you will be prompted to install DNS. If there isn't an existing domain, the wizard helps you create a domain and configure Active Directory in a new domain. The wizard can also help you add child domains to existing domain structures. To verify that a domain controller is installed correctly, you can:

- Check the Directory Service event log for errors.
- Ensure that the SYSVOL folder is accessible to clients.
- Verify that name resolution is working through DNS.
- Verify the replication of changes to Active Directory.

Note In the rest of this chapter I'll often use the terms *directory* and *domains* to refer to Active Directory and Active Directory domains, respectively, except when I need to distinguish Active Directory structures from DNS or other types of directories.

Read-Only Domain Controller Deployment

As discussed in Chapter 1, "Microsoft Windows Server 2008 Administration Overview," domain controllers running Windows Server 2008 can be configured as read-only domain controllers (RODCs). When you install the DNS Server service on an RODC, the RODC can act as a read-only DNS Server (RODNS Server). In this configuration, the following conditions are true:

- The RODC replicates the application directory partitions that DNS uses, including the ForestDNSZones and DomainDNSZones partitions. Clients can query an RODNS Server for name resolution. However, the RODNS Server does not support client updates directly because the RODNS Server does not register resource records for any Active Directory–integrated zone that it hosts.
- When a client attempts to update its DNS records, the server returns a referral. The client can then attempt to update against the DNS server that is provided in the referral. Through replication in the background, the RODNS Server will then attempt to retrieve the updated record from the DNS server that made the update. This replication request is only for the changed DNS record. The entire list of changed zone or domain data is not replicated during this special request.

The first Windows Server 2008 domain controller installed in a forest or domain cannot be an RODC. However, you can configure subsequent domain controllers as read-only. For planning purposes, keep the following in mind:

- Prior to adding Active Directory Domain Services (AD DS) for the first time to a server that is running Windows Server 2008 in a Windows Server 2003 or Windows 2000 forest, you must update the schema on the schema operations master in the forest by running adprep /forestprep.
- Prior to adding AD DS for the first time to a server that is running Windows Server 2008 in a Windows Server 2003 or Windows 2000 Server domain, you must update the infrastructure master in the domain by running adprep /domainprep /gpprep.
- Prior to installing AD DS to create your first RODC in a forest, you must prepare the forest by running adprep /rodcprep.

Windows Server 2008 with Windows NT 4.0

Windows Server 2008 domain functions are not designed to interoperate with Windows NT 4.0 domain functions. Domain controllers that are running the Windows NT Server 4.0 are not supported with Windows Server 2008. Servers running Windows NT Server 4.0 are not supported by domain controllers that are running Windows Server 2008. Because of these interoperability issues, you should take the following actions:

- Upgrade domain controllers running Windows NT Server 4.0 prior to deploying any computers running Windows Server 2008.
- Upgrade all computers running Windows NT Server 4.0 prior to deploying any domain controllers running Windows Server 2008.

You can upgrade Windows NT Server 4.0 to Windows 2000 Server or Windows Server 2003. It is important to remember that a Primary Domain Controller (PDC) emulator operations master is still required when you upgrade all computers running Windows NT Server 4.0.

Working with Domain Structures

Active Directory provides both logical and physical structures for network components. Logical structures help you organize directory objects and manage network accounts and shared resources. Logical structures include the following:

Organizational units
A subgroup of domains that often mirrors the organization's business or functional structure.

Domains
A group of computers that share a common directory database.

Domain trees
One or more domains that share a contiguous namespace.

Domain forests
One or more domain trees that share common directory information.

Physical structures serve to facilitate network communication and to set physical boundaries around network resources. Physical structures that help you map the physical network structure include the following:

Subnets
A network group with a specific Internet Protocol (IP) address range and network mask.

Sites
One or more subnets. Sites are used to configure directory access and replication.

Understanding Domains

An Active Directory domain is simply a group of computers that share a common directory database. Active Directory domain names must be unique. For example, you can't have two microsoft.com domains, but you could have a microsoft.com parent domain with seattle.microsoft.com and ny.microsoft.com child domains. If the domain is part of a private network, the name assigned to a new domain must not conflict with any existing domain name on the private network. If the domain is part of the global Internet, the name assigned to a new domain must not conflict with any existing domain name throughout the Internet. To ensure uniqueness on the Internet, you must register the parent domain name before using it. You can register a domain through any designated registrar. You can find a current list of designated registrars at InterNIC (*http:// www.internic.net*).

Each domain has its own security policies and trust relationships with other domains. Domains can also span more than one physical location, which means that a domain can consist of multiple sites and those sites can have multiple subnets, as shown in Figure 7-1. Within a domain's directory database, you'll find objects defining accounts for users, groups, and computers as well as shared resources such as printers and folders.

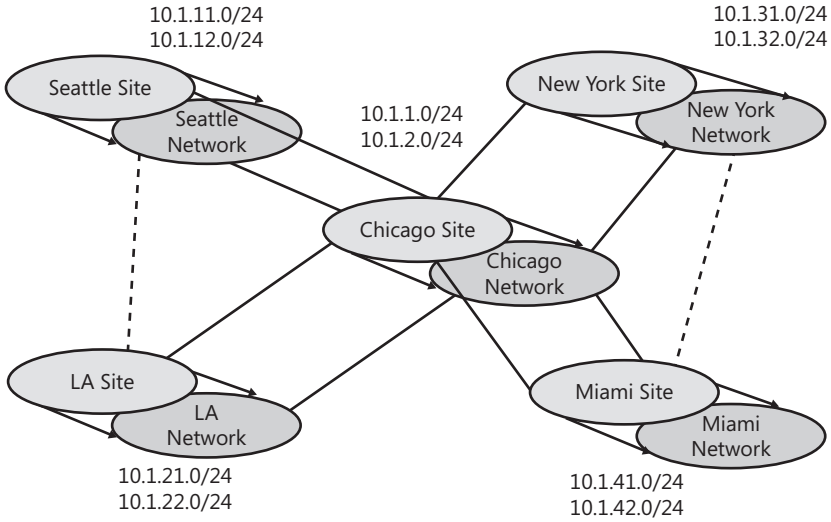

Figure 7-1 This network diagram depicts a wide area network (WAN) with multiple sites and subnets.

> **Note** User and group accounts are discussed in Chapter 9, "Understanding User and Group Accounts." Computer accounts and the various types of computers used in Windows Server 2008 domains are discussed in "Working with Active Directory Domains."

Domain functions are limited and controlled by the domain functional level. Several domain functional levels are available, including the following:

Windows 2000 mixed
Supports domain controllers running Windows NT 4.0 and later releases of Windows Server. However, you cannot use Windows NT 4.0 domain controllers with Windows Server 2008 and you cannot use Windows Server 2008 domain controllers with Windows NT 4.0 servers.

Windows 2000 native
Supports domain controllers running Windows 2000 and later.

Windows Server 2003
Supports domain controllers running Windows Server 2003 and Windows Server 2008.

Windows Server 2008
Supports domain controllers running Windows Server 2008.

For a further discussion of domain functional levels, see "Working with Domain Functional Levels."

Understanding Domain Forests and Domain Trees

Each Active Directory domain has a DNS domain name, such as microsoft.com. One or more domains sharing the same directory data are referred to as a *forest*. The domain names within this forest can be discontiguous or contiguous in the DNS naming hierarchy.

When domains have a contiguous naming structure, they're said to be in the same *domain tree*. Figure 7-2 shows an example of a domain tree. In this example the root domain msnbc.com has two child domains—seattle.msnbc.com and ny.msnbc.com. These

domains in turn have subdomains. All the domains are part of the same tree because they have the same root domain.

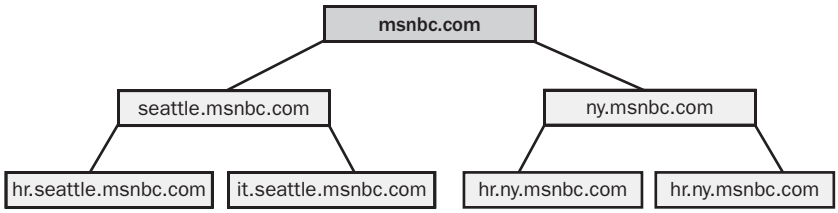

Figure 7-2 Domains in the same tree share a contiguous naming structure.

If the domains in a forest have discontiguous DNS names, they form separate domain trees within the forest. As shown in Figure 7-3, a domain forest can have one or more domain trees. In this example the msnbc.com and microsoft.com domains form the roots of separate domain trees in the same forest.

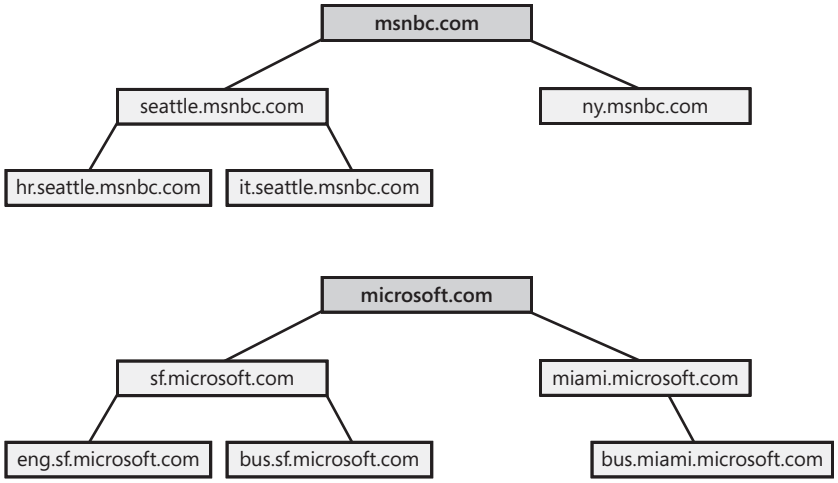

Figure 7-3 Multiple trees in a forest have discontiguous naming structures.

You access domain structures in Active Directory Domains And Trusts, which is shown in Figure 7-4. Active Directory Domains And Trusts is a snap-in for the Microsoft Management Console (MMC); you can also start it from the Administrative Tools menu. You'll find separate entries for each root domain. In Figure 7-4, the active domain is cpandl.com.

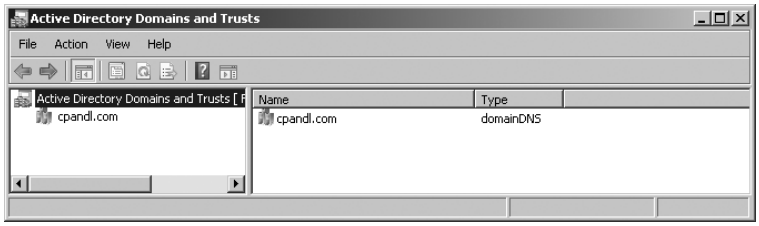

Figure 7-4 Use Active Directory Domains And Trusts to work with domains, domain trees, and domain forests.

Forest functions are limited and controlled by the forest functional level. Several forest functional levels are available, including:

Windows 2000
Supports domain controllers running Windows NT 4.0 and later releases of Windows Server. However, you cannot use Windows NT 4.0 domain controllers with Windows Server 2008 and you cannot use Windows Server 2008 domain controllers with Windows NT 4.0 servers.

Windows Server 2003
Supports domain controllers running Windows Server 2003 and Windows Server 2008.

Windows Server 2008
Supports domain controllers running Windows Server 2008.

The Windows Server 2003 forest functional level offers substantial improvements in Active Directory performance and features over the Windows 2000 forest functional level. When all domains within a forest are operating in this mode, you'll see improvements in global catalog replication and improved replication efficiency for Active Directory data. Because link values are replicated, you might see improved intersite replication as well. You'll be able to deactivate schema class objects and attributes; use dynamic auxiliary classes; rename domains; and create one-way, two-way, and transitive forest trusts.

The Windows Server 2008 forest functional level offers incremental improvements in Active Directory performance and features over the Windows Server 2003 forest functional level. When all domains within a forest are operating in this mode, you'll see improvements in both intersite and intrasite replication throughout the organization. Domain controllers will use DFS replication rather than FRS replication as well. Further, Windows Server 2008 security principals are not created until the PDC emulator operations master in the forest root domain is running Windows Server 2008. This requirement is similar to the Windows Server 2003 requirement.

Understanding Organizational Units

Organizational units are subgroups within domains that often mirror an organization's functional or business structure. You can also think of organizational units as logical containers into which you can place accounts, shared resources, and other organizational units. For example, you could create organizational units named HumanResources, IT, Engineering, and Marketing for the microsoft.com domain. You could later expand this scheme to include child units. Child organizational units for Marketing could include OnlineSales, ChannelSales, and PrintSales.

Objects placed in an organizational unit can only come from the parent domain. For example, organizational units associated with seattle.microsoft.com can contain objects for this domain only. You can't add objects from ny.microsoft.com to these containers, but you could create separate organizational units to mirror the business structure of seattle.microsoft.com.

Organizational units are very helpful in organizing the objects around the organization's business or functional structure. Still, this isn't the only reason to use organizational units. Other reasons include:

- Organizational units allow you to assign a group policy to a small set of resources in a domain without applying this policy to the entire domain. This helps you set and manage group policies at the appropriate level in the enterprise.
- Organizational units create smaller, more manageable views of directory objects in a domain. This helps you manage resources more efficiently.
- Organizational units allow you to delegate authority and to easily control administrative access to domain resources. This helps you control the scope of administrator privileges in the domain. You could grant user A administrative authority for one organizational unit and not for others. Meanwhile, you could grant user B administrative authority for all organizational units in the domain.

Organizational units are represented as folders in Active Directory Users And Computers, as shown in Figure 7-5. This utility is a snap-in for the MMC, and you can also start it from the Administrative Tools menu.

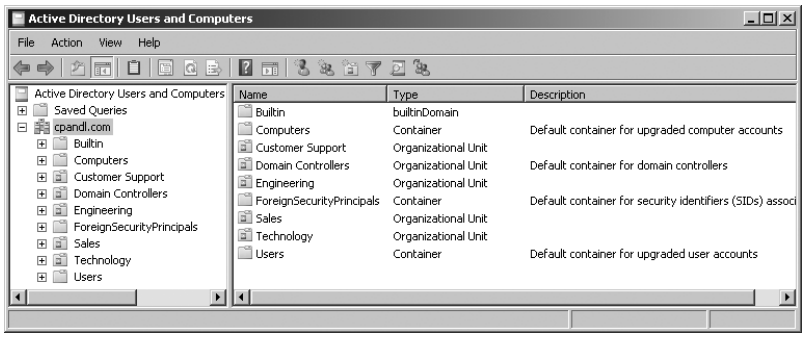

Figure 7-5 Use Active Directory Users And Computers to manage users, groups, computers, and organizational units.

Understanding Sites and Subnets

A site is a group of computers in one or more IP subnets. You use sites to map your network's physical structure. Site mappings are independent from logical domain structures, so there's no necessary relationship between a network's physical structure and its logical domain structure. With Active Directory you can create multiple sites within a single domain or create a single site that serves multiple domains. The IP address ranges used by a site and the domain namespace also have no connection.

You can think of a subnet as a group of network addresses. Unlike sites, which can have multiple IP address ranges, subnets have a specific IP address range and network mask. Subnet names are shown in the form *network/bits-masked*, such as 192.168.19.0/24. Here, the network address 192.168.19.9 and network mask 255.255.255.0 are combined to create the subnet name 192.168.19.0/24.

> **Note** Don't worry, you don't need to know how to create a subnet name. In most cases you enter the network address and the network mask and then Windows Server 2008 generates the subnet name for you.

Computers are assigned to sites based on their location in a subnet or a set of subnets. If computers in subnets can communicate efficiently with one another over the network, they're said to be *well connected*. Ideally, sites consist of subnets and computers that are all well connected. If the subnets and computers aren't well connected, you might need to set up multiple sites. Being well connected gives sites several advantages:

- When clients log on to a domain, the authentication process first searches for domain controllers that are in the same site as the client. This means that local domain controllers are used first, if possible, which localizes network traffic and can speed up the authentication process.
- Directory information is replicated more frequently within sites than between sites. This reduces the network traffic load caused by replication while ensuring that local domain controllers get up-to-date information quickly. You can also use site links to customize how directory information is replicated between sites. A domain controller designated to perform intersite replication is called a *bridgehead server*. By designating a bridgehead server to handle replication between sites, you place the bulk of the intersite replication burden on a specific server rather than on any available server in a site.

You access sites and subnets through Active Directory Sites And Services, as shown in Figure 7-6. Because this is a snap-in for the MMC, you can add it to any updateable console. You can also open Active Directory Sites And Services from the Administrative Tools menu.

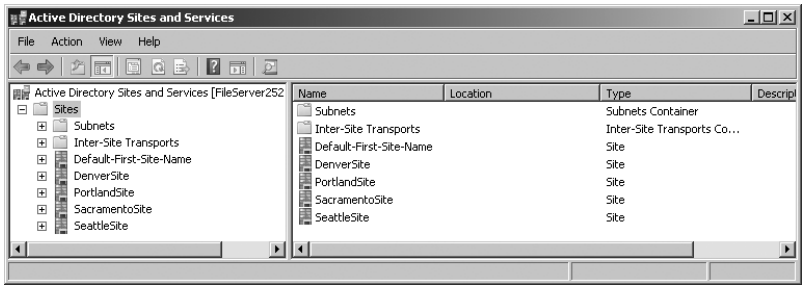

Figure 7-6 Use Active Directory Sites And Services to manage sites and subnets.

Working with Active Directory Domains

Although you must configure both Active Directory and DNS on a Windows Server 2008 network, Active Directory domains and DNS domains have different purposes. Active Directory domains help you manage accounts, resources, and security. DNS domains establish a domain hierarchy primarily used for name resolution. Windows Server 2008 uses DNS to map host names, such as zeta.microsoft.com, to numeric TCP/IP addresses, such as 172.16.18.8. To learn more about DNS and DNS domains, see Chapter 20.

Active Directory is designed to work with systems running Windows Server 2008 as well as systems running Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, and Windows Server 2008. If the necessary client software is installed, Windows 95, Windows 98, Windows 2000, and Windows XP systems access the network as Active Directory clients. Windows NT systems (and Windows 95 or Windows 98 systems not upgraded with Active Directory client software) access the network as if they were in a

Windows NT domain, provided that Active Directory's domain functional level allows this and a Windows NT domain is configured. As discussed previously, domain controllers running Windows NT Server 4.0 are not supported with Windows Server 2008 and servers running Windows NT Server 4.0 are not supported by domain controllers running Windows Server 2008.

Using Windows 2000 and Later Computers with Active Directory

Computers running Windows 2000, Windows XP Professional, and Windows Vista can make full use of Active Directory. These computers access the network as Active Directory clients and have full use of Active Directory features. As clients, these systems can use transitive trust relationships that exist within the domain tree or forest. A transitive trust is one that isn't established explicitly. Rather, the trust is established automatically based on the forest structure and permissions set in the forest. These relationships allow authorized users to access resources in any domain in the forest.

Systems running Windows Server 2000, Windows Server 2003, and Windows Server 2008 provide services to other systems and can act as domain controllers or member servers. A domain controller is distinguished from a member server because it runs Active Directory Domain Services. You promote member servers to domain controllers by installing Active Directory Domain Services. You demote domain controllers to member servers by uninstalling Active Directory Domain Services. You use the Add Role and Remove Role Wizards to add or remove Active Directory Domain Services. You promote or demote a server through the Active Directory Installation Wizard (dcpromo.exe).

Domains can have one or more domain controllers. When there are multiple domain controllers, the controllers automatically replicate directory data with one another using a multimaster replication model. This model allows any domain controller to process directory changes and then replicate those changes to other domain controllers.

Because of the multimaster domain structure, all domain controllers have equal responsibility by default. You can, however, give some domain controllers precedence over others for certain tasks, such as specifying a bridgehead server that has priority in replicating directory information to other sites. In addition, some tasks are best performed by a single server. A server that handles this type of task is called an *operations master*. There are five flexible single master operations (FSMO) roles, and you can assign each to a different domain controller. For more information, see "Understanding Operations Master Roles."

All Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003, and Windows Server 2008 computers that join a domain have computer accounts. Like other resources, computer accounts are stored in Active Directory as objects. You use computer accounts to control access to the network and its resources. A computer accesses a domain using its account, which is authenticated before the computer can access the network.

Real World

Domain controllers use Active Directory's global catalog to authenticate both computer and user logons. If the global catalog is unavailable, only members of the Domain Admins group can log on to the domain. This is because the universal group membership information is stored in the global catalog and this information is required for authentication. In Windows Server 2003 and Windows Server 2008, you have the option of caching universal group membership locally, which solves this problem. For more information, see "Understanding the Directory Structure."

Using Windows 95 and Windows 98 with Active Directory

Systems running Windows 95 and Windows 98 can work with Active Directory in two ways. They can access the network as part of a Windows NT domain, or they can access the network as part of an Active Directory domain. Both techniques depend on a specific network configuration.

Accessing the Network Through a Windows NT Domain

When Windows 95 and Windows 98 systems are used on the network but Active Directory clients aren't installed, these systems can access the network as part of an existing Windows NT domain. Keep the following in mind:

- When Active Directory is in mixed-mode operations, a PDC emulator or a backup domain controller (BDC) must be available to authenticate logons.
- When Active Directory is in native-mode operations, a BDC must be available to authenticate logons.
- When acting as part of a Windows NT domain, Windows 95 and Windows 98 systems can access only resources available through Windows NT one-way trusts, which must be explicitly established by administrators.

Accessing the Network as an Active Directory Client

When using native-mode operations, Windows 95 and Windows 98 systems can access the network as part of an Active Directory domain. To allow a system to access the network as part of an Active Directory domain, you must install Active Directory client software on the system. With the client software, these systems have full use of Active Directory features and can use transitive trust relationships that exist within the domain tree or forest. Transitive trust relationships allow authorized users to access resources in any domain in the domain tree or forest automatically.

Tip Transitive trusts are automatically configured during installation of a domain controller, and you might not need to configure explicit trust relationships. Still, Windows Server 2008 does support explicit trust relationships, and you can establish these relationships if necessary. The main reasons to establish an explicit trust are to enable user authentication in another domain or to simplify the trust path in a complex domain forest.

Installing Active Directory Clients

You install Active Directory client on a Windows 95 or Windows 98 system by following these steps:

1.Log on to the Windows 95 or Windows 98 system you want to configure as a client. Then insert the Windows 2000 Server or Windows Server 2008 distribution CD-ROM into the CD-ROM drive.

Open the Run dialog box by clicking Start and then clicking Run.

In the Open text box, type **E:\Clients\Win9X\Dsclient.exe**, where E is the drive letter of the CD-ROM drive, and click OK, or click Browse to search the distribution CD-ROM. In the Clients folder you'll find a subfolder called Win9X. This folder should contain the client executable. Select the client executable, click Open, and then click OK.

Running the client executable transfers a few essential files to the client and then starts the Directory Service Client Setup Wizard. Read the welcome page, and then click Next.

Install the client software by clicking Next. The wizard detects the system configuration and then installs the necessary client files on the system.

Click Finish to complete the operation and restart the system.

Click Start, choose Settings, and then choose Control Panel. In Control Panel, double-click Network.

On the Configuration tab, select the Ethernet adapter card entry and then click Properties. Make sure that the TCP/IP settings are configured properly to access the Active Directory domain. Configuring TCP/IP settings is discussed in Chapter 17, "Managing TCP/IP Networking."

On the Identification tab, verify the computer name and workgroup information provided. The computer name and workgroup should be set as explained in Chapter 17.

If you changed settings, you'll probably need to restart the computer. After the computer restarts, log on to the system using an account with user permissions in the Active Directory domain. You should be able to access resources in the domain.

Note Windows 95 and Windows 98 systems running as clients don't have computer accounts and aren't displayed in Network Neighborhood. You can, however, view session information for Windows 95 and Windows 98 running as Active Directory clients. Start Computer Management, double-click System Tools, double-click Shared Folders, and then select Sessions. Current user and computer sessions are displayed in the details pane. For more information on shared resources, see Chapter 15, "Data Sharing, Security, and Auditing."

Working with Domain Functional Levels

All Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008 computers must have computer accounts before they can join a domain. To support domain structures, Active Directory includes support for several domain functional levels, including:

Windows 2000 mixed mode
When the domain is operating in Windows 2000 mixed mode, the directory can support Windows Server 2008, Windows Server 2003, Windows 2000, and Windows NT domains. Although it is an advantage to be able to work with Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008, domains operating in this mode can't use many of the latest Active Directory features, including universal groups, group nesting, group type conversion, easy domain controller renaming, update logon timestamps, and Kerberos key distribution center (KDC) key version numbers.

Windows 2000 native mode
When the domain is operating in Windows 2000 native mode, the directory supports Windows Server 2008, Windows Server 2003, and Windows 2000 domains only. Windows NT domains are no longer supported. Domains operating in this mode aren't able to use easy domain controller renaming, update logon timestamps, and Kerberos KDC key version numbers.

Windows Server 2003 mode
When the domain is operating in Windows Server 2003 mode, the directory supports Windows Server 2008 and Windows Server 2003 domains. Windows NT and Windows 2000 domains are no longer supported. A domain operating in Windows Server 2003 mode can use many Active Directory feature enhancements, including universal groups, group nesting, group type conversion, easy domain controller renaming, update logon timestamps, and Kerberos KDC key version numbers.

Windows Server 2008 mode
When the domain is operating in Windows Server 2008 mode, the directory supports only Windows Server 2008 domains. Windows NT, Windows 2000, and Windows Server 2003 domains are no longer supported. The good news, however, is that a domain operating in Windows Server 2003 mode can use all the latest Active Directory feature enhancements, including the DFS Replication service for enhanced intersite and intrasite replication.

Using Windows 2000 Mixed-Mode Operations

You set the domain functional level when you install Active Directory on the first domain controller in a domain. If your domain uses Windows NT 4.0 Server, Windows 2000 Server, Windows Server 2003, and Windows Server 2008, you'll want to use mixed-mode operations (at least initially). However, because of interoperability issues, you will not be able to use domain controllers running either Windows NT 4.0 Server or Windows Server 2008.

In mixed-mode operations, systems that are configured to use Windows NT domains access the network as if they were part of a Windows NT domain. These systems can include Windows 95 and Windows 98 systems that aren't running the Active Directory client, Windows NT workstations, and Windows NT servers. Although the role of Windows

NT workstations doesn't change, Windows NT servers have a slightly different role. Here, Windows NT servers can act as BDCs or member servers only. The Windows NT domain no longer has a PDC. Instead, the Windows NT domain has a domain controller running Windows 2000 Server or later that acts as a PDC to replicate read-only copies of Active Directory and to synchronize security changes to any remaining Windows NT BDCs.

The domain controller acting as a PDC is automatically configured as a PDC emulator operations master. You can assign this role to another domain controller at any time. A controller acting as a PDC emulator supports two authentication protocols:

Kerberos
Kerberos is a standard Internet protocol for authenticating users and systems and the primary authentication mechanism for Windows Server 2008.

NTLM
NT LAN Manager (NTLM) is the primary Windows NT authentication protocol. It's used to authenticate computers in a Windows NT domain.

Note Windows Server 2003 and Windows Server 2008 also support Secure Socket Layer/Transport Layer Security (SSL/TLS) authentication. This authentication mechanism is used with secure Web servers.

Using Windows 2000 Native-Mode Operations

After you upgrade the PDC, BDCs, and other Windows NT systems—and if you still have Windows 2000 domain resources—you can change to the Windows 2000 native-mode operations and then use only Windows 2000, Windows Server 2003, and Windows Server 2008 resources in the domain. Once you set the Windows 2000 native-mode operations, however, you can't go back to mixed mode. Because of this, you should use native-mode operations only when you're certain that you don't need the old Windows NT domain structure or Windows NT BDCs.

When you change to Windows 2000 native mode, you'll notice the following:

- NTLM authentication is no longer supported.
- The PDC emulator can no longer synchronize data with any existing Windows NT BDCs.
- You can't add any Windows NT domain controllers to the domain.

In Windows Server 2008, you switch from Windows 2000 mixed-mode to Windows 2000 native-mode operations by raising the domain functional level.

Using Windows Server 2003 Mode Operations

After you've upgraded the Windows NT structures in your organization, you can begin upgrading to Windows Server 2003 domain structures. You do this by upgrading Windows 2000 domain controllers to Windows Server 2003 or Windows Server 2008 domain controllers and then, if desired, you can change the functional level to the Windows Server 2003 operations mode.

Before being allowed to update Windows 2000 domain controllers, you'll be prompted to prepare the domain for Windows Server 2003. To do this, you'll need to update the forest and the domain schema so that they are compatible with Windows Server 2003 domains. A tool called Adprep.exe is provided to automatically perform the update for you. All you need to do is run the tool on the schema operations master in the forest and then on the infrastructure operations master for each domain in the forest. As always, you should test out any procedure in the lab before performing it in an operational environment.

To perform the upgrade, follow these steps:

1. Check upgrade compatibility on the schema operations master and the infrastructure operations master for each domain in the forest. After inserting the Windows Server 2003 media into the CD/DVD-ROM drive, click Start and then select Run.
2. Type **E:\i386\winnt32.exe /checkupgradeonly**, where E is the drive letter for the CD/DVD-ROM drive, in the Open field of the Run dialog box, and then click OK. This starts the Microsoft Windows Upgrade Advisor.
3. Select No, Skip This Step and then click Next. The Microsoft Windows Upgrade Advisor searches the hardware for any incompatibilities. You should note and correct any incompatibilities before continuing.
4. Upgrade all Windows 2000 domain controllers in the forest to Service Pack 2 or later before continuing. Open Control Panel and then double-click System to check the current service pack. The service pack is listed on the General tab.
5. Log on to the schema operations master for the first domain you want to upgrade in the forest, and then insert the Windows Server 2003 media into the CD/DVD-ROM drive. Click Start and then select Run.
6. In the Open field of the Run dialog box, type **E:\i386\adprep.exe /forestprep**, where E is the drive letter for the CD/DVD-ROM drive, and then click OK. The Command Prompt window opens. Read the directions carefully before continuing. Type **C** to continue or press any other letter to quit.

> **Note** To determine which server is the current schema operations master for the domain, open a command prompt and type **dsquery server -hasfsmo schema**. A directory service path string is returned containing the name of the server, such as: "CN=CORPSERVER01,CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=microsoft, DC=com." This string tells you that the schema operations master is COPRSERVER01 in the microsoft.com domain.

7. Log on to the infrastructure operations master for the first domain you want to upgrade in the forest and then insert the Windows Server 2003 media into the CD/DVD-ROM drive. Click Start and then select Run.
8. In the Open field of the Run dialog box, type **E:\i386\adprep.exe /domainprep**, where E is the drive letter for the CD/DVD-ROM drive, and then click OK. This starts a Command Prompt window. Read the directions carefully before continuing. Type **C** to continue or press any other letter to quit.

Note To determine which server is the current infrastructure operations master for the domain, start a command prompt and type **dsquery server -hasfsmo infr**.

9. Repeat steps 5 to 8 for other domains in the forest as necessary. Upgrade all Windows NT and Windows 2000 domain controllers to Windows Server 2003 or later. Upgrade all Windows NT member servers to Windows 2000 or later.

After upgrading your servers, you can raise the domain and forest level functionality to take advantage of the latest Active Directory features. If you do this, however, you can use only Windows Server 2003 and Windows Server 2008 resources in the domain. After you set the Windows Server 2003 domain or forest functional level, however, you can't go back to any other mode. Therefore, you should use Windows Server 2003 mode only when you're certain that you don't need old Windows NT domain structures, Windows NT BDCs, or Windows 2000 domain structures.

Using Windows Server 2008 Mode Operations

After you've upgraded the Windows NT and Windows 2000 structures in your organization, you can begin upgrading to Windows Server 2008 domain structures. You do this by upgrading Windows Server 2003 domain controllers to Windows Server 2008 domain controllers and then, if desired, you can change the functional level to the Windows Server 2008 operations mode.

Before being allowed to update Windows Server 2003 domain controllers, you'll be prompted to prepare the domain for Windows Server 2008. To do this, you'll need to use Adprep.exe to update the forest and the domain schema so that they are compatible with Windows Server 2008 domains. All you need to do is run **adprep.exe /forestprep** on the schema operations master in the forest and then run **adprep.exe /domainprep** on the infrastructure operations master for each domain in the forest. On the Windows Server 2008 installation media, you'll find Adprep.exe in the sources/adprep folder. As always, you should test out any procedure in the lab before performing it in an operational environment.

Note To determine which server is the current schema operations master for the domain, start a command prompt and type **dsquery server -hasfsmo schema**. To determine which server is the current infrastructure operations master for the domain, start a command prompt and type **dsquery server -hasfsmo infr**.

After upgrading all domain controllers to Windows Server 2008, you can raise the domain and forest level functionality to take advantage of the latest Active Directory features. If you do this, however, you can use only Windows Server 2008 resources in the domain and you can't go back to any other mode. Because of this, you should use Windows Server 2008 mode only when you're certain that you don't need old Windows NT domain structures, Windows NT BDCs, Windows 2000, or Windows Server 2003 domain structures.

Raising Domain and Forest Functionality

Domains operating in Windows Server 2003 or higher functional level can use many enhancements for Active Directory domains, including universal groups, group nesting, group type conversion, update logon timestamps, and Kerberos KDC key version numbers. In this mode administrators will also be able to do the following:

- Rename domain controllers without having to demote them first
- Rename domains running on Windows Server 2008 domain controllers
- Create extended two-way trusts between two forests
- Restructure domains in the domain hierarchy by renaming them and putting them at different levels
- Take advantage of replication enhancements for individual group members and global catalogs

Forests operating in Windows Server 2003 or higher functional level can use the many enhancements for Active Directory forests, which means improved global catalog replication and intrasite and intersite replication efficiency, as well as the ability to establish one-way, two-way, and transitive forest trusts.

Real World

The domain and forest upgrade process can generate a lot of network traffic as information is being replicated around the network. Sometimes the entire upgrade process can take 15 minutes or longer to complete. During this time you might experience delayed responsiveness when communicating with servers and higher latency on the network. You therefore might want to schedule the upgrade outside of normal business hours. It's also a good idea to thoroughly test compatibility with existing applications (especially legacy applications) before performing this operation.

You can raise the domain level functionality by following these steps:

1. Click Start, choose Administrative Tools, and then select Active Directory Domains And Trusts.
2. Right-click the domain you want to work with in the console tree and then select Raise Domain Functional Level.
3. The current domain name and functional level are displayed in the Raise Domain Functional Level dialog box.
4. To change the domain functionality, select the new domain functional level from the selection list provided and then click Raise. However, you can't reverse this action. Consider the implications carefully before you do this.
5. When you click OK, the new domain functional level will be replicated to each domain controller in the domain. This operation can take some time in a large organization.

You can raise the forest level functionality by following these steps:

1. Click Start, choose Administrative Tools, and then select Active Directory Domains And Trusts.
2. Right-click the Active Directory Domains And Trusts node in the console tree and then select Raise Forest Functional Level.
3. The current forest name and functional level are displayed in the Raise Forest Functional Level dialog box.
4. To change the forest functionality, select the new forest functional level using the selection list provided and then click Raise. However, you can't reverse this action. Consider the implications carefully before you do this.
5. When you click OK, the new forest functional level will be replicated to each domain controller in each domain in the forest. This operation can take some time in a large organization.

Understanding the Directory Structure

Active Directory has many components and is built on many technologies. Directory data is made available to users and computers through data stores and global catalogs. Although most Active Directory tasks affect the data store, global catalogs are equally important because they're used during logon and for information searches. In fact, if the global catalog is unavailable, normal users can't log on to the domain. The only way to change this behavior is to cache universal group membership locally. As you might expect, caching universal group membership has advantages and disadvantages, which I'll discuss in a moment.

You access and distribute Active Directory data using directory access protocols and replication. Directory access protocols allow clients to communicate with computers running Active Directory. Replication is necessary to ensure that updates to data are distributed to domain controllers. Although multimaster replication is the primary technique that you use to distribute updates, some data changes can be handled only by individual domain controllers called *operations masters*. A new feature of Windows Server 2008 called *application directory partitions* also changes the way multimaster replication works.

With application directory partitions, enterprise administrators (those belonging to the Enterprise Admins group) can create replication partitions in the domain forest. These partitions are logical structures used to control replication of data within a domain forest. For example, you could create a partition to strictly control the replication of DNS information within a domain, thereby preventing other systems in the domain from replicating DNS information.

An application directory partition can appear as a child of a domain, a child of another application partition, or a new tree in the domain forest. Replicas of the application directory partition can be made available on any Active Directory domain controller running Windows Server 2008, including global catalogs. Although application directory

partitions are useful in large domains and forests, they add overhead in terms of planning, administration, and maintenance.

Exploring the Data Store

The data store contains information about objects such as accounts, shared resources, organizational units, and group policies. Another name for the data store is the directory, which refers to Active Directory itself.

Domain controllers store the directory in a file called Ntds.dit. This file's location is set when Active Directory is installed, and it must be on an NTFS file system drive formatted for use with Windows Server 2008. You can also save directory data separately from the main data store. This is true for group policies, scripts, and other types of public information stored on the shared system volume (Sysvol).

Because the data store is a container for objects, sharing directory information is called *publishing*. For example, you publish information about a printer by sharing the printer over the network. Similarly, you publish information about a folder by sharing the folder over the network.

Domain controllers replicate most changes to the data store in multimaster fashion. As an administrator for a small or medium-sized organization, you'll rarely need to manage replication of the data store. Replication is handled automatically, but you can customize it to meet the needs of large organizations or organizations with special requirements.

Not all directory data is replicated. Instead, only public information that falls into one of the following three categories is replicated:

Domain data
Contains information about objects within a domain. This includes objects for accounts, shared resources, organizational units, and group policies.

Configuration data
Describes the directory's topology. This includes a list of all domains, domain trees, and forests, as well as the locations of the domain controllers and global catalog servers.

Schema data
Describes all objects and data types that can be stored in the directory. The default schema provided with Windows Server 2008 describes account objects, shared resource objects, and more. You can extend the default schema by defining new objects and attributes or by adding attributes to existing objects.

Exploring Global Catalogs

When universal group membership isn't cached locally, global catalogs enable network logon by providing universal group membership information when a logon process is initiated. Global catalogs also enable directory searches throughout all the domains in a forest. A domain controller designated as a global catalog stores a full replica of all objects in the directory for its host domain and a partial replica for all other domains in the domain forest.

Note Partial replicas are used because only certain object properties are needed for logon and search operations. Partial replication also means that less information needs to be circulated on the network, reducing the amount of network traffic.

By default, the first domain controller installed on a domain is designated as the global catalog. So if only one domain controller is in the domain, the domain controller and the global catalog are the same server. Otherwise, the global catalog is on the domain controller that you've configured as such. You can also add global catalogs to a domain to help improve response time for logon and search requests. The recommended technique is to have one global catalog per site within a domain.

Domain controllers hosting the global catalog should be well connected to domain controllers acting as infrastructure masters. The role of infrastructure master is one of the five operations master roles that you can assign to a domain controller. In a domain, the infrastructure master is responsible for updating object references. The infrastructure master does this by comparing its data with that of a global catalog. If the infrastructure master finds outdated data, it requests the updated data from a global catalog. The infrastructure master then replicates the changes to the other domain controllers in the domain. For more information on operations master roles, see "Understanding Operations Master Roles."

When only one domain controller is in a domain, you can assign the infrastructure master role and the global catalog to the same domain controller. When two or more domain controllers are in the domain, however, the global catalog and the infrastructure master must be on separate domain controllers. If they aren't, the infrastructure master won't find out-of-date data and, as a result, will never replicate changes. The only exception is when all domain controllers in the domain host the global catalog. In this case it doesn't matter which domain controller serves as the infrastructure master.

One of the key reasons to configure additional global catalogs in a domain is to ensure that a catalog is available to service logon and directory search requests. Again, if the domain has only one global catalog and the catalog isn't available, and there's no local caching of universal group membership, normal users can't log on and you can't search the directory. In this scenario the only users who can log on to the domain when the global catalog is unavailable are members of the Domain Admins group.

Searches in the global catalog are very efficient. The catalog contains information about objects in all domains in the forest. This allows directory search requests to be resolved in a local domain rather than in a domain in another part of the network. Resolving queries locally reduces the network load and allows for quicker responses in most cases.

Tip If you notice slow logon or query response times, you might want to configure additional global catalogs. But more global catalogs usually mean more replication data being transferred over the network.

Universal Group Membership Caching

In a large organization it might not be practical to have global catalogs at every office location. Not having global catalogs at every office location presents a problem, however, if a remote office loses connectivity with the main office or a designated branch office where global catalog servers reside: normal users won't be able to log on; only domain admins will be able to log on. This is because logon requests must be routed over the network to a global catalog server at a different office; with no connectivity, this isn't possible.

As you might expect, you can resolve this problem in many ways. You could make one of the domain controllers at the remote office a global catalog server by following the procedure discussed in the section titled "Configuring Global Catalogs" in Chapter 8, "Core Active Directory Administration." The disadvantage is that the designated server or servers will have an additional burden placed on them and might require additional resources. You also have to more carefully manage the up time of the global catalog server.

Another way to resolve this problem is to cache universal group membership locally. Here, any domain controller can resolve logon requests locally without having to go through the global catalog server. This allows for faster logons and makes managing server outages much easier: your domain isn't relying on a single server or a group of servers for logons. This solution also reduces replication traffic. Instead of replicating the entire global catalog periodically over the network, only the universal group membership information in the cache is refreshed. By default, a refresh occurs every eight hours on each domain controller that's caching membership locally.

Universal group membership is site-specific. Remember, a site is a physical directory structure consisting of one or more subnets with a specific IP address range and network mask. The domain controllers running Windows Server 2008 and the global catalog they're contacting must be in the same site. If you have multiple sites, you'll need to configure local caching in each site. Additionally, users in the site must be part of a Windows Server 2008 domain running in Windows Server 2008 forest functional mode. To learn how to configure caching, see "Configuring Universal Group Membership Caching" in Chapter 8.

Replication and Active Directory

Regardless of whether you use FRS or DFS replication, the three types of information stored in the directory are domain data, schema data, and configuration data.

Domain data is replicated to all domain controllers within a particular domain. Schema and configuration data are replicated to all domains in the domain tree or forest. In addition, all objects in an individual domain, and a subset of object properties in the domain forest, are replicated to global catalogs.

This means that domain controllers store and replicate the following:

- Schema information for the domain tree or forest
- Configuration information for all domains in the domain tree or forest
- All directory objects and properties for their respective domains

Domain controllers hosting a global catalog, however, store and replicate schema information for the forest, configuration information for all domains in the forest, a subset of the properties for all directory objects in the forest that's replicated between servers hosting global catalogs only, and all directory objects and properties for their respective domain.

To get a better understanding of replication, consider the following scenario, in which you're installing a new network:

1.Start by installing the first domain controller in domain A. The server is the only domain controller and also hosts the global catalog. No replication occurs because other domain controllers are on the network.

Install a second domain controller in domain A. Because there are now two domain controllers, replication begins. To make sure that data is replicated properly, assign one domain controller as the infrastructure master and the other as the global catalog. The infrastructure master watches for updates to the global catalog and requests updates to changed objects. The two domain controllers also replicate schema and configuration data.

Install a third domain controller in domain A. This server isn't a global catalog. The infrastructure master watches for updates to the global catalog, requests updates to changed objects, and then replicates those changes to the third domain controller. The three domain controllers also replicate schema and configuration data.

Install a new domain, domain B, and add domain controllers to it. The global catalog hosts in domain A and domain B begin replicating all schema and configuration data, as well as a subset of the domain data in each domain. Replication within domain A continues as previously described. Replication within domain B begins.

Active Directory and LDAP

The Lightweight Directory Access Protocol (LDAP) is a standard Internet communications protocol for TCP/IP networks. LDAP is designed specifically for accessing directory services with the least amount of overhead. LDAP also defines operations that can be used to query and modify directory information.

Active Directory clients use LDAP to communicate with computers running Active Directory whenever they log on to the network or search for shared resources. You can also use LDAP to manage Active Directory.

LDAP is an open standard that many other directory services can use. This makes interdirectory communications easier and provides a clearer migration path from other directory services to Active Directory. You can also use Active Directory Service Interface (ADSI) to enhance interoperability. ADSI supports the standard application programming interfaces (APIs) for LDAP that are specified in Internet standard Request For Comments

(RFC) 1823. You can use ADSI with Windows Script Host to script objects in Active Directory.

Understanding Operations Master Roles

Operations master roles accomplish tasks that are impractical to perform in multimaster fashion. Five operations master roles are defined; you can assign them to one or more domain controllers. Although certain roles can be assigned only once in a domain forest, other roles must be defined once in each domain.

Every Active Directory forest must have the following roles:

Schema master
Controls updates and modifications to directory schema. To update directory schema, you must have access to the schema master. To determine which server is the current schema master for the domain, start a command prompt and type **dsquery server -hasfsmo schema**.

Domain naming master
Controls the addition or removal of domains in the forest. To add or remove domains, you must have access to the domain-naming master. To determine which server is the current domain naming master for the domain, start a command prompt and type **dsquery server -hasfsmo name**.

These forest-wide roles must be unique in the forest. This means you can assign only one schema master and one domain naming master in a forest.

Every Active Directory domain must have the following roles:

Relative ID master
Allocates relative IDs to domain controllers. Whenever you create a user, group, or computer object, domain controllers assign a unique security ID to the related object. The security ID consists of the domain's security ID prefix and a unique relative ID, which was allocated by the relative ID master. To determine which server is the current relative ID master for the domain, start a command prompt and type **dsquery server -hasfsmo rid**.

PDC emulator
When you use mixed- or interim-mode operations, the PDC emulator acts as a Windows NT PDC. Its job is to authenticate Windows NT logons, process password changes, and replicate updates to the BDCs. To determine which server is the current PDC emulator master for the domain, start a command prompt and type **dsquery server -hasfsmo pdc**.

Infrastructure master
Updates object references by comparing its directory data with that of a global catalog. If the data is outdated, the infrastructure master requests the updated data from a global catalog and then replicates the changes to the other domain controllers in the domain. To determine which server is the current infrastructure operations master for the domain, start a command prompt and type **dsquery server -hasfsmo infr**.

These domain-wide roles must be unique in each domain. This means you can assign only one relative ID master, one PDC emulator, and one infrastructure master in each domain.

Operations master roles are usually assigned automatically, but you can reassign them. When you install a new network, the first domain controller in the first domain is assigned all the operations master roles. If you later create a new child domain or a root domain in a new tree, the first domain controller in the new domain is automatically assigned operations master roles as well. In a new domain forest, the domain controller is assigned all operations master roles. If the new domain is in the same forest, the assigned roles are relative ID master, PDC emulator, and infrastructure master. The schema master and domain naming master roles remain in the first domain in the forest.

When a domain has only one domain controller, that computer handles all the operations master roles. If you're working with a single site, the default operations master locations should be sufficient. As you add domain controllers and domains, however, you'll probably want to move the operations master roles to other domain controllers.

When a domain has two or more domain controllers, you should configure two domain controllers to handle operations master roles. Here, you would make one domain controller the operations master and the second the standby operations master. The standby operations master is then used if the primary fails. Be sure that the domain controllers are direct replication partners and are well connected.

As the domain structure grows, you might want to split up the operations master roles and place them on separate domain controllers. This can improve the responsiveness of the operations masters. Pay particular attention to the current responsibilities of the domain controller you plan to use.

Best Practices Two roles that you should not separate are schema master and domain naming master. Always assign these roles to the same server. For the most efficient operations, you'll usually want the relative ID master and PDC emulator to be on the same server as well. But you can separate these roles if necessary. For example, on a large network where peak loads are causing performance problems, you would probably want to place the relative ID master and PDC emulator on separate domain controllers. Additionally, you usually shouldn't place the infrastructure master on a domain controller hosting a global catalog. See "Exploring Global Catalogs" for details.