Now that you have had an introduction to the concepts of Active Directory and have reviewed DNS, it is time to start looking at how to work with Active Directory. Some of the objectives and subobjectives from the units “Installing, Configuring, and Troubleshooting Active Directory” and “Managing, Monitoring, and Optimizing the Components of Active Directory” are covered in this chapter. The other objectives and subobjectives are covered in other chapters.

The first part of this chapter will look at the logical structure of Active Directory. The last part of the chapter will show you how to create a root domain.

**Install, configure, and troubleshoot the components of Active Directory.**

- Install Active Directory.
- Verify Active Directory installation.
- Create sites.
- Create subnets.
- Create connection objects.
- Create site links.
- Create site link bridges.
- Move server objects between sites.
- Create global catalog servers.

This objective is included primarily to make sure you can install Active Directory and verify that it is installed. This objective also is included to ensure that you can configure a domain to match the physical network. You should know the requirements for installation, primarily the DNS server requirements. You should also understand the changes made to the system due to the installation.
The domain configuration aspect of this objective requires that you know how to set up Active Directory based on the network. This includes creating sites, which are collections of subnets, and then making sure replication is possible using site links and site link bridges. You also need to know how to create a connection object. Using connection objects, you can override the system-generated connections. Finally, you need to know how to create a global catalog server.

Manage and troubleshoot Active Directory replication.

• Manage intrasite replication.
• Manage intersite replication.

This objective is included to ensure that you are familiar with the replication process and are able to recognize and resolve replication issues. An important aspect of managing and troubleshooting Active Directory replication includes understanding the Knowledge Consistency Checker and how it works with site links to build the replication topology. You also need to know how to control the replication topology with the NTDS settings.

Outline

Introduction 90

Understanding AD’s Logical Structure 90

Domains 90
Trees and Forests 91
Organizational Units 95

Installing the First Domain 96

Prerequisites 97
Naming Your Domain 98
The Installation Process 98
Verifying the Installation 102

Other Installations 103

Adding a Domain Controller 104
Adding a Child Domain 105
Creating a Forest 107

Working in the Physical Network 108

Working with Sites 109
Adding a Site 110
Renaming a Site 111
Deleting a Site 111
Site Properties 112
Working with Subnets 113
Adding a Subnet 113
Deleting a Subnet 114
Moving a Subnet 114
This chapter covers three main topics: logical structure, physical structure, and replication. You should understand how these work together to move information around an Active Directory network. Most notably, you should pay attention to the following:

- The installation of domain controllers and their differences depending on where they are logically located
- The creation and use of sites and site links
- The role and function of the Knowledge Consistency Checker
- The ways in which replication takes place and how replication works
- How to use global catalog servers and where they should be placed
INTRODUCTION

The domain controllers serve as the backbone to the network, and being able to implement them in a logical manner is key to the success of any Windows 2000 deployment. In this chapter, you will look at how to roll out the domain controllers and how to configure replication between these controllers. Keeping your organization running smoothly requires the replication of information about both the structure of and the objects in Active Directory.

The chapter begins with a discussion of the logical structures that make up the Active Directory and then moves on to installing domain controllers. After that, the physical world is introduced, and the discussion will turn to subnets and sites. This leads to the discussion of the replication of Active Directory both within a site and between sites.

UNDERSTANDING AD’S LOGICAL STRUCTURE

Although some of the following information has already been introduced, it is worth taking a closer look at the logical structures that make up Active Directory.

The discussion will begin with a look at domains and the purpose of domains, which are the building blocks of the logical structure. Then the discussion will turn to the ways in which you can tie domains together into trees and, eventually, how trees can expand to make up a forest.

Domains

The basic unit you deal with is the domain, just like Windows NT 4.0. By breaking your enterprise into different domains, you achieve several benefits:

- Domains enable you to organize objects within a single department or a single location. Within the domain, all information about the objects is available.
Domains act as a security boundary; domain administrators have complete control over all the resources within the domain. Group policies can be applied at the domain level. Group policies determine how resources can be accessed, configured, and used.

Domain objects can be made available to other domains and can be published in the Active Directory.

Domain names follow the DNS naming structure. This permits an infinite number of child domains.

Domains enable you to control replication; objects stored in the domain are only fully replicated to other domain controllers in the domain.

There are two ways to create Active Directory domains: by upgrading a Windows NT 4.0 domain or by installing a Windows 2000 Server and then promoting it to be a domain controller.

After you have created a root domain, you can then move on to create trees. A tree always starts with the root domain but then can branch out to include other domains. This provides you with the first level of hierarchies within Active Directory.

**Trees and Forests**

When you are controlling the domain, you are dealing with the working level of the network. Users are located in domains. Computers are located in domains. To tie the domains together, you need to organize them into a logical structure. This structure will either be a domain tree or a forest.

Obviously, this is why we had the discussion on DNS in Chapter 2, "Configuring DNS for Active Directory." The DNS hierarchy is used in Windows 2000 to tie the various domains together and to create the domain tree. If you start with a domain such as Widgets.com, for example, you could create a single domain that contains all the objects in your enterprise. However, this might not be practical if your organization has offices in two major geographical areas and if each area works independently from the other. In this case, you might opt to create separate domains that could be independently managed. In Figure 3.1, you will notice that there
is a Widgets.com as well as an East.Widgets.com and a West.Widgets.com. In this case, the top domain is simply a pointer to one or the other of the lower-level domains.

If you were to break the organization down along the lines of an organizational chart, the tree might look more like Figure 3.2. In this figure, there is a domain for sales and marketing, a domain for logistics (production and shipping), and a domain for research and development. The administration and other support roles, in this case, would be in the top-level domain.

Remember from Chapter 1, “Understanding Active Directory,” that throughout this enterprise, there would be a single schema, a common global catalog, and transitive two-way trust relationships.
There are some cases, however, in which a domain tree will not work. In cases in which different parts of the organization need to have separate public identities, you cannot use the same structure if the internal naming is to mirror the external nature. In a case such as this, you might have more than one tree. However, it is still important to keep the three common elements: shared schema, shared configuration, and the global catalog. To do this, one of the domains will become the root of the enterprise. The other domains will be children even though their names look different. In Figure 3.3, Stuff.com has been added. Convention dictates that the line joining the new tree to the forest is drawn to the top of the root to show that it is not just a child domain.
From here, you could add children to Stuff.com (see Figure 3.4).

**FIGURE 3.4**
An expanded domain forest.

After you have installed the first domain controller for the first domain, you can begin to build the hierarchy by using DCPROMO to create other domain controllers. During the promotion, you will have the option of creating new domain controllers in the existing domain, a new controller for a new child domain, or a new root controller for a new tree in the forest.

The combination of trees and forests provides you absolute flexibility in the design of your domain structure and, therefore, in the design of your Active Directory.

Now that you have knowledge of domains, which provide your first level of hierarchy, it makes sense to move on and talk about organizational units (OUs). OUs provide the secondary level of hierarchy. They let you break down a domain into logical units that you can control, to a degree, independently.
Organizational Units

The capability to delegate control of part of a domain to a user or a group of users is new to Windows 2000. This is achieved through the use of organizational units. An organizational unit is a container within the Active Directory you create. After you create the container, you can move computers, users, and other objects into the container.

After this is accomplished, you could delegate control of those objects in the container to a set of users or groups. As a domain administrator, you would still have control, but the people you delegate can also control these objects. This enables you to create workgroup administrators who can handle a limited section of your domain. You can also apply group policies to the organizational unit that are different from those policies you applied to the domain.

Figure 3.5 shows an example of how the Widgets.com network could be fit into a single domain while still providing local administrators to deal with a group of users and computers.

FIGURE 3.5
The Widgets.com network designed using organizational units.
You can even create organizational units within another organizational unit. This enables you to create a hierarchy of organizational units within a domain.

You need to decide for your organization whether you should use domains or organizational units to manage users, computers, and the other objects in Active Directory. The following guidelines should be used to decide whether to use domains or organizational units:

- Use domains if the organization is one in which different users and resources are managed by completely different sets of administrators.
- Use domains for a network in which parts of the network are separated by a slow link. This can also be accomplished using sites, which we will see later in the section “Working in the Physical Network.”
- Use organizational units to mimic the structure of your organization.
- Use organizational units to delegate administrative control over smaller groups of users, groups, and other objects.
- Use organizational units if this particular part of your company is likely to change later.

As you can see, the logical structure of Active Directory is used to build a hierarchy that enables you to organize users within any size of organization. Using domains, you can create security and replication boundaries; and then using organizational units, you can further divide domains into manageable sections.

The planning of the Active Directory structure is the domain of the network planners. As the implementer, you now need to create the root domain and the rest of the tree and then the organization units.

**INSTALLING THE FIRST DOMAIN**

*Install, configure, and troubleshoot the components of Active Directory.*

- Install Active Directory.
Obviously, this is an important objective because all the other work you will do depends on the capability to install Active Directory. This section starts with an examination of the root installation and then looks at verifying installations. From there, the discussion will turn to the other types of installations.

Now that you are familiar with the logical structure of Active Directory, it is time to look at the installation of Active Directory. The installation is a simple process. Before beginning installation, however, you will want to have planned the structure of your enterprise.

**Prerequisites**

As you have probably guessed, a number of necessary items and tasks need to be completed before you install Active Directory. The following is a list of the key items that need to be in place:

- You need to have a Windows 2000 Server, Advanced Server, or Data Center Server installed and running.
- You should have a DNS server installed with a forward lookup zone configured. The DNS server needs to support Service (SRV) records and should allow for dynamic updates and standard zones incremental transfers.
- You need to be sure that the correct DNS server is selected for the computer you are making a domain controller and that the name of the computer is correct. The computer also needs to have TCP/IP installed and correctly functioning.
- You need to be sure that you have an NTFS partition on the computer you are making into a domain controller. You also need to have enough space for the directory (1GB is recommended).
- You need to be sure that the system time zone is correct. You also need to be sure that the correct time is set on the system.

In addition to the physical systems in place to install the domain controller, you need to know the name of the domain controller to install. You also need to know the domain name for the domain you are creating.
Naming Your Domain

There are several different ways you can decide to name the domain. The three main choices are:

❖ **Use your organization’s real Internet domain name.** This would mean that your internal and external identities would be the same, and the risk is that your Active Directory structure could easily become exposed to the public Internet.

❖ **Use a subdomain under your existing Internet domain.** In other words, create something like AD.widgets.com as the starting point for the Active Directory. This makes it easier to separate the public and private structure. However, this approach adds complexity to the naming system.

❖ **Use a totally separate name internally.** This means you can keep the public and private parts of the network completely separate. Microsoft suggests that you can use .local if you plan to separate the internal and external naming of the organization. You might use Widgets.com for the Internet and Widgets.local for the Active Directory.

The domain name, of course, should be decided before you begin to perform the installations. Naming domains will require probably a lot of discussion. Assuming you have all the required information and the prerequisites are met, it is time to install Active Directory.

The Installation Process

The installation of the root domain is very straightforward, and the complete process is outlined in the following Step by Step.

**STEP BY STEP**

3.1 Installing Active Directory

1. From the Start menu, choose Run. Enter `dcpromo` and then click OK.

2. Click Next to pass the introductory screen of the Active Directory Installation Wizard.
3. Choose Domain Controller for a New Domain and then click Next (see Figure 3.6).

4. Choose Create a New Domain Tree and then click Next (see Figure 3.7).

5. Choose Create a New Forest of Domain Trees and click Next (See Figure 3.8).

6. Enter the Full DNS name for the new domain and click Next (See Figure 3.9).

NOTE

If the first part of the name is the name for your existing NT domain, you will receive a warning, and the down-level (NetBIOS) domain name will include a number to differentiate it from the existing domain. This will not happen when you upgrade an existing PDC (see Figure 3.10).
7. Confirm the down-level (NetBIOS) domain name (see Figure 3.11).

8. Confirm the location of the Active Directory database and log files. It is best to place these on different drives for recoverability. Both must be located on a drive formatted with NTFS (see Figure 3.12).

9. Confirm the location of the SYSVOL directory (which replaces the Netlogon share). This must be located on a drive formatted with NTFS 5 (see Figure 3.13).
10. The wizard now confirms your DNS server. You will receive a warning if it does not find the server (see Figure 3.14).

11. Next you will receive a security warning about pre-Windows 2000 RAS security. In NT 4.0 and prior, the RAS server had to allow clients to read domain information before authentication. If you run down-level RAS servers, you need to allow the weaker permissions. Choose the appropriate option and click Next (see Figure 3.16).

12. Next you are prompted to enter the directory services Restore-mode password. You should make this a secure password and should safely store the password so it can’t be forgotten (see Figure 3.17).
13. The next screen will summarise all the choices you have made to this point. You should review the entries and, if necessary, use the Back button to go back and change any of the options that are not correct (see Figure 3.18).

At this point, Active Directory will be installed. After the system has restarted, you might want to verify the installation.

14. Assuming that all has gone well, you should now get a final screen confirming the installation of Active Directory. Click Finish and then restart the computer (see Figure 3.19).

Verifying the Installation

- Verify Active Directory installation.

After the installation of Active Directory, you should verify that the installation worked and that the system is running correctly. This will ensure that the other servers you add to the domain and the other domains you add to the tree will install correctly.
It is a fairly simple matter to verify that Active Directory is installed on the computer. All you need to do is verify that the following options are now in the Administrative Tools folder on the Start menu.

- **Active Directory Users and Computer.** This is used to manage users and computers as well as organizational units within your domain.
- **Active Directory Domains and Trusts.** This is used to manage domains and trust relationships with NT 4.0 domains.
- **Active Directory Sites and Services.** This is used to configure the directory services site and the replication between sites.

You can also use the following steps to make sure Active Directory is installed.

**STEP BY STEP**

3.2 Verifying That Active Directory Is Installed

1. Open Active Directory Users and Computers.
2. Click on the Domain Controllers folder.
3. Verify that your computer is listed.

Getting the first domain controller installed and running correctly is critical because all the other installations will need to communicate with this system as they proceed.

After you have your first domain controller, you will need to add others. The next few sections cover the differences for the various types of setups you will need to perform.

**Other Installations**

Now that you have a working domain controller, you will want to add at least one other domain controller for redundancy. In most
cases, you will add several more domain controllers to a domain. In addition, you need to be able to add other domains to your domain tree or more trees to the forest. This section looks at these types of installations.

**Adding a Domain Controller**

To provide redundancy and load balancing, you need to add more domain controllers to the domains you create. The process for adding a domain controller is straightforward. You begin with a computer with Windows 2000 Server, Advanced Server, or Data Center Server installed. Then you do the following.

**STEP BY STEP**

3.3 Adding a Domain Controller to an Existing Domain

1. From the Start menu, choose Run. Enter `dcpromo` and then click OK.

2. Click Next to pass the introductory screen of the Active Directory Installation Wizard.

3. Choose Additional Domain Controller for an existing domain and then click Next.

4. You will be asked for your network credentials. The credentials you provide should be those of a member of the Domain Admins group. When you have entered the credentials, click Next to continue.

5. Next you will be asked for the name of the domain you want to join. This is the full DNS name of the domain. You should make sure the system is using a DNS server that can resolve the name. After this is entered, click Next to continue.

6. You will now be asked where you want to put the database and the log for Active Directory. This needs to be on an NTFS partition. Enter the location for these files and then click Next to continue.
7. Next you need to enter the location of the SYSVOL directory. This also needs to be on an NTFS partition; after you have entered the location, click Next to continue.

8. You will be asked for the Active Directory Restore-mode password. Enter the password and click Next.

9. Next you will get the summary screen. Click the Finish button and the Active Directory information will be copied.

10. When the copy is finished, you are prompted to restart the computer.

You should now be able to add a domain controller to an existing domain. Using multiple domain controllers is important for redundancy and for load balancing. The next section looks at adding a child domain to an existing domain.

**Adding a Child Domain**

As you build the Active Directory structure for your organization, you will probably need to add child domains. The process is more like creating a new domain than adding a domain controller. The basic steps follow.

**STEP BY STEP**

3.4 Adding a Child Domain to a Domain Tree

1. From the Start menu, choose Run. Enter `dcpromo` and then click OK.

2. Click Next to pass the introductory screen of the Active Directory Installation Wizard.

3. Choose Domain Controller for a New Domain and then click Next.

4. Choose Create a New Child Domain in an Existing Tree and then click Next.

continues
5. Enter the network credentials for a user in the Enterprise Admins group from the parent domain and then click Next.

6. Enter the DNS name for the new domain and the parent domain and click Next.

7. Confirm the down-level (NetBIOS) domain name and click Next.

8. Confirm the location of the Active Directory database and log files. It is best to place these on different drives for recoverability. Both must be located on a drive formatted with NTFS.

9. Confirm the location of the SYSVOL directory (which replaces the Netlogon share). This must be located on a drive formatted with NTFS.

10. Next you get a security warning about pre-Windows 2000 RAS security. In NT 4.0 and prior, the RAS server had to allow clients to read domain information before authentication. If you run down-level RAS servers, you need to allow the weaker permissions. Choose the appropriate option and click Next.

11. You will be asked for the Active Directory Restore-mode password. Enter the password and click Next.

12. Assuming all has gone well, you should now get a summary screen confirming the installation of Active Directory. Click Next and then restart the computer.

After this installation, you would proceed to add more domain controllers to the new domain using the steps in Step by Step 3.3. Remember that child domains act as boundaries for replication and security. Child domains become part of the same namespace. In some cases, this isn’t what you require, and you need to create a new tree, making a forest.
Creating a Forest

Creating a forest is the final setup we'll discuss. Your internal organization will probably use one naming scheme, so creating a forest is not a common event. In any case, the process is almost identical to that of adding a child domain. The following steps help you to create a forest.

STEP BY STEP

3.5 Adding a Root Server in a Forest

1. From the Start menu, choose Run. Enter `dcpromo` and then click OK.

2. Click Next to pass the introductory screen of the Active Directory Installation Wizard.

3. Choose Domain Controller for a New Domain and then click Next.

4. Choose Create a New Domain Tree and then click Next.

5. Choose Place this New Domain Tree in an Existing Forest and then click Next.

6. Enter the network credentials for a user in the Enterprise Admins group from the root domain and then click Next.

7. Enter the DNS name for the new domain and click Next.

8. Confirm the down-level (NetBIOS) domain name and click Next.

9. Confirm the location of the Active Directory database and log files. It is best to place these on different drives for recoverability. Both must be located on a drive formatted with NTFS.

10. Confirm the location of the SYSVOL directory (which replaces the Netlogon share). This must be located on a drive formatted with NTFS.

**NOTE**

DNS Support  Because this domain will be the start of a new tree, it will also be the start of a separate namespace. If the DNS server is not set up correctly, you will have the same options as you did during the installation of the initial domain controller as seen in Step by Step 3.1.
11. You next get a security warning about pre-Windows 2000 RAS security. In NT 4.0 and prior, the RAS server had to allow clients to read domain information before authentication. If you run down-level RAS servers, you need to allow the weaker permissions. Choose the appropriate option and click Next.

12. You will be asked for the Active Directory Restore-mode password. Enter the password and click Next.

13. Assuming all has gone well, you should now get a final screen confirming the installation of Active Directory. Click Finish and then restart the computer.

As you can see, building the logical structure of Active Directory is fairly simple, and with good planning, it should go fairly smoothly. Remember that domains act as security and replication boundaries, and this is the key reason for using them.

If you were to put hundreds of domain controllers in a single domain, perhaps in different locations, you would still have a replication problem. This problem is addressed by using sites that enable you to further control replication. This requires addressing the physical network.

**WORKING IN THE PHYSICAL NETWORK**

Now that you have seen how to configure the logical portion of Active Directory, it is time to look at configuring the physical side. The physical parts of Active Directory, sites and subnets, are used to control replication. By creating sites and later site links, you will be able to determine at what times replication can occur and how often during that period it will happen.

One of the key parts of using Active Directory is the TCP/IP requirement. TCP/IP is not required simply to enable Windows 2000 to use the DNS system, although that is very important.
TCP/IP enables you to break your enterprise into sites and to control replication between sites. You will also be able to apply group policies to sites, enforcing certain settings for all the computers in a single location.

A site is very simply one or more IP subnets connected by high-speed links. This is perhaps a little vague. High-speed is relative to your environment. Many factors need to be examined when determining what exactly is meant by high-speed. If your domain contains three million objects, your password policy requires passwords to be changed every seven days, and you experience a high turnover of employees, then a 10Mbps LAN might not be able to keep up with the replication required. On the other hand, if you have a few hundred objects in the Active Directory and there are few changes in your environment and only two domain controllers, you might find that a 128Kbps ISDN link is fine.

As a rule of thumb, consider anything that runs T1 (1.54Mbps) and below to be a slow link. In these cases, you want to consider the effect of replication on the link. You probably need to create two sites so you can control the replication between them.

The good news is that sites follow what most organizations already do with their networks. Also, sites are very easy to create and manage in Active Directory. Normally, you already have sites defined in your network, breaking the segments into manageable sections. These sections are normally implemented to control the traffic because this is also the point of sites; the translation from the physical segments into sites is very straightforward.

**Working with Sites**

*Install, configure, and troubleshoot the components of Active Directory.*

- Create sites.

If you were to allow uncontrolled replication on your network, you would have many problems with available bandwidth. This is notably the case when you have a link to a remote office. In these cases, you need to remember that sites are used to control replication traffic and to create the sites you need to control the traffic.
You need to be able to create and manage sites within the Active Directory. The following sections outline how to create and remove sites. Then you will see how to add subnets to a site and how to move domain controllers to a site.

Adding a Site
Adding a site is a very simple procedure. The following steps are involved.

**STEP BY STEP**

3.6 Creating a Site


2. Right-click on the Sites folder and choose New Site (see Figure 3.20).

![Figure 3.20](image)

Choose New Site from the context menu.

3. In the New Object – Site dialog box, enter the name of the new site (see Figure 3.21). Letters and numbers are allowed, but spaces and special characters are not.
4. Click one of the site links and then click OK. Site links are covered later in this chapter.

5. You will get a message telling what the next steps are (see Figure 3.22). Click OK to continue.

As you can see, creating a site is a simple process. You can also rename and delete sites.

**Renaming a Site**

Renaming a site is as simple as renaming a file. The following steps are all you need to do to rename a site.

**STEP BY STEP**

3.7 Renaming a Site

1. Open Active Directory Sites and Services.

2. Open the Sites folder and click on the site you want to rename.

3. Click once again or right-click and choose Rename.

4. Enter the new name and press Enter.

Renaming is useful when you are reorganizing your network or if a remote office changes purpose. Renaming is also useful when a site no longer is needed.

**Deleting a Site**

Deleting a site is just as simple as renaming a site. You should make sure the site is empty before you delete the site; otherwise, some objects could be lost. The following Step by Step walks you through deleting a site.
3.8 Deleting a Site

1. Open Active Directory Sites and Services.
2. Open the Sites folder and click on the site you want to delete.
3. Press the Delete key or right-click and choose Delete. You will get a confirmation dialog box (see Figure 3.23).
4. If you're sure you want to delete the site, click Yes. You will get a warning about a site being a container object and that deleting the site will delete the other objects (see Figure 3.24).
5. Choose Yes to complete the deletion.

Again, you normally only delete sites if you are reorganizing your physical network.

In addition to creating, renaming, and deleting sites, you should be aware of and be able to set the properties of the sites in your network.

### Site Properties

There are some properties you can set for the sites you create in the Active Directory. The following sections describe the properties that can be set for a site. To set the properties, right-click on the site name and choose Properties. This will bring up the Properties dialog box (see Figure 3.25).

The following are the properties you can set on each tab:

- **Site**: Enter a description for the site on this tab.
- **Location**: This enables you to enter a location for the site.
- **Object**: This enables you to see the full name of the object and other details such as when it was created. There is nothing you can edit on this tab.
Chapter 3  BUILDING YOUR ACTIVE DIRECTORY STRUCTURE  113

- **Security.** This enables you to set the security for the object in Active Directory. The default security enables administrators to manage the site and enables others to read the information.
- **Group Policy.** This enables you to assign group policies to the site and create and modify the policies.

Remember that a site is defined as a group of IP subnets connected using high-speed networking. This means you need to be able to work with subnets as well.

**Working with Subnets**

*Install, configure, and troubleshoot the components of Active Directory.*

- **Create subnets.**

Now that you can create and delete sites, you need to be able to populate the sites. This is a matter of deciding which subnets should be in a site and creating them in Active Directory. Decisions about which subnets to include will depend on the network design and how you will actually control the location of objects in Active Directory.

Subnets need to be added, deleted, and moved between sites. In addition, like the other objects in Active Directory, you can set various properties for subnets. The next few sections show you how to perform these functions.

**Adding a Subnet**

Adding a subnet is very simple, as you will see in the following Step by Step.

**STEP BY STEP**

3.9 Creating a Subnet in Active Directory

1. Open Active Directory Sites and Services.
2. Right-click on the Subnets folder and choose New Subnet.

continues
3. In the dialog box, enter the IP address and subnet mask for a system on that subnet.

4. The system automatically converts the information to network ID/number of bits notation (see Figure 3.26).

5. Select the site to which you want to add the subnet and then click OK.

Again, adding a subnet is very simple, but before you click OK, you should make sure you have entered the correct information. Sometimes you will need to delete a subnet.

Deleting a Subnet

Deleting a subnet is as simple as adding a subnet. Follow the following steps to learn how to delete a subnet.

**STEP BY STEP**

3.10 Deleting a Subnet

1. Open Active Directory Sites and Services.

2. Open the Subnets folder and click on the subnet to delete.

3. Press the Delete key or right-click and choose Delete. You will get a confirmation dialog box.

4. Click Yes to confirm the deletion.

Although you can delete subnets, it is far more common to move a subnet to a different site. This happens as the network changes and the distribution of users and servers changes.

Moving a Subnet

There will be times when you need to move a subnet. This can happen when the network grows or shrinks or as the bandwidth between sites is increased.
The steps for moving a subnet are, again, very simple, as shown in the following Step by Step.

**STEP BY STEP**

3.11 Moving a Subnet to Another Site

1. Open Active Directory Sites and Services.
2. Open the Subnets folder and click on the subnet you want to move.
3. Right-click and choose Properties.
4. In the Properties dialog box (see Figure 3.27) on the Subnet tab, use the Site drop-down list to choose the site to which you want to move the subnet.
5. Click OK to complete the move.

In most cases, even moving subnets is a rare occurrence. Moving subnets only happens when the physical network is reorganized.

As you can see, there are other tabs in this dialog box. The following list describes the other options you can set on each tab.

- **Subnet.** This tab enables you to enter a description for the subnet and move it to another site.
- **Location.** This enables you to enter a location for the subnet.
- **Object.** This enables you to see the full name of the object and other details such as when it was created. There is nothing you can edit on this tab.
- **Security.** This enables you to set the security for the object in Active Directory. The default security enables administrators to manage the site and enables others to read the information.

Now that you have created the sites, you need to move the domain controllers into the sites and configure the replication between the sites.
Replicating Active Directory Information

Replication is the process of taking information from one system and copying it to another system. In Windows 2000, replication is a very important element. Changes can occur at any domain controller, not just at a primary domain controller, which was the case in Windows NT 4.0.

In addition to the multiple-master replication model for the domain objects, there is additional information that needs to be replicated throughout the organization. The following is a list of the key information that needs to be replicated.

This section looks at Active Directory replication, starting with an overview of how it works. From there, the specifics of the intrasite replication will be discussed including a look at connections. After that, the discussion turn to how you can control replication between sites. Finally, there will be a quick look at how you configure a global catalog server.

- **Schema information.** You saw in Chapter 1, “Understanding Active Directory,” that this is the actual structure of the database that holds information about the objects in your enterprise. You might recall that all the domains and, therefore, all the domain controllers need to use the same schema for Active Directory to work correctly. The schema must be replicated to all domain controllers.

- **Configuration information.** This is the overall design of the entire enterprise. It includes the domains, their names, and where they fit into the hierarchy. It also includes other information such as the replication topology. This information is used by all the domain controllers and therefore is replicated to all domain controllers.

- **Domain data.** This is the information you store about the objects making up your domain. All the information is replicated within a domain by the domain controllers. The global catalog servers throughout the enterprise replicate a subset of the information.
As you can see, there are two levels of replication. There is the replication within a domain and the replication handled by the global catalog servers. The replication within a domain is primarily handled by the domain controllers. This replication is principally interested in the replication of all the objects in the domain with all the attributes for each of the objects.

The global catalog servers handle the other replication. At least one global catalog server is required in the enterprise. There should also be one global catalog server for each domain and for each site in the enterprise.

The global catalog servers are responsible for replication of the following information:

- The schema information for the forest
- The configuration information for all domains in the forest
- A subset of the properties for all directory objects in the forest (replicated between global catalogs only)
- All directory objects and all their properties for the domain in which the global catalog is located

Now that you know what is replicated, we will look at how replication works.

**How Replication Works**

Replication is based on the *Update Sequence Number* (USN) in Active Directory. The USN tracks, for each domain controller, the number of changes it has made to its version of the directory. As a change is made, the current USN is assigned to the object, and the USN for the domain controller is incremented.

Each domain controller keeps track of its own USN and the USNs for its replication partners. Periodically (every five minutes by default), the server checks for changes on its replication partners. Requesting any changes since the last-known USN for the partner accomplishes this check. The partner can then send all the changes since the USN number.
A domain controller could be offline for a period of time, and after it comes back, it will quickly be able to get back up-to-date.

There is a danger here. Assume a domain controller receives an update. It makes the change and then updates its USN. The domain controller that made the change originally now requests the USN for the server that got the change. Its USN is updated, and therefore, the change is requested. The system that originated the change now has its own change back. If the system made the change and updated its USN, this whole cycle would repeat ad infinitum.

To avoid this scenario, Active Directory tracks the number of originating writes that have occurred for each attribute. The number of times a user changed the value, rather than the number of times it was changed using replication, is tracked. In the preceding case, the first system in which the change was made will find that it has the correct originating write value and will not make the change.

There is also the possibility that two different users could be changing the same attribute of the same object at the same time on two different controllers. When these changes both start to replicate, a conflict will be detected. Windows 2000 will choose the change with the newer time stamp (the more recent change) to resolve the conflict. If the two changes were made at the same millisecond, then the change with the higher globally unique ID will win.

Now that you have seen the theory of replication, it is time to see how the replication is configured within a site and between sites.

**Replication Within a Site**

*Manage and troubleshoot Active Directory replication.*

*Manage intrasite replication.*

Although there is little you need to do with intrasite replication, it is important for you to understand how it works and the components involved. This serves as a basis for intersite replication.

Replication within a site is handled by Active Directory. There is no need for you to take any action. The Knowledge Consistency Checker (KCC) evaluates the domain controllers in the site and automatically creates a replication topology. In general, the KCC configures connections so that each domain controller replicates with at least two other domain controllers.
Chapter 3  BUILDING YOUR ACTIVE DIRECTORY STRUCTURE  119

The KCC automatically adjusts the replication topology as the network conditions change. As domain controllers are added or removed (or just moved), the KCC continues to make sure that each domain controller replicates with at least two others. Within a site, replication does not use compression, and in some cases (such as a password change), the replication is completed on an immediate basis.

Replication within a site is quite easy to work with; there is nothing to do. The KCC does most of the work for you by creating the correct connection objects to link all your servers together.

Connection Objects

Install, configure, and troubleshoot the components of Active Directory.

• Create connection objects.

Connection objects serve as the backbone for replication; they define network paths through which replication can occur. You need to know what these are and how they are defined; you should also be able to define them yourself.

The KCC essentially manages the replication within a site by creating connection objects between the various domain controllers in the site. The KCC also creates connection objects between sites where required.

A connection represents a permanent or temporary network path that can be used for replication. Normally, you will not create the connection objects within a site yourself. It is assumed that all the paths between servers are of equal speed, and therefore, the KCC should be able to handle creating the connection objects.

You can create connections within a site. You can also edit the connections created by the KCC; however, you should be careful when doing this. In the case of a connection that you create, the connection is never evaluated by the KCC and is never deleted until you do so. This could cause problems if your network changes and you neglect to remove the connection you created. In cases in which you edit the connection that the KCC makes, the changes you make will be lost when the KCC next updates the connections.
The main reason you might want to create a connection object is to specify the bridgehead servers that will be used to link to sites. The bridgehead servers will be the main method of replication across a site link. To create a connection object, follow these steps.

**STEP BY STEP**

**3.12 Creating a Connection Object Manually**

1. Open Active Directory Sites and Services.
2. Expand the Sites folder and then expand the site for which you want to create a link.
3. Expand the Servers folder for the site and then expand the server that will be part of the connection.
5. In the dialog box that appears, choose (or find) the server to which you want to create the link and then choose OK.

Connection objects, as you have seen, provide the network paths for replication. This is true whether the connection is within a site or is used to link two sites together.

**Replication Between Sites**

Manage and troubleshoot Active Directory replication.

- Manage intersite replication.

The capability to manage intersite replication is critical for administrators on Windows 2000 networks. Without this capability, the replication would easily saturate WAN connections and make Windows 2000 Active Directory unmanageable.

When the replication within a site is not compressed, replication between sites will be. Within a site, Active Directory assumes a high-speed connection and, to save processing time, does not compress the data. Between-site bandwidth is assumed to be lower. Therefore, Active Directory compresses the data being transferred between sites.
Active Directory also enables the replication between the sites to be scheduled so that it only happens during scheduled hours. During those hours, you still have the option of changing the interval of the replication. Before you can set this up, you need to move a domain controller to another site. Then you need to create a connection between that domain controller and one in another site.

Because replication is done between domain controllers, you need to add domain controllers to the site to which they physically belong. Clients within a site also look for a domain controller in the site to log on to, and by moving a domain controller to the site, you decrease the logon times, increasing satisfaction with the network.

Moving Domain Controllers
Install, configure, and troubleshoot the components of Active Directory.
• Move server objects between sites.

The capability to control replication and to ensure that users are able to log on within a reasonable amount of time requires that you be able to locate domain controllers near the users. This requires that you occasionally move a domain controller between sites.

The purposes of a site are to help manage the replication between domain controllers and to manage replication across slow network links. In addition to creating the site and adding subnets to that site, you need to move domain controllers into the site.

To move a domain controller, follow these simple steps.

STEP BY STEP
3.13 Moving a Domain Controller

1. Open Active Directory Sites and Services.

2. Expand the Sites folder and then expand the site where the server is currently located.

3. In the site, expand the Servers folder.

4. Right-click on the server and choose Move.

5. From the dialog box (see Figure 3.28), choose the destination subnet and click OK.
Moving a domain controller to a site is part of creating and managing sites within Active Directory.

Now that you have moved the domain controllers to different sites, you need to create a site link between the sites. This provides the path through which replication to this site takes place.

**Connecting Sites**

Install, configure, and troubleshoot the components of Active Directory.

- Create site links.

The key to controlling replication is to create sites. Sites enable you to create site links that enable you to control when a link exists and how often replication can take place while the link is available. Multiple site links can be used to create different replication schedules at different times or to provide redundant links with higher costs.

Now that you have moved the domain controllers to different sites, you need to create a site link between the sites. This provides the path through which replication to this site takes place.

By creating and configuring site links, you provide the KCC with information about what connection objects to create to replicate directory data. Site links indicate where connection objects should be created. Connection objects use the network to exchange directory information.

Follow these general steps to create a site link.

**STEP BY STEP**

3.14 Creating a Site Link

1. Open Active Directory Sites and Services.
2. Expand the Sites folder and then the Inter-Site Transports.
3. Right click on the IP or SMTP folder, depending on the protocol you want to use (see the following discussion of the protocols), and then choose New Site Link.
4. Enter a name for the site link in the Name text box. From the Sites Not in This Site Link list, choose the site this will connect and click the Add button. Click OK when you're finished.

When creating site links, you have the option of using either IP or SMTP as the transport protocol for the site link.

- **SMTP replication.** SMTP can only be used for replication over site links. SMTP is asynchronous, meaning it typically ignores all schedules. Beware if you choose to use SMTP over site links; you must install and configure an enterprise certification authority. The certification authority (CA) signs SMTP messages that are exchanged between domain controllers, ensuring the authenticity of directory updates.

- **IP replication.** IP replication uses Remote Procedure Calls (RPC) for replication. This is the same for both intersite and intrasite replication.

After the site link is created, you can go back and set the other properties of the site link. You do this by locating the site link in the IP or SMTP folder and then bringing up the properties of the link.

The General tab on the Properties sheet sets the properties for the site link. There are also Object and Security tabs, which are the same as the tabs previously discussed. The items you can configure follow:

- **Description.** This is a description of the link for your information.

- **Site in This Site Link.** This area can be used to add domain controllers to and remove them from a site link.

- **Cost.** This is a relative value, and it is used by Active Directory to decide what route to use when replicating information. The cheapest available route is used based on the overall cost. This is easy to determine between two sites. When the sites are not directly connected, however, all the combinations of sites that link the two will be evaluated, and the total costs through all the sites are compared.
Replicate Every. This is the interval at which replication takes place over this link.

Change Schedule. This button enables you to change when the site link is available for replication. Replication during the period that the link is available occurs at a frequency determined by the interval.

Site connectors provide the flexibility required to work with the physical network within a domain. In some cases, you might want to control which servers are used for replication. To do this, you need to configure a bridgehead server.

Bridgehead Servers

A bridgehead server is the main server used for intersite replication. You can configure a bridgehead server for each site you create for each of the intersite replication protocols. This enables you to control which server in a site is used to replicate information to other servers. Step by Step 3.15 walks you through the configuration of a bridgehead server.

STEP BY STEP

3.15 Configuring a Server as a Bridgehead Server

1. Open Active Directory Sites and Services and expand the Sites folder.

2. Expand the site in which you want to create a bridgehead server and then expand the Servers folder.

3. Right-click on the server and choose Properties.

4. In the Transports available for intersite transfer area, select the protocol or protocols for which this server should be a bridgehead and click Add.

5. Click OK to set the properties and then close Active Directory Sites and Services.
The capability to configure a server as a bridgehead server gives you greater control over the resources that used for replication between two sites or in cases such as a site link bridge between multiple sites.

**Site Link Bridges**

*Install, configure, and troubleshoot the components of Active Directory.*

- **Create site link bridges.**

In many cases, you do not need to deal with site link bridges. By default, all site links are automatically bridged, a property known as transitive site links. In some cases, you will want to control through which sites data can flow. In these cases, you need to create site link bridges.

By default, all the site links you create are bridged together. This bridging enables all the sites to communicate with each other. If this is not physically possible because of the structure of your network, you need to disable the automatic bridging and create the appropriate site link bridges.

For example, consider the diagram in Figure 3.29. You see three sites (1, 2, and 3) directly connected to each other. In this case, automatic bridging would work fine. However, Site 4 is connected using a low-speed connection, and therefore, you would not want it to replicate with all the other sites. In this case, you would want Site 4 to replicate only with Site 1.

![FIGURE 3.29](image-url)
To resolve this replication problem, you would turn off automatic bridging. Then create a site link containing the three sites that are directly connected. Create a second site link between Site 1 and Site 4. Then create a site link bridge that gives Active Directory a way to get information from Sites 2 and 3 to Site 4 through Site 1 and vice versa.

To disable the automatic bridging, follow these steps.

**STEP BY STEP**

3.16 **Disabling Transitive Site Links (Automatic Bridging)**

1. Open Active Directory Sites and Services.

2. Expand the Sites folder and then the Inter-Site Transports.

3. Right-click on the transport for which you want to turn off the automatic bridging and choose Properties (see Figure 3.30).

4. On the General tab, clear the Bridge all site links check box and click OK.

On the General tab, notice that there is also an option to ignore all schedules. This option is only used to force changes to flow through whether or not replication was currently scheduled.

After you have ensured that transitive site links exist—in other words, that automatic bridging is off—you will need to create the site link bridge (or bridges). This process is outlined in the following Step by Step.

**STEP BY STEP**

3.17 **Creating a Site Link Bridge**

1. Open Active Directory Sites and Services.

2. Expand the Sites folder and then the Inter-Site Transports.
3. Right-click on the transport you want to use and choose New Site Link Bridge.

4. In the Name box, enter a name for the site link bridge.

5. From the list of Site links not in this bridge, select the site links you want to add. Remove any extra site links in the Site links in this bridge box. Click OK when the correct site links are part of the bridge.

Until now, we have dealt with the replication of the domain information. You need to consider the replication of the schema and configuration partitions and of the global catalog. This is handled by global catalog servers.

**Global Catalog Servers**

*Install, configure, and troubleshoot the components of Active Directory.*

- **Create global catalog servers.**

Global catalog servers provide essential information that is used to glue together all the parts of the Active Directory. The global catalog server ensures that the schema and configuration information is distributed to all the domains and it also handles universal group membership. It also provides a method of locating objects in Active Directory.

At the beginning of the preceding discussion on replication, you were told that the global catalog servers would replicate with each other. This replication is accomplished as though the global catalog servers were all in one domain and the KCC handles the replication. Your only choice is whether a domain controller will be a global catalog server. The following Step by Step outlines how to make a domain controller a global catalog server.
3.18 Configuring a Server as a Global Catalog Server

1. Open Active Directory Sites and Services.

2. Expand the Sites folder and expand the site where the server is located. Expand the Servers folder and then expand the server.

3. Right-click the NTDS Setting and choose Properties (see Figure 3.31).

4. If the server should be a global catalog server, make sure the Global Catalog check box is checked. Otherwise, clear the check box. Click OK and you’re finished.

One of the key jobs of an administrator is to keep the directory information up-to-date and to ensure that all the domain controllers have the correct information. Replication makes this possible. You need to understand this for both the exam and real life.
ESSENCE OF THE CASE
There are a few points that you need to consider as you look at this case:

- Some of the physical locations only have a link to one other location. Some form of backup link is needed.
- Some of the locations are large and probably need multiple controllers. These locations might require multiple sites.
- To ensure that locating objects around the world is possible and that users can log on from anywhere, global catalog servers are required at each site.
- Because the domains are divided by function instead of geography, each location requires at least one domain controller for each domain.
- The overall size of any domain is comparatively small. Combined with low turnover and infrequent password changes, there should be minimal replication.
- Because there are domain controllers from each domain local to the location, users are able to make changes that are reflected at their locality, meaning replication does not have to happen immediately.

SCENARIO
In this chapter, you have looked at the physical and logical configuration of Active Directory. In addition, you have seen how to install the domain controller and child domains as well as how to install another tree in the forest.

The other major topic discussed was replication. You should now understand the three partitions of Active Directory: schema, configuration, and domain. You should also understand how these partitions would be replicated.

Recall from the previous case studies that Sunshine Brewing is located in 15 different cities around the world with some of those locations having multiple sites. You might also recall that the domain structure was to follow reporting lines instead of geography because of the very different needs of the users around the world.

Now it is time to implement this in the real world and to look at the concerns and issues that will be faced.

The scenario is very simple. You need to install an Active Directory tree that spans the globe. In addition, you need to ensure that replication is able to keep all the domains in all the locations up-to-date without saturating the bandwidth between any of the locations.

With these facts in mind and considering the general purpose of the network, the following analysis presents a solution for this scenario.
**ANALYSIS**

In looking at this scenario, there are a couple of factors driving the analysis. First, you need to ensure replication. The replication, however, does not need to be any faster than the time it takes a user to physically move between two offices.

This being said, the shorter distances such as Victoria to Los Angeles or Ottawa to New York or Paris to London all take over an hour in the air. This means we should aim for replication every three hours between the main sites and longer between the other sites such as between Cape Town and Buenos Aires.

The other consideration with respect to replication is that not all the locations will have a back link to another location and could become isolated if the main link goes down. To ensure that replication can continue in these cases, secondary sites links need to be configured between locations using the Internet and a virtual private network (VPN) or SMTP as the intersite transport.

SMTP is a choice because the certificate server is able to create a certificate for us, but that only handles the replication. Because you would also want to be able to move other traffic if the main link goes, the VPN makes more sense.

This leaves intersite replication within a location. This can be handled simply by having all the sites within a location use the same site link. Therefore, there is a site link per location. The replication within the site takes place using the defaults. In each location, one site is created to link the locations, and these sites are also part of a site link to at least one other site using the network and two more sites either using the network or a VPN connection. If site links are configured that use VPNs, the cost is set to double the value of the highest network-connected site link.

To control the replication, three hours is used as the interval for sites connected via T1 during the day. Another site link is created for each that replicates once every hour overnight. The timing for other types of connections is based on these timing for T1 connections.
This chapter provided opportunities for hands-on work with Active Directory. As you can see, the structure of Active Directory is basically organized into two parts: the logical and the physical designs. The logical design consists of organizational units that break down the administration of domains, domains that make up the root and branches of a tree, and trees that make up forests.

There is also the physical design that takes the enterprise and breaks this down into high-speed networks. On the physical side, there are multiple sites that make up the network and a Knowledge Consistency Checker that tracks all the site links building the connections forming the replication topology. You have the option of creating your own connections and of modifying the replication topology using your own site link bridges. All these things are put into place to ensure your ability to replicate all the objects in your domain.

In addition, you need to create global catalog servers, typically one per site and one per domain. These global catalog servers replicate the enterprise-wide information such as the global catalog (a list of the objects from all domains with a subset of the attributes), the schema, and the configuration information.

Moving on, you will see how to create and manage objects in Active Directory in Chapter 4, “Administering Active Directory Services,” and how to manage the servers and the special roles some of them take on in Chapter 5, “Managing Servers.”

**KEY TERMS**

- Child domain
- Configuration partition
- Connection objects
- DCPROMO
- Domain partition
- Forest
- Knowledge Consistency Checker
- NTFS
- Originating write
- RAS
- Remote procedure call
- Schema partition
- Simple Mail Transfer Protocol
- Site
- Site link bridges
- site links
- Subnet
- SYSVOL
- Tree
- Update Sequence Number
Exercises

During these exercises, you will need to have at least two computers with which you can work. The computers will be promoted and demoted a few times, so if the computer contains any important information, you should back this information up before you proceed.

### 3.1 Preparing the DNS Server

In this exercise, you will create a DNS standard primary zone that will be used for the remaining exercises. This exercise assumes you have a system with Windows 2000 Server or Advanced Server and the DNS server installed. If this is not the case, refer to Chapter 2, “Configuring DNS for Active Directory,” for how to install DNS.

**Estimated time:** 10 minutes.

1. From the Start menu, choose Programs, Administrative Tools, DNS.
2. Expand your local server and click on the Forward Lookup Zones to set the focus.
3. Right-click on Forward Lookup Zones and choose New Zone.
4. Click Next to skip the introductory screen. Then choose Standard Primary and click Next.
5. Enter `W2KBrewing.com` as the domain name and click Next.
6. On the next screen of the wizard, verify that the filename is `W2KBrewing.com.dns` and then click Next.
7. Click Finish to complete the creation of the zone.
8. Expand Forward Lookup Zones (if it isn’t already expanded) and click on W2KBrewing.com.
9. Right-click W2KBrewing.com and choose Properties.
10. In the Allow dynamic updates? drop-down text box, choose Yes. Click OK and then close the DNS Manager.
12. On the connection for your network card, right-click and choose Properties.
13. Double-click the Internet Protocol and make sure your primary DNS server entry contains your IP address. (Hint: Make sure your IP address is the same as the IP address listed above.)
14. Click OK to close the TCP/IP properties and then click OK again to close the connection properties. Close the My Network Places Properties.

### 3.2 Install a Root Domain Controller

Now that the DNS server is configured to work with Active Directory (that is, it supports SRV records and allows dynamic updates), you can install Active Directory. This exercise assumes that the drive on which Windows 2000 is installed is NTFS. If it is not, use the `CONVERT` command to change it to NTFS.

**Estimated time:** 20 minutes.

1. From the start menu, choose Run and enter `dcpromo`.
2. Click Next to pass the introductory screen of the Active Directory Installation Wizard.
3. Choose Domain Controller for a New Domain and then click Next.
Chapter 3  BUILDING YOUR ACTIVE DIRECTORY STRUCTURE  133

Apply Your Knowledge

4. Choose Create a New Domain Tree and then click Next.
5. Choose Create a New Forest of Domain Trees and click Next.
6. Enter W2KBrewing.com as the full DNS name for the new domain and click Next.
7. Confirm that the down-level domain name is W2KBrewing.
8. Observe the default locations for the Active Directory database and log file. Click Next to accept the default.
9. Observe the location of the SYSVOL directory. Click Next to accept the default.
10. Next you’ll receive the security warning about pre-Windows 2000 RAS security. Click Next to continue.
11. Enter password as the Directory Services Restore-mode password and click Next to continue.
12. Review the summary screen to make sure all the selections are correct and click Next to continue. If they are not, use the Back button to return and correct them.
13. Click Finish and restart your computer when prompted.

3.3 Verifying the Installation of Active Directory

In this exercise, you will verify that Active Directory was correctly installed and that the correct resource records have been added to the DNS server.

Estimated time: 5 minutes.

3.4 Adding a Second Domain Controller

In this exercise, you will add a second domain controller to your domain. This enables you to create sites and configure site links and bridges. This exercise should be performed on a server running Windows 2000 Server or Advanced Server, but not the server installed in Exercise 3.2. The drive that Windows 2000 is installed on also needs to be NTFS.

Estimated time: 15 minutes.

1. Log on to the server as an administrator.
4. For the primary DNS server, enter the address of your existing server. This address was created in the preceding exercises.

5. Close the TCP/IP properties by clicking OK and then close the connection properties by clicking OK. Close the Connections dialog box.

6. From the Start button, choose Run, enter \texttt{dcpromo}, and then press Enter.

7. Click Next to skip the introductory screen.

8. Choose Additional domain controller for an existing domain and click Next.

9. For the network credentials, enter \textit{Administrator} for the username, your administrator password, and the domain \texttt{W2Kbrewing.com} as the domain and click Next.

10. In the Domain to Join text box, enter \texttt{W2Kbrewing.com} and click Next.

11. Accept the default for the database and log locations by clicking Next.

12. Accept the default for the SYSVOL location by clicking Next.

13. When the completion screen is displayed, click Finish and then restart the computer when prompted.

3.5 Managing Sites and Replication

In this exercise, you will create sites and subnets. You will also move one of the domain controllers to a different site. You will configure site links and site link bridges. Finally, you will be configuring a domain controller as a global catalog server. This exercise can be completed from either computer.

This exercise is configuring the network shown in Figure 3.32.

\textbf{FIGURE 3.32}

A sample network for Exercise 3.5.
Chapter 3 BUILDING YOUR ACTIVE DIRECTORY STRUCTURE

APPLY YOUR KNOWLEDGE

Estimated time: 20 minutes.

1. Log on as the Administrator.
2. Open Active Directory Sites and Services (Start, Programs, Administrative Tools).
3. Expand the Sites folder and observe the default contents.
4. Right-click on the Sites folder and choose New Site.
5. Enter HeadOffice and click DEFAULTIP-SITELINK in the list of site links. Click OK to add the site.
6. Read the message and then click OK to clear it.
7. Using steps 4 through 6 as a reference, add the following sites:
   • Production
   • Shipping
   • Sales
8. Expand the Inter-Site Transports folder and right-click on IP. Choose New Site Link.
9. Enter Warehouse as the site link name.
10. Click Production in the list of Sites that are not in this link and click Add. Do the same for Shipping. Click OK to create the site link.
11. Create another site link called Office that contains the HeadOffice and Sales sites.
12. Expand the Default-First-Site-Name and then expand the Servers folder. Your two servers should be listed.
13. Right-click on one of the servers and choose move. Select HeadOffice from the list and click OK.
14. In the same way, move the other server to Production.
15. Right-click the Subnets folder and choose New Subnet.
16. Enter the IP address 10.1.1.0 with a subnet mask of 255.255.255.0. Select HeadOffice as the site for this subnet and click OK.
17. Using steps 15 and 16, add these additional subnets:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.0</td>
<td>255.255.255.0</td>
<td>HeadOffice</td>
</tr>
<tr>
<td>10.1.3.0</td>
<td>255.255.255.0</td>
<td>HeadOffice</td>
</tr>
<tr>
<td>10.2.1.0</td>
<td>255.255.255.0</td>
<td>Production</td>
</tr>
<tr>
<td>10.2.2.0</td>
<td>255.255.255.0</td>
<td>Production</td>
</tr>
<tr>
<td>10.3.1.0</td>
<td>255.255.255.0</td>
<td>Sales</td>
</tr>
<tr>
<td>10.3.2.0</td>
<td>255.255.255.0</td>
<td>Sales</td>
</tr>
<tr>
<td>10.4.1.0</td>
<td>255.255.255.0</td>
<td>Shipping</td>
</tr>
</tbody>
</table>

18. Under Inter-Site Transports, right-click on IP and choose Properties.
19. Clear the check box for Bridge All Site Links and click OK.
20. Right-click IP again and choose New Site Link Bridge.
21. Enter Crosstown as the name and add the Office and Warehouse site links. Click OK to create the bridge.
22. Expand the HeadOffice site and the Servers folder under it. Expand your server and right-click the NTDS Settings.
APPLY YOUR KNOWLEDGE

23. Choose New Active Directory Connection. Click the other domain controller in the list and click OK.

24. Using steps 22 and 23, create a connection from the server in Production to the server in HeadOffice.

25. Right-click either server and choose Properties. In each case, choose IP from the available list of transports for intersite data transfer. Click Add to make this the preferred bridgehead server. Click OK.

26. Repeat step 25 for the other server.

27. Right-click the NTDS Settings for either server and choose Properties. Make sure the Global Catalog is selected and click OK. Repeat for the other server.

28. Close the Sites and Services manager.

8. What options can you set on a site link to control replication?

9. If you create site link bridges manually, what must you do to make sure your site link bridges are used?

10. What can you do to force replication across all site links to take place?

Review Questions

1. What are two main reasons for creating a domain?

2. What is the purpose of an organizational unit?

3. What is the difference between a site link and a site link bridge?

4. When would you create an Active Directory connection?

5. What is the definition of a site?

6. What is difference between a forest and a tree?

7. What type of server is used to replicate the schema for an enterprise?

Exam Questions

1. Colin installs a Windows 2000 Server that will be used during the installation of the Active Directory structure for his organization. He installs the DNS server, creates the domain, and configures it for dynamic updates. When he tries to install the first domain controller, he gets a message that the domain controller for the domain is not available. He decides to continue the installation and fix the problem later. What problem will he need to fix later?

   A. The DNS server needs to be stopped and started.
   B. The server he is installing needs to point to the DNS server.
   C. Only Active Directory–integrated DNS can be used when installing Active Directory. Colin should have chosen to have the wizard install it.
   D. The DNS server needs to be configured for dynamic updates, not the zone.
Apply Your Knowledge

2. Sally is a network administrator and is currently installing Windows 2000 with Active Directory. She has noticed that the replication between the 15 domain controllers is taking a lot of the bandwidth on her 10Mbps Ethernet network.

The location she is working in has three floors. Sally wants to create a separate site for each floor. She has created the three sites and the site links between them, but it doesn't seem to have made a difference. What should she do next?

A. She needs to reboot all the domain controllers.
B. She needs to wait for the Knowledge Consistency Checker to calculate the new connections.
C. She needs to move the domain controllers to the subnets in the Sites and Services manager.
D. There is nothing she can do except upgrade to 100Mbps Ethernet.

3. Marc is the administrator for a network that is part of an Active Directory tree. His network is divided into four different sites spread across two large floors in a downtown office tower.

To work on the hardware on a domain controller, he has shut it down. Everything is going well until a user calls and tells Marc that he can't find the resources in another domain in the tree.

What could be the problem?

A. The site link between that domain the local domain is on the domain controller on which Marc is working.
B. The other domain has lost its primary domain controller.
C. The replication is not scheduled until later in the day.
D. The system Marc is working on is the global catalog server for the site.

4. Harvey has created a Windows 2000 Active Directory structure for his organization. He has set up a single domain containing the 700 users and their computers. The company is divided into two offices with a 56Kbps link between them.

Harvey configures two sites, one for each office, and he configures a site link between them using SMTP. The replication between the sites doesn't seem to be working. What should Harvey do?

A. He needs to create an enterprise certification authority.
B. He needs to install Microsoft Exchange.
C. He needs to install an SMTP-based mail system.
D. He needs a connection faster than 56Kbps.

5. You are writing out the procedures for creating a site for a new administrator who is starting up a new office for your organization. Which of the following is the best method for creating a site?

A. Create the site, select the site link, add the subnets, and then move in the domain controllers.
B. Move the domain controllers, create the site, add the subnets, and then select the site links.
C. Create a temporary site link bridge, add the domain controllers, rename the site that's created, and then add subnets.
D. Create the subnets and then create a site by grouping them. Next create the links and then move in the domain controllers.

6. You are explaining Active Directory replication to your manager to try to convince him that you will need to upgrade your network from the current 2Mbps ARCnet. You are explaining the differences between intersite and intrasite replication. Which of the following is true only of intersite replication?
   A. Managed by the Knowledge Consistency Checker.
   B. Uses remote procedure calls over the Internet Protocol.
   C. Sends the data in a compressed format.
   D. Defined by connection objects.

7. You have a single remote site on your network, and you want to make sure you use the link as little as possible for replication. You create a site link for your office, and then you create a site link between the main site and the remote site. You create a site link bridge so that data going to the remote site will all flow through the main site.

   You monitor the link, and you notice that replication is still taking place from sites other than the main site. What should you do to correct this?
   A. Check for and correct manually created link objects.
   B. Make sure the Ignore Schedule option is not selected.
   C. Make sure the Enable option is set on the site link bridge.
   D. Make sure the Bridge all site links option is not selected.

8. You are helping colleagues study for the 70-217 exam. You are currently studying Active Directory replication and the various partitions. You give them the following four choices listed and ask them to pick out the one that is not a partition of Active Directory. Which item should they choose?
   A. Schema
   B. Configuration
   C. Global catalog
   D. Domain

9. Users in the two remote sites you manage are complaining that the links to the head office where you work are slow. They report that the links have been slow for the last couple days. You check the links and find that they are, in fact, running at 100% capacity. When you investigate further, you determine the cause of the problem is Active Directory replication. When you check the site links you have created, the information is correct that the links should only be checking for changes every four hours during the day and every two hours at night. What else should you check?
   A. You should check the schedule on the site link bridges.
   B. You should check the Ignore Schedule option.
   C. You should make sure other operators are not forcing the replication for some reason.
   D. You should check how many users have been added in the previous 24 hours.
Chapter 3 BUILDING YOUR ACTIVE DIRECTORY STRUCTURE

APPLY YOUR KNOWLEDGE

10. Your company has two separate locations, one of which is in Tokyo and the other in Cape Town. Each location has its own IT department, and each controls all its own users, computers, and groups. Currently, you have a 512Kbps Frame Relay link between them, and the link is close to 100% capacity. The company is currently running as a single domain. You are asked, as the Windows 2000 expert, to suggest the best way to reduce the load on the link. Which of the following do you suggest?
   A. The network is optimal now. Do nothing.
   B. You suggest two sites, one for each location.
   C. You suggest two organization units, one for each location.
   D. You suggest two domains, one for each location.

11. You are writing up a document that will be used as a reference by administrators on your network. You currently have 74,234 users on the network, and your network spans the globe. You are summarizing the steps involved in the creation of a site before you go into details. Which of the following is the correct series of steps that you will summarize?
   A. Create the subnets, name the site, and then move the subnets.
   B. Create the site and connect it to a site link, create the subnets, and then move a controller to the site.
   C. Create the site link and then the site, move a domain controller to the site, and then create the subnets.
   D. Create the site and make sure the site links are correct, create the subnets, and then move the servers to it.

12. You are adding a remote site to your network that will be connected using a 128Kbps ISDN line. The ISDN line is expected to be busy during the day, approximately 80% utilized, and to only have 30% utilization at night. You want to ensure that replication does not use too much bandwidth during the day but that at night it will have sufficient bandwidth to complete any synchronization. The network designers have told you that you must have the capability to replicate at least once during the day. Which of the following will best deal with these requirements?
   A. Create a site link that will only replicate at night and manually force the replication once a day.
   B. Create a site link used during the night that has an interval of 30 minutes and one during the day with an interval of 6 hours.
   C. Create a site link used during the night with a cost of 10 and a day schedule with a cost of 99.
   D. Create a site link used during the night with the default cost and interval and another site link available only from noon until 1 p.m.

13. You have two sites that are linked using a fractional T1 connection. You are working to optimize the replication traffic between the sites. Each site contains one high-end domain controller that is dedicated to global catalog. You want to ensure that replication over the site link uses these two controllers. What should you do to ensure this?
**Apply Your Knowledge**

A. Create connections objects that link these servers.
B. Create a site link bridge that links these servers.
C. Make sure the site link specifies these servers as the bridgehead servers.
D. Create a separate site for each server and link these sites. Then configure a site link between each of the servers and the other servers on their network.

14. You have configured the site links and site link bridges for your network. Replication is working, and all the sites are receiving the updates to Active Directory. You are describing the network you're working on to a colleague, and she tells you that you didn't need to configure site link bridges. Why didn't you have to create the site link bridges?

A. The KCC will create the site link bridges for you.
B. The sites will be automatically bridged.
C. The domain naming master will handle this for you.
D. The global catalog will handle this for you.

15. Your network is very stable. The users don’t change much and neither do the computers. The structure in place is working, and you rarely change anything in Active Directory. You have been working on a bandwidth problem between the main site and a remote site and have determined that there is some replication traffic going across the link during the day. What can you do to remove this traffic?

A. Create a site link that only replicates at night.
B. Create a site link bridge that only replicates at night.
C. Create two site links, one that replicates on a slow schedule during the day and another that replicates more frequently at night.
D. Create two site link bridges, one that replicates on a slow schedule during the day and another that replicates more frequently at night.

**Answers to Review Questions**

1. Domains create a replication and a security boundary within your organization. Users who are members of the Enterprise Administrators security group have the capability to control all domains. However, users who are members of the Domain Admins security group only have control over their own domain. See the section “Understanding AD Logical Structure.”

2. An organizational unit can be used to delegate control of a selected group of computers, users, and other objects within a domain to a user or group. This effectively creates an administrator-type account with a limited scope. Organizational units can also be used to apply group policies. See the section “Organizational Units.”

3. A site link is used to describe a network path that exists directly between two sites, whereas a site link bridge describes a path between two sites that uses a third site to which both of the sites have a site link. See the section “Replication Between Sites.”
Chapter 3  BUILDING YOUR ACTIVE DIRECTORY STRUCTURE  141

**Apply Your Knowledge**

4. Normally, you don’t need to create Active Directory connections. The exception is a case in which the Knowledge Consistency Checker will not be able to correctly find the connection between two servers. Connections represent a direct network path between two servers. See the section “Connection Objects.”

5. A site is best defined as one or more IP subnets interconnected using a high-speed (above T1) network. See the section “Working with Sites.”

6. A tree is a structure that starts at a root domain containing only direct descendants. All the domains share a common namespace. A forest enables you to create the same type of structure; however, there is more than one namespace. See the section “Trees and Forests.”

7. Whereas the domain controllers for a domain are responsible for the replication of objects that belong to the domain, the global catalog servers replicate the information about the enterprise including a list of all objects, the schema, and configuration information. See the section “Global Catalog Servers.”

8. The options you can set on a site link include the scheduled periods during which the site link is available and the interval (frequency) at which the controllers check for updates. See the section “Replication Between Sites.”

9. By default, all site links are bridged. This means that all the sites can be reached through any combination of site links. If you are going to manage this manually, you need to disable the automatic site link bridging in the IP or SMTP properties. See the section “Replication Between Sites.”

10. Site links are only available during scheduled times. If you need to force them all to be available, you need to select the Ignore All Schedules option in the IP or SMTP properties. See the section “Replication Between Sites.”

**Answers to Exam Questions**

1. **B.** In this case, the most likely cause is that the new domain controller is not pointing at the right DNS server. The DNS service in Windows 2000 can host both dynamic and nondynamic zones. In this question, it is set on the zone level, so answer D is incorrect. The switch between modes does not require stopping and starting, so answer A is incorrect. Answer C is interesting because it leads to a chicken-and-egg problem, but it is definitely wrong. See the section “Installing the First Domain.”

2. **C.** Although an upgrade to 100Mbps would probably make all of Sally’s users happy, this is not required and it makes answer D wrong. If you needed to reboot all the servers in your organization every time you added a site, no one would use the operating system. This means answer A is wrong. There might be a delay of a few minutes, but there wouldn’t be that long of a delay in recalculating the connections. Answer B is wrong. C is the correct answer. This makes sense because the domain controllers are all still in the site and would continue to replicate at the same rate. See the section “Moving Domain Controllers.”

3. **D.** In this case, answer A is wrong because site links are between sites in the same domain. Answer B is also wrong because there are no
longer PDCs, only domain controllers. Replication scheduling is set on a site link, and the resources the user wants are in another domain, so answer C is also wrong. This leaves answer D, which is correct. Because the global catalog replicates the entire set of objects from the enterprise (with a few attributes) so that resources can be found, it makes sense that the users can’t find the resource without the global catalog server. See the section “Global Catalog Server.”

4. A. If you are using SMTP for your site links, you need to have an enterprise certification authority. The authority will be used to sign the SMTP packets being sent. The SMTP packets are sent between servers in the sites involved in the site link and do not actually use mail servers, meaning answers B and C are incorrect. SMTP (email) can run over a modem that is as slow as 110 baud (that’s what was available way back when); therefore, answer D is incorrect. See the section “Replication Between Sites.”

5. A. In this case, the best answer is to create the site first, so answers B, C, and D are wrong. You are asked for the site link that the site will be part of during the creation of that site. This means you are selecting the site link as you create it. You can then add subnets and domain controllers (in any order). See the section “Replicating AD Information.”

6. C. In this case, the only difference listed is that it will use compression on the data. The other differences are that you can schedule the replication between sites and set the interval to check for updates. You can also have different links with different costs between two sites, and between sites you could use SMTP. After you define a site link, the KCC handles the connections for you, so answer A is not correct. The intersite replication can use SMTP, but it also uses RPC over IP, so answer B isn’t right. Answer D is incorrect because the KCC automatically establishes all required links for you. See the section “Replicating Active Directory Information.”

7. D. In this case, you might have a problem with a manually created connection, but even a manually created connection has to follow the site link information, so answer A is incorrect. Answer B would be a problem because replication would happen continuously; however, this would not ignore the site link bridge. Answer C is not a valid option. This means that answer D must be and is correct. This option is on by default, and you need to make sure it is off if you need to create site link bridges. See the section “Replication Between Sites.”

8. C. There are three partitions that make up Active Directory: the schema partition that contains all the attributes and classes defining the database, the configuration partition used to hold the domain configuration and trust information, and the domain partition, which is the information about every object in each domain. The global catalog is a subset of the attributes and is not actually a separate partition. See the section “Replicating Active Directory Information.”

9. B. Site link bridges do not have schedules, so answer A is not correct. Although other operators might be forcing replication across the link, you should probably assume they would not be continually doing this for an entire week, meaning answer C is wrong. Answer D falls for a
Apply Your Knowledge

similar reason. It should not take a week for Active Directory replication to complete unless you're using a 110-baud modem. This leaves answer B, which makes sense. This option can be used to force replication if required but should be turned off immediately so that the site link schedules are again respected. See the section “Replication Between Sites.”

10. **D.** In a case like this, in which you have administration on both sides of the link and the locations are essentially running separately either because of geography such as this case or because of business line, you will normally consider a domain. Remember that a domain is a replication and a security boundary. The network is obviously not optimal if you are looking into it. The idea of two sites could work if there was only administration in one site or if the units had to work closely together. This is not the case here. Using an organizational unit, although useful for applying policy and delegating control, does not let you schedule replication and would not fix the problem in this case. See the section “Understanding AD Logical Structure.”

11. **B.** When you are creating a site, first create the site name and choose the site link to which it belongs. If the site link is not appropriate, you should create a new one. Next you create the subnets that will be part of the site, and then you move or create domain controllers in the site. You should also configure the Licensing Site Settings. See the section “Working with Sites.”

12. **D.** In this case, you would use two site links so that everything is automatic. The night schedule is fine with the default or could even be made more frequent. All you need to do additionally is replicate once a day, and doing that replication during lunchtime probably will cause the least interruption. See the section “Replication Between Sites.”

13. **A.** By creating a connection, a network path, between these servers, you will have specified the path replication should take. You could also configure the server objects as the bridgehead servers for that replication protocol; however, that would cause them to be used as the main servers for all site links using that protocol. The site link does not have an option to specify the bridgehead servers, and a site link bridge is used to link sites, not servers. The last option, D, might work if you turned off the automatic site bridging. See the section “Connection Objects.”

14. **B.** Although the KCC won't actually create site link bridges, it will create the required connections so that all the sites will receive the Active Directory updates. The domain naming master deals with domains, so answer C is wrong; the global catalog has nothing to do with this, meaning answer D is wrong. See the section “Site Link Bridges.”

15. **A.** In this case, you can force replication if there is a problem, but after the network reaches a stable point, there is not so much need for replication. Answers B and D are wrong because they talk about site link bridges, and answer C is not the best answer because there would still be replication during the day. See the section “Replication Between Sites.”
### Suggested Readings and Resources