MCSE EXAM MATERIAL

▶ Directory Services

EXAM OBJECTIVES

Directory Services ▶

Exam 70-217

- Install, configure, and troubleshoot the components of Active Directory.
  - Create sites.
  - Create subnets.
  - Create site links.
  - Create site link bridges.
  - Create connection objects.
  - Create global catalog servers.
  - Move server objects between sites.
  - Transfer Operations Master roles.
- Manage Active Directory performance.
  - Monitor, maintain, and troubleshoot domain controller performance.
  - Monitor, maintain, and troubleshoot Active Directory components.
- Manage and troubleshoot Active Directory replication.
  - Manage intersite replication.
  - Manage intrasite replication.

CHAPTER

22

Managing, Optimizing, and Troubleshooting Active Directory Performance

This chapter examines two advanced Active Directory topics: Active Directory replication and Active Directory performance. It also explores how to create, manage, and troubleshoot several Active Directory components that affect replication and performance.

If you administer a small network, you'll probably never need to use the features I'm about to discuss. However, if you administer a large, complex Windows 2000 network, you may find a few ideas in the following pages that could improve the way Active Directory works on your network. In addition, every subject in this chapter is fair game on the Directory Services exam.

Chapter Pre-Test

1. List the three replication partitions in Active Directory.
2. What is intrasite replication?
3. What is intersite replication?
4. What Windows 2000 Server service is responsible for generating the replication topology?
5. Until ________ ________ are created and assigned to a site, the site has no definition and no functionality—it's just an empty Active Directory object.
6. True or False: Bridging is automatically configured for all site links, by default.
7. What are the five operations master roles?
8. What tool can you use to specifically monitor Active Directory Replication?

Overview of Active Directory Replication

The term *replication*, as applied to Active Directory, refers to the process of copying information—and information updates—from the Active Directory data store on one domain controller to other domain controllers. The purpose of replication is to synchronize Active Directory data among the domain controllers in the domain and forest.

Replication of Active Directory is usually partial, meaning that only changes, and not a complete copy of the Active Directory data store, are copied. Typically the only time a complete replication is performed is when you install a new domain controller on the network.

Windows 2000 automatically performs replication in Windows 2000 domains or forests that are fully contained within a single site. Because of this, unless your network consists of multiple sites, you'll probably never have to worry about configuring Active Directory replication. In fact, you can skip the rest of this chapter—unless, of course, you want to pass the Directory Services exam.

EXAM TIP

Study this chapter carefully before you take the Directory Services exam. This chapter alone covers material for 15 of this exam's objectives. Make sure you're thoroughly comfortable with Active Directory replication before you spend the time and money to take this exam.

For the most part, Windows 2000 Active Directory uses a multimaster replication model. In multimaster replication, changes can be made on *any* domain controller. In addition, changes made on any domain controller are replicated to all other domain controllers. No one domain controller controls changes made to Active Directory or Active Directory replication, and so Active Directory is said to use a *multi*master model. This is in contrast to synchronization in Windows NT 4.0, which uses a single-master model, and all changes to objects are controlled by the primary domain controller.

Active Directory uses update sequence numbers (USNs), along with stamps, to track changes made to objects stored in the Active Directory data store. When an object (or any of its attributes) is changed, Active Directory increases the object's USN, and assigns the object a unique stamp that contains a version number, a timestamp, and the GUID of the domain controller on which the change was made. Because each Active Directory object exists on all domain controllers in the domain, during replication, Active Directory must compare the USNs and stamps of each object being replicated to determine which version of the object is the most current. Active Directory replicates only the most current version of each object, and only replicates objects that have changed since the last time replication occurred.

In the next few sections I'll explain three basic Active Directory replication concepts: replication partitions, intrasite replication, and intersite replication.

CROSS-REFERENCE

If it's been a while since you've read Chapter 2, you might want to reread it now before you try to take on the many complex Active Directory concepts in this chapter.

Replication Partitions

The information contained in the Active Directory data store is logically separated into three categories, which Microsoft calls partitions. Each of these partitions is replicated separately, on a partition-by-partition basis, and is replicated to a specified set of replication partners. The Active Directory replication partitions are:

- **Schema partition:** This partition contains the rules that define how objects are created within a forest. The schema partition is replicated to all domain controllers in the forest.
- **Configuration partition:** This partition contains information about the logical structure of Active Directory for the entire forest, including the structure and use of domains, trees, sites, and trust relationships within the forest. The configuration partition is replicated to all domain controllers in the forest.
- **Domain partition:** This partition contains complete, detailed information about every object in the domain. The domain partition is replicated only to the domain controllers within this domain.

Intrasite Replication

Intrasite replication is Active Directory replication that takes place within a single site. A *site*, as you may remember, consists of one or more TCP/IP subnets, which are specified by an administrator and are connected by high-speed, reliable links. Sites do not necessarily correspond to domains: you can have two or more sites within a single domain, or you can have multiple domains in a single site. A site is solely a grouping based on IP addresses.

Windows 2000, by default, automatically performs intrasite replication. Because intrasite replication takes place between domain controllers within the same site, and all of the TCP/IP subnets in a site are connected by high-speed links, intrasite replication is fast. Windows 2000 uses the Remote Procedure Call (RPC) over IP protocol for intrasite replication. All intrasite replication is sent in an uncompressed format.

Windows 2000 automatically determines which domain controllers in a site will replicate with other domain controllers in the site. The Windows 2000 Server service that makes this determination is called the Knowledge Consistency Checker (KCC). The KCC, which runs on all Windows 2000 domain controllers, builds a list of connections between domain controllers within a site, and these connections dictate the path that replication takes between domain controllers. The list of connections that the KCC generates is called the *replication topology*.

By design, the KCC builds the replication topology to ensure that:

- Changes made to any object on any domain controller will be replicated to every domain controller in the site.
- In addition, Active Directory updates will pass through no more than three connections between the domain controller on which the change is made and any other domain controller in the site. (In routing terms, this would be considered a maximum of three hops.)

Although Windows 2000 automatically creates the replication topology within a site, you can add additional connections to this topology to optimize replication within a site. I'll discuss how to create these intrasite connections later in this chapter.

Intrasite replication, by default, takes place once every hour if no changes are made. If a change is made to an Active Directory object, the domain controller on which the change is made initiates intrasite replication with all of its connection partners within five minutes after the change is made. In addition, domain controllers that receive replication updates from other domain controllers also initiate intrasite replication within five minutes after receiving such an update. Because updates are replicated across no more than three connections (hops), this means that any change made to an object is replicated to all domain controllers in the site within 15 minutes.

Intersite Replication

Intersite replication is Active Directory replication that takes place between sites. Unlike intrasite replication, intersite replication is not automatically configured and performed by Windows 2000. An Administrator must manually create and configure sites and other Active Directory components before intersite replication will occur.

Because intersite replication takes place between domain controllers in different sites that are typically separated by WAN links, intersite replication is normally slower than intrasite replication, and often should be scheduled by the administrator so that use of network bandwidth for replication is minimized during the network's peak activity hours. All intersite replication is sent in a compressed format to save network bandwidth.

Two different Windows 2000 protocols can be used for intersite replication: Remote Procedure Call (RPC) over IP, and Simple Mail Transfer Protocol (SMTP). RPC over IP is the preferred protocol and requires the use of fully routed TCP/IP connections between sites. RPC over IP is faster than SMTP.

However, if you don't have fully routed TCP/IP connections between sites, SMTP is your only choice. SMTP can also be used when fully routed TCP/IP connections exist between sites (but this is not recommended) or when other protocols that support SMTP (such as X.400) are used between sites. Another reason SMTP is not recommended is because it can only be used to replicate the schema and configuration partitions. You can't use SMTP to replicate the domain partition.

Managing Components that Affect Replication

There are numerous Active Directory components that affect replication, and I'll introduce you to them shortly. Many of these components must be created by an Administrator, and, once created, must be configured, maintained, or both. Since Windows 2000 automatically configures and performs intrasite replication, the emphasis of this section is on intersite replication, and the Active Directory components involved in this process.

In the following sections, I'll define and discuss how to create and configure sites, subnets, site links, site link bridges, and global catalog servers.

I'll also explain how to move server objects between sites, and how to manage and maintain operations master roles.

Creating Sites

Sites provide a means of grouping computers so that required services (such as logon and authentication) are provided by nearby computers instead of by computers located across costly, slow links. If your network consists of several locations that are connected by slow-to-medium speed WAN links, you might want to consider using sites to manage your network.

Active Directory replication uses sites to determine replication areas and their boundaries. Intrasite replication occurs freely and automatically over high-speed local area connections. Intersite replication, in contrast, can be carefully controlled by an administrator to limit the amount of replication traffic transmitted over WAN links.

When Active Directory is installed, Windows 2000 creates a single, original site named Default-First-Site-Name. All other sites must be manually created by the Administrator. You can use the Active Directory Sites and Services administrative tool to create and manage sites. Active Directory Sites and Services is available on all domain controllers, and on all other Windows 2000 computers on which the ADMINPAK has been installed.

EXAM TIP

The primary tool for creating and configuring Active Directory components and replication is Active Directory Sites and Services. I recommend you use this tool to practice creating sites and other components that affect replication. You'll be glad you did.

STEP BY STEP

CREATING SITES

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. The AD Sites and Services dialog box appears, as shown in Figure 22-1.

   In the left pane of the AD Sites and Services dialog box, right-click the Sites container, and select New Site from the menu that appears.

STEP BY STEP *Continued*

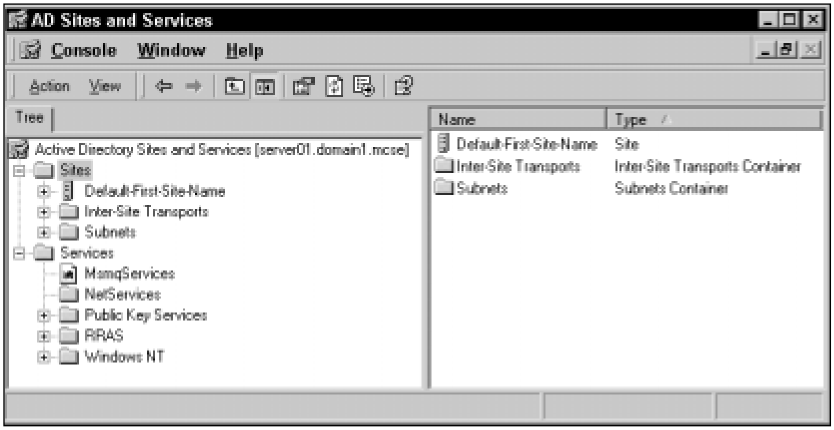
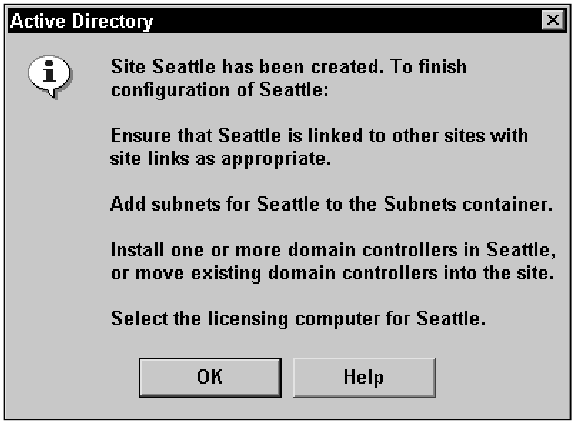


FIGURE 22-1 Active Directory Sites and Services

3. In the New Object – Site dialog box, enter a name for the new site. Then select a site link object for this site from the list box. If you have not yet created any site links, highlight DEFAULTIPSITELINK. Click OK.
4. Active Directory confirms that the site has been created, as shown in Figure 22-2. Notice the various tasks you should perform to complete the configuration of the site. I'll explain how to perform many of these tasks in the sections that follow. Click OK.



Site Seattle has been created. To finish configuration of Seattle:

Ensure that Seattle is linked to other sites with site links as appropriate.

Add subnets for Seattle to the Subnets container.

Install one or more domain controllers in Seattle, or move existing domain controllers into the site.

Select the licensing computer for Seattle.

FIGURE 22-2 Active Directory message: a site has been created

5. The new site appears in the AD Sites and Services dialog box. Close Active Directory Sites and Services.

If you want to configure your newly created site, right-click the site in Active Directory Sites and Services, and select Properties from the menu that appears. In the site's Properties dialog box you can configure a description of the site, the location of the site, and Active Directory permissions for the site object. You can also view the object's properties, and create and configure Group Policy objects (GPOs) for the site in this dialog box.

Creating Subnets

A site, by definition, is a grouping of TCP/IP subnets. Before you created an additional site, you never really had to think about subnets, because when only the default site exists, Windows 2000 assumes that if no subnets are specified, all existing subnets belong to the default site.

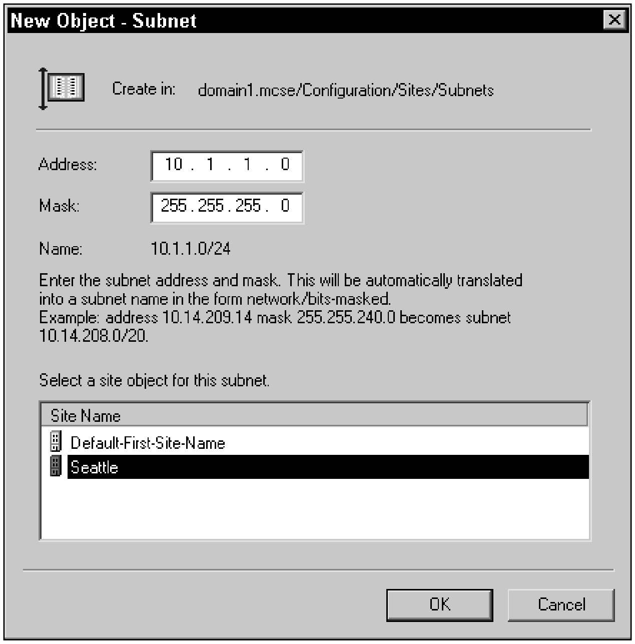
However, now that you've created one or more additional sites, you must specify the TCP/IP subnets that belong to each site. Until subnet objects are created and assigned to a site, the site has no definition and no functionality — it's just an empty Active Directory object.

You can create and manage subnets, like sites, by using Active Directory Sites and Services.

STEP BY STEP

CREATING AND ASSIGNING SUBNETS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Then right-click the Subnets container, and select New Subnet from the menu that appears.
3. The New Object – Subnet dialog box appears. In the Address text box, type in the IP address of the subnet. In the Mask text box, type in the subnet mask for the subnet. Then, highlight the site to which you want to assign this subnet from the list in the lower portion of the dialog box. Figure 22-3 shows this dialog box after it has been configured. Click OK.
4. The subnet is created and assigned. Close Active Directory Sites and Services.



New Object - Subnet

Create in: domain1.mcse/Configuration/Sites/Subnets

Address: 10 . 1 . 1 . 0

Mask: 255 . 255 . 255 . 0

Name: 10.1.1.0/24

Enter the subnet address and mask. This will be automatically translated into a subnet name in the form network/bits-masked.
Example: address 10.14.209.14 mask 255.255.240.0 becomes subnet 10.14.208.0/20.

Select a site object for this subnet.

Site Name
Default-First-Site-Name
Seattle

FIGURE 22-3 Creating a new subnet object in Active Directory

Creating Site Links

A *site link* is an object in Active Directory that specifies a list of two or more sites that are connected to each other, the cost associated with the site link, and a replication schedule. The KCC uses site link information to determine the path over which replication between sites will occur. Site links can be configured to use either IP or SMTP for intersite replication.

Normally, an administrator assigns a low cost to a site link that is associated with two sites when those two sites are connected by a high-speed WAN link. Conversely, the administrator assigns a high cost to a site link when two sites are connected by a low-speed WAN link.

You may remember that when you created your first additional site that you had to select a site link object for that site. The only site link object you could choose was a site link named DEFAULTIPSITELINK. If your company has only two sites, using the default site link is all you need to do.

If you have more than two sites, you should manually create a site link for each pair of sites that are connected to each other. Normally, an administrator creates a site link for each WAN link used by the company's network. Because of this practice, a site link is usually associated with exactly two sites. Figure 22-4 shows two common configurations of site links.

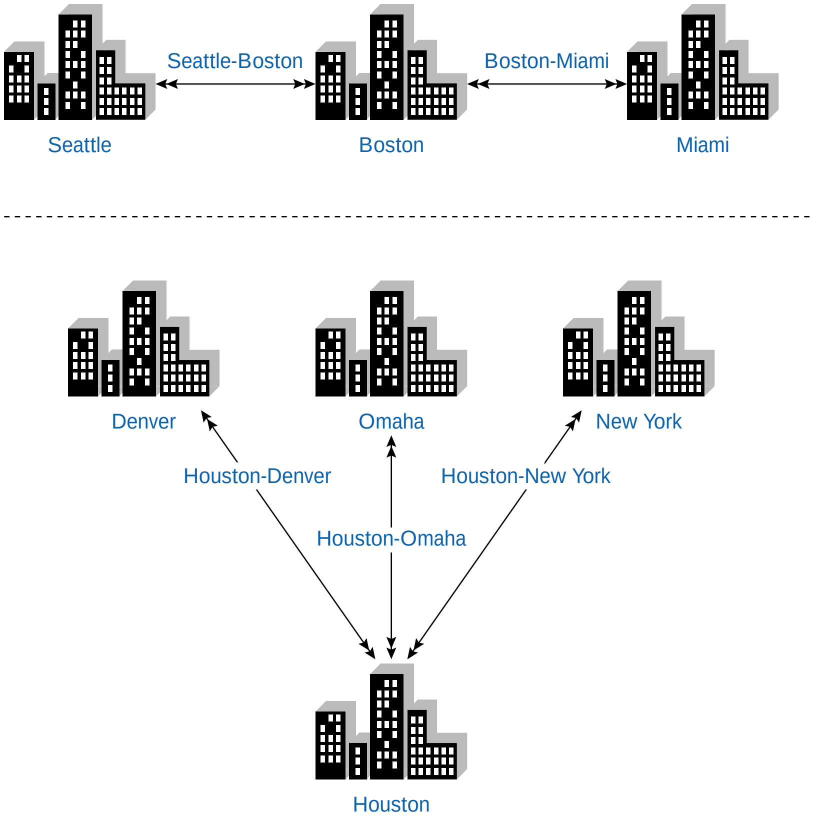


FIGURE 22-4 Common site link configurations

However, it's possible to create a site link that is associated with more than two sites. In this situation, the site link implies that each site associated with the site link has a WAN link connection to every other site associated with the site link. This configuration also implies that the WAN links are of the same speed and cost. Figure 22-5 shows one site link that is associated with three sites. Note that there are three WAN links involved, and that each WAN link has the same speed.

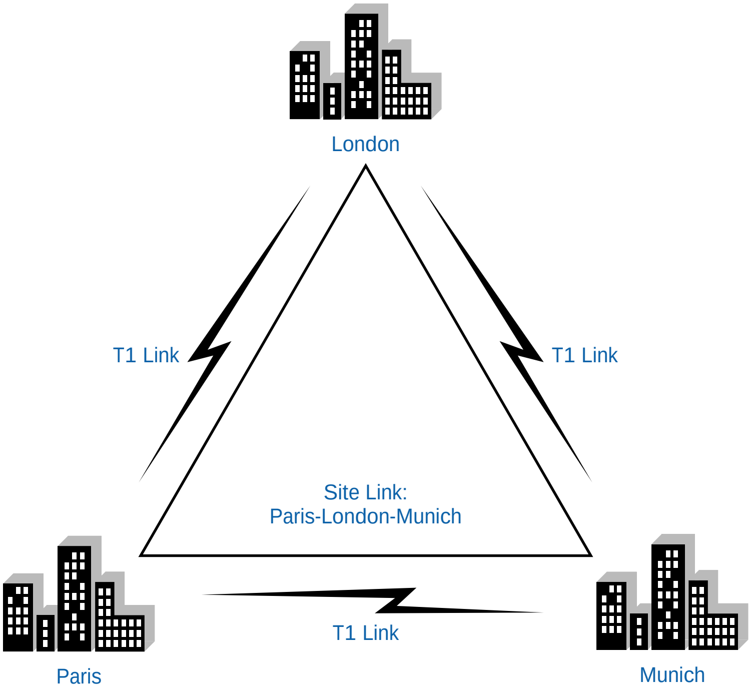


FIGURE 22-5 Using a single site link for three sites

Site links can be configured to use either IP or SMTP for intersite replication.

CAUTION

You should decide which protocol you want to use for intersite replication *before* you create a site link—you can't change a site link's protocol after it is created.

Site links, like other site components, are created and managed by using Active Directory sites and services.

STEP BY STEP

CREATING AND CONFIGURING SITE LINKS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the Inter-Site Transports container. Then right-click either the IP or SMTP container, depending on which protocol you want the site link to use.

STEP BY STEP ***Continued***

TIP

When you select the IP container, you're actually selecting the RPC over IP protocol.

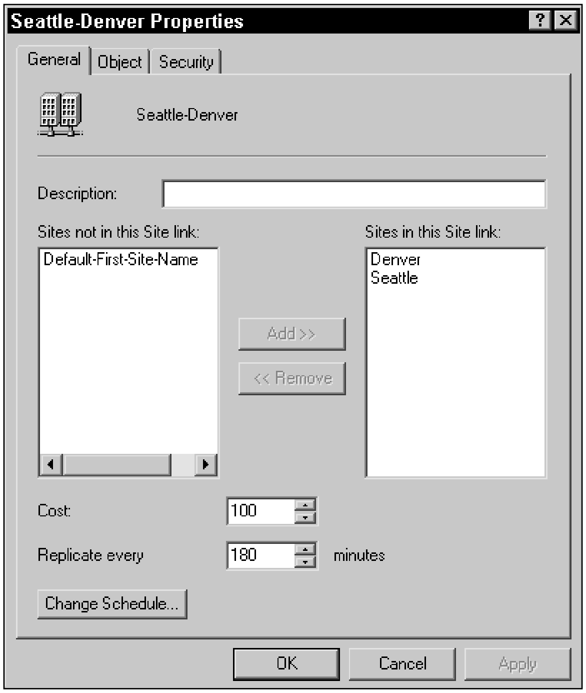
Select New Site Link from the menu that appears.

3. In the New Object – Site Link dialog box, type in a name for the site link. Site links are often named for the sites with which they are associated. For example, a site link associated with sites located in Seattle and Denver might be called Seattle-Denver.

   Next, in the "Sites not in this site link" list box, highlight the sites you want to associate with this site link. Click Add to move these sites to the "Sites in this site link" list box. A site link *must* contain at least two sites. Click OK.

4. The site link is created. In the left pane of the AD Sites and Services dialog box, highlight either the IP or SMTP container, depending on which container you created your site link in. Then, in the right-pane, double-click the site link you just created.

5. The site link's Properties dialog box appears, as shown in Figure 22-6.



Seattle-Denver Properties

Seattle-Denver

Description:

Sites not in this Site link:
Default-First-Site-Name

Sites in this Site link:
Denver
Seattle

Cost: 100

Replicate every 180 minutes

FIGURE 22-6 Configuring a site link

STEP BY STEP *Continued*

On the General tab, you can enter a description for the site link. You can also add and remove sites from the site link.

You can also assign a higher or lower cost to the site link. The default cost associated with a new site link is 100. The range for this setting is 1 – 32,767.

You can change the replication interval, which is 180 minutes (3 hours), by default. This setting must be changed in 15 minute increments.

Finally, you can schedule when intersite replication can and can't occur by clicking Change Schedule and configuring a replication schedule. (This dialog box looks and works just like the dialog box used to set a user's logon hours.)

Make any needed configurations on the General tab. You can view the object's properties by clicking the Object tab, and you can set Active Directory permissions for the site link object by clicking the Security tab.

When you finish configuring the site link, click OK.

6. Close Active Directory Sites and Services.

Creating Site Link Bridges

A *site link bridge* is an Active Directory object that groups two or more site links in order to create a "virtual site link" between all of the sites specified by the grouped site links. The purpose of a site link bridge is to enable replication between sites that use site links but that are *not* directly associated with each other via site links.

Here's an example of how a site link bridge might work. Suppose that you have three sites: Site A, Site B, and Site C. You use two site links, Site_Link A-B, and Site_Link B-C. However, sites A and C are not directly associated by a site link. Figure 22-7 shows this site link configuration.

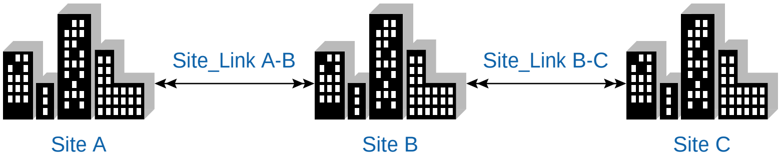


FIGURE 22-7 Site links between Site A, Site B, and Site C

You can create a site link bridge that specifies Site_Link A-B and Site_Link B-C. This site link bridge would enable Site A to replicate data to Site C by using Site_Link A-B and Site_Link B-C.

So why would you ever want to use a site link bridge? Well, the fact of the matter is that in the large majority of cases, you would never want to use a site link bridge, because by default, *all site links are bridged*. This means that replication takes place between all sites, by default, even if a specific pair of sites is *not* directly associated by the use of site links. So, going back to my earlier example, this means replication will occur between Site A and Site C even if I never configure the site link bridge.

So why am I even talking about site link bridges? Well, for one reason, because they're tested on the Directory Services exam. And because an administrator of an extremely large, complex network might someday want to disable Active Directory's automatic bridging feature and manually configure site link bridges so he or she can finely control how intersite replication occurs.

Before you create a site link bridge, you should disable Active Directory's feature that automatically bridges all site links. Then, after you create site link bridges, you should be prepared to maintain and update your site link bridges every time you add or remove a site or a site link.

Site link bridges, like other site components, are created and managed by using Active Directory sites and services.

STEP BY STEP

CREATING A SITE LINK BRIDGE

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the Inter-Site Transports container. Then right-click either the IP or SMTP container, depending on the protocol for which you want to disable the automatic site link bridging feature. Select Properties from the menu that appears.

TIP

When you disable automatic site link bridging, it is disabled for *all* site links that use the selected protocol, either IP or SMTP.

3. In the IP (or SMTP) Properties dialog box, clear the check box next to "Bridge all site links." Click OK.
4. In the left pane, right-click the IP or SMTP container, depending on the protocol for which you want to create a site link bridge. Select New Site Link Bridge from the menu that appears.

STEP BY STEP *Continued*

5. In the New Object – Site Link Bridge dialog box, enter a name for the site link bridge in the Name text box. Then, in the "Site links not in this site link bridge" list box, highlight the site links that you want to associate with this site link bridge. Click Add to cause these site links to be moved to the "Site links in this site link bridge" list box. Click OK.
6. The site link bridge is created. Close Active Directory Sites and Services.

Creating Global Catalog Servers

A *global catalog server* is a Windows 2000 domain controller that has an additional duty — it maintains the global catalog. You may recall that the global catalog is a master, searchable database that contains information about every object in every domain in a forest. The global catalog contains a complete replica of all objects in Active Directory for its host domain, and, in addition, contains a partial replica of all objects in Active Directory for every other domain in the forest.

A global catalog server performs two important functions: It provides group membership information during logon and authentication, and it helps users locate resources in Active Directory.

By default, the first domain controller established in a domain serves as the global catalog server. And, by default, there is only one global catalog server in each domain. For small domains that are fully contained within a single site, this is a good idea, but on multisite networks you might choose to have one or more global catalog servers in each site. In a multisite network, because global catalog servers are used for logon and authentication, and because users commonly search the global catalog to locate objects, it's often beneficial to have these services performed by a nearby server, rather than by a server located on the other side of a slow WAN link.

When multiple global catalog servers are used in a *single* domain, only the normal replication between domain controllers occurs — no additional replication within the domain occurs. When multiple global catalog servers are used in a *multiple* domain environment, additional replication between the domains occurs, because each global catalog server maintains a partial replica of all Active Directory objects for every other domain in the forest, in addition to a full replica of all Active Directory objects in its own domain.

You can establish additional global catalog servers by using Active Directory Sites and Services.

STEP BY STEP

CREATING AN ADDITIONAL GLOBAL CATALOG SERVER

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the site that contains the domain controller which you want to configure as an additional global catalog server. Click the + next to the Servers container. Click the + next to the specific server you want to configure. Right-click NTDS Settings, and select Properties from the menu that appears.
3. In the NTDS Settings Properties dialog box, select the check box next to Global Catalog. Click OK.
4. The server is now configured as a global catalog server. Close Active Directory Sites and Services.

Moving Server Objects Between Sites

When you first install Active Directory on the first domain controller on your Windows 2000 network, Active Directory automatically adds a server object for the domain controller to the Servers container in the default site. If you install additional domain controllers on your network before you create sites, server objects for these domain controllers are also added to the Servers container in the default site.

TIP

It's kind of confusing, but domain controllers actually have two objects in Active Directory. One object is stored in the Domain Controller's container within a domain, and the second is stored in the Servers container within a site.

When you later create sites, the server objects for the existing domain controllers will *not* automatically be moved to the Servers container in the appropriate site, even if the IP addresses of these domain controllers belong to a subnet that has been created and associated with one of the new sites.

An administrator must *manually* move the Active Directory server object for the existing domain controller to the appropriate site.

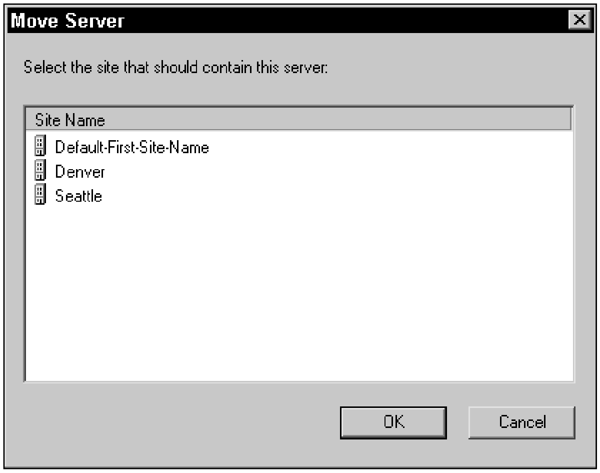
It's a different story, however, when new domain controllers are created *after* sites and subnets have been established. When a new domain controller is installed after sites are created, Active Directory automatically adds a server object for the new domain controller to the Servers container in the site to which its IP address belongs.

If you need to move the server objects for existing domain controllers to a different site, the following steps show you how to accomplish this task.

STEP BY STEP

MOVING SERVER OBJECTS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the site that contains the domain controller object you want to move. Click the + next to the Servers container. Right-click the server object you want to move, and select Move from the menu that appears.
3. The Move Server dialog box appears, as shown in Figure 22-8.



Move Server

Select the site that should contain this server:

Site Name
Default-First-Site-Name
Denver
Seattle

FIGURE 22-8 Moving a server object

Highlight the site to which you want to move the server object. Click OK.

4. The server is moved. Close Active Directory Sites and Services.

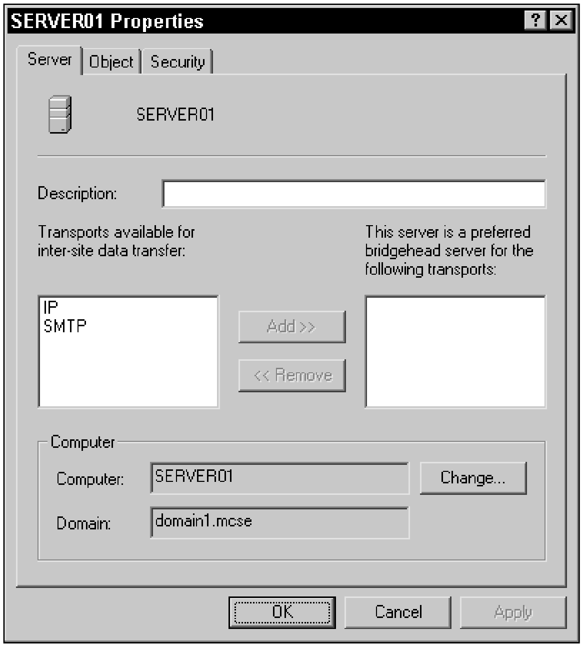
After you've moved servers into your new sites, you may want to specify a particular domain controller in each site that will be used for intersite replication. This domain controller is called the *bridgehead server*. The KCC automatically chooses a bridgehead server for each site, but you can manually override the KCC's choice.

When you designate a domain controller as a preferred bridgehead server, it's generally a good idea to specify the domain controller located closest to the router that connects the two sites.

STEP BY STEP

DESIGNATING A BRIDGEHEAD SERVER

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the site that contains the domain controller you want to designate as a bridgehead server for the site. Click the + next to the Servers container. Right-click the desired server, and select Properties from the menu that appears.
3. The server's Properties dialog box appears, as shown in Figure 22-9. Notice the "This server is a preferred bridgehead server for the following transports" list box.



SERVER01

Description:

Transports available for inter-site data transfer:
IP
SMTP

This server is a preferred bridgehead server for the following transports:

Computer: SERVER01

Domain: domain1.mcse

FIGURE 22-9 Specifying a bridgehead server

STEP BY STEP *Continued*

In the “Transports available for inter-site data transport” list box, highlight the protocol (or protocols) for which this server will function as a bridgehead server for this site. Click Add to move this protocol (or protocols) to the “This server is a preferred bridgehead server for the following transports” list box. Click OK.

4. Close Active Directory Sites and Services.

Managing and Maintaining Operations Master Roles

When Microsoft designed Windows 2000, its goal was to have every domain controller equal — instead of having a primary domain controller (PDC) and backup domain controllers (BDCs) like Windows NT 4.0 had, Microsoft wanted to have one class of domain controller that could perform every domain controller–related task.

However, when Microsoft implemented Active Directory, it discovered that a purely multimaster design just wasn’t going to work for Windows 2000. Although most domain controller–related tasks can be performed by any domain controller, a few critical tasks had to be limited to one domain controller in a domain, or to one domain controller in a forest. The result — a largely multimaster design, with some restricted single master operations. These operations are called flexible single master operations (FSMO). The term *flexible* refers to the fact that an administrator can choose which domain controller will perform the particular restricted single master operation.

There are five different types of flexible single master operations roles (often called *operations master roles*) that a domain controller can perform: *schema master*, *domain naming master*, *PDC emulator*, *relative ID master*, and *infrastructure master*. Each of these roles defines a specific set of flexible single master operations that only the domain controller assigned to that role can perform.

CROSS-REFERENCE

See the “Understanding Flexible Single Master Operations (FSMO)” section in Chapter 2 for detailed descriptions of each of the operations master roles.

When you first install Active Directory on the first domain controller in the forest, that domain controller automatically assumes all five of the operations master roles. As you add domain controllers, you can manually reassign or transfer these operations master roles to other domain controllers as needed.

In the following sections I'll explain how to transfer operations master roles and how to seize operations master roles.

Transferring Operations Master Roles

You should carefully consider which domain controllers on your network will perform each of the operations master roles. In general, when selecting a server that will perform an operations master role, the server should be located in a site that is central to your network. The goal here is that the server should be easily accessible from any computer on the network.

In addition, a domain controller that performs an operations master role should be highly reliable, because there's only one server that performs the specialized operations, and if it's not available, those operations can't be performed.

TIP

Microsoft recommends that the infrastructure master role be assigned to a domain controller that does *not* also function as a global catalog server. However, the infrastructure master should have a high-speed network connection to a global catalog server.

If you need to shut down a domain controller that performs an operations master role for maintenance, it's important that you transfer that server's role to another domain controller on the network so that network operations are not interrupted.

The tool you use to transfer an operations master role to another domain controller depends on the role you want to transfer. If you want to transfer the relative ID master, the PDC emulator, or the infrastructure master role, you can use Active Directory Users and Computers. If you want to transfer the schema master role you can use the Active Directory snap-in to the MMC. If you want to transfer the domain naming master role you can use Active Directory Domains and Trusts. Finally, you can transfer any operations master role by using the `ntdsutil.exe` command-line utility.

The first step in transferring an operations master role is connecting to the domain controller to which the role will be transferred. In the following section I'll show you how to transfer an operations master role by using Active Directory Users and Computers.

STEP BY STEP

TRANSFERRING OPERATIONS MASTER ROLES

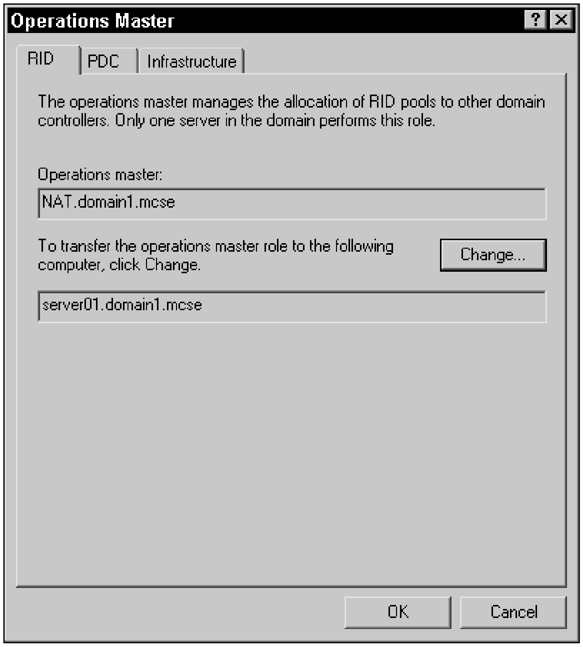
1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, right-click Active Directory Users and Computers (*server_name)* at the top of the tree, and select Connect to Domain Controller from the menu that appears.
3. In the Connect to Domain Controller dialog box, highlight the domain controller to which you want to transfer an operations master role, so that this server appears in the "Change to" text box. (This is *not* the computer that is currently performing the operations master role, but the computer to which you want to reassign the role.) Click OK.
4. In the left pane of the Active Directory Users and Computers dialog box, right-click the domain in which you want to transfer operations master roles, and select Operations Masters from the menu that appears.
5. The Operations Master dialog box appears, as shown in Figure 22-10. Notice the three tabs in this dialog box: RID, PDC, and Infrastructure.

   Click the tab associated with the type of operations master role you want to transfer.

   The "Operations master" list box displays the name of the server currently performing the selected role.

   To transfer the operations master role to the server displayed in the second list box, click Change.
6. In the Active Directory confirmation dialog box, click Yes to transfer the operations master role.
7. Active Directory displays a message indicating that the role was successfully transferred. Click OK.
8. In the Operations Master dialog box, click OK.
9. Close Active Directory Users and Computers.

STEP BY STEP *Continued*



Operations Master

The operations master manages the allocation of RID pools to other domain controllers. Only one server in the domain performs this role.

Operations master:

NAT.domain1.mcse

To transfer the operations master role to the following computer, click Change.

server01.domain1.mcse

FIGURE 22-10 Transferring an operations master role

Seizing Operations Master Roles

When a domain controller that performs an operations master role fails, and you decide (for whatever reason) to never bring this server back on-line, you should reassign the operations master role this domain controller performed to another domain controller. This process is called “seizing” operations master roles.

CAUTION

If you bring a domain controller that previously performed an operations master role back on-line after its role has been seized, serious Active Directory problems may result. Never seize a role unless you’re *sure* the server that failed will not be used again on your network.

Microsoft didn't go out of their way to make seizing an operations master role an easy task to perform—and this is probably a good thing. You can only perform this task by using the `ntdsutil.exe` command-line utility.

As with transferring an operations master role, the first step in the "seizing" process is to connect to the domain controller to which the role (that was performed by the failed server) will be assigned.

STEP BY STEP

SEIZING AN OPERATIONS MASTER ROLE

1. Select Start ➪ Programs ➪ Accessories ➪ Command Prompt.
2. At the command prompt, type **ntdsutil** and press Enter.
3. At the ntdsutil prompt, type **roles** and press Enter.
4. At the fsmo maintenance prompt, type **connections** and press Enter.
5. At the server connections prompt, type

   ```
   connect to server FQDN_of_server_you_want_to_connect_to
   ```

   and press Enter.
6. At the server connections prompt, type **quit** and press Enter.
7. At the fsmo maintenance prompt, type

   ```
   seize role_you_want_to_transfer
   ```

   and press Enter. For example, you could type **seize PDC**, **seize RID master**, **seize schema master**, **seize domain naming master**, or **seize infrastructure master**.

TIP

If you want to use the `ntdsutil.exe` command-line utility to transfer roles, instead of typing **seize** (and the name of the role), type **transfer** and the name of the role.

8. A Role Seizure Confirmation Dialog box appears. Click Yes to seize the role.
9. At the fsmo maintenance prompt, type **quit** and press Enter.
10. At the ntdsutil prompt, type **quit** and press Enter.
11. At the command prompt, type **Exit**.

Managing Active Directory Replication

Now that you understand what Active Directory replication is, and are familiar with the numerous Active Directory components that affect replication, you're ready to decide if you want to manually manage intrasite or intersite replication, or if Windows 2000's default configurations for replication will be adequate for your network.

You can manage both intrasite replication and intersite replication. However, there are substantially fewer things you can do to manage intrasite replication than intersite replication. You can use the Active Directory Sites and Services administrative tool to manage Active Directory replication.

In the next two sections I'll explain some of the ways you can manage intrasite and intersite replication.

Managing Intrasite Replication

Because intrasite replication is automatically configured and performed by Windows 2000, administrators don't normally need to do much to manage it. One task that is commonly performed, however, is to specify the schedule Active Directory will use for replication, thereby controlling when *scheduled* replication takes place.

TIP

You can configure when scheduled replication takes place, but you can't schedule update replication.

Here's how you can change when scheduled Active Directory intrasite replication occurs.

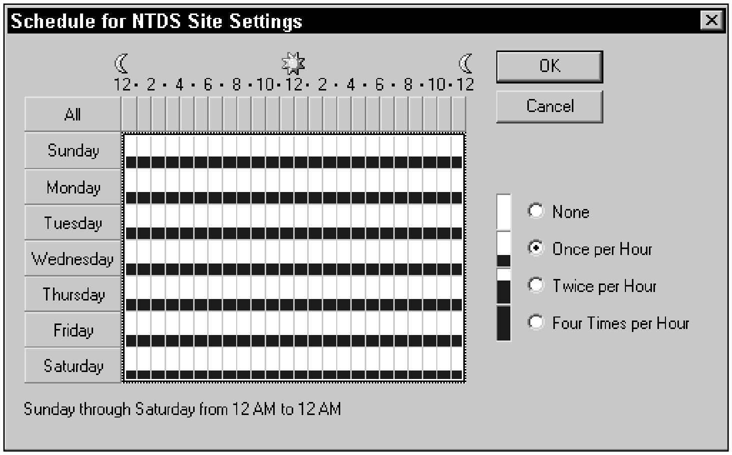
STEP BY STEP

CHANGING WHEN SCHEDULED REPLICATION OCCURS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Then highlight the site for which you want to configure the replication schedule. In the right pane, right-click NTDS Site Settings, and select Properties from the menu that appears.
3. In the NTDS Site Settings Properties dialog box, click Change Schedule.

STEP BY STEP *Continued*

4. The Schedule for NTDS Site Settings dialog box appears, as shown in Figure 22-11. Notice that, by default, replication is scheduled to occur once per hour, seven days a week, 24 hours a day.



○ None
● Once per Hour
○ Twice per Hour
○ Four Times per Hour

Sunday through Saturday from 12 AM to 12 AM

FIGURE 22-11 Scheduling replication

You can configure, for each hour of each day, whether scheduled replication will occur once per hour, twice per hour, four times per hour, or not at all. For example, maybe you don't want replication to occur during the hours you schedule for tape backup throughout the site. To make these configurations, highlight the hour(s) you want to configure, then select the appropriate option for that time period.

CAUTION

If you select the "None" option for all days and all hours, replication will not occur until you manually force it to do so. This is *not* a preferred practice.

When you finish configuring the replication schedule for the site, click OK.

5. In the NTDS Site Settings Properties dialog box, click OK.
6. Close Active Directory Sites and Services.

In addition to configuring the Active Directory replication schedule, you might want to manually configure the replication topology within a site. Every 15 minutes the KCC automatically generates the replication topology, and by doing so determines which domain controllers in a site will replicate with one another. The KCC does this by generating connections between pairs of domain controllers that it determines should replicate with one another. Normally, an administrator can just let the KCC do its job, because the default replication settings will work just fine.

It's possible, however, in some instances, that the administrator might want to manually specify replication partners. It's really a rare occasion when any administrator might do this in real life, but let me try to dream up a plausible scenario. Suppose that you want to ensure that Active Directory updates are replicated to all domain controllers in the site within five minutes, instead of the default 15 minutes. To accomplish this, you could modify the replication topology in such a way to ensure that updates from any domain controller need to pass through no more than one connection (hop) between domain controllers (instead of the normal three). To implement this change to the replication topology, you'd need to create connection objects between each domain controller and every other domain controller in the site.

Connection objects don't replace the KCC replication topology. Instead, connection objects are used in addition to the connections created by the KCC. The only exception to this rule is if you create a connection object for a connection automatically generated by the KCC—in this case, the KCC won't duplicate your efforts by replicating twice over the specified connection.

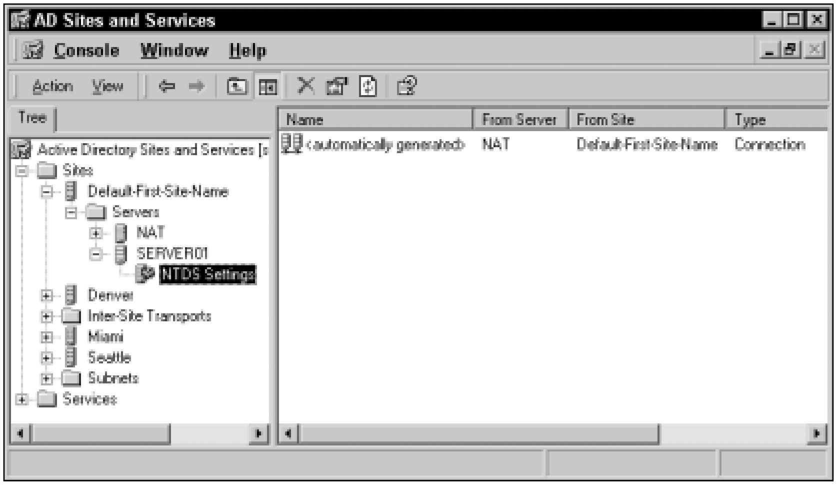
When creating connection objects, keep in mind that these connections specify a *one-way* communications path. In order for two domain controllers to replicate with each other, you need to create two connection objects—one on each server that points at the other server. You can create connection objects by using Active Directory Sites and Services.

STEP BY STEP

CREATING CONNECTION OBJECTS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Click the + next to the site that contains the domain controller for which you want to create a new connection. Click the + next to the Servers container. Click the + next to the desired server. Under the server, highlight NTDS Settings. The server's existing connections (both the connections automatically generated by the KCC and any manually created connections) are displayed in the right pane, as shown in Figure 22-12.

STEP BY STEP *Continued*



- Active Directory Sites and Services [s
  - Sites
    - Default-First-Site-Name
      - Servers
        - NAT
        - SERVER01
          - NTDS Settings
    - Denver
    - Inter-Site Transports
    - Miami
    - Seattle
    - Subnets
  - Services

Name	From Server	From Site	Type
<automatically generated>	NAT	Default-First-Site-Name	Connection

FIGURE 22-12 Viewing replication connections

Select Action ➪ New Active Directory Connection.

3. In the Find Domain Controllers dialog box, double-click the domain controller in the list to which you want the domain controller you selected in Step 2 to connect.
4. In the New Object – Connection dialog box, click OK.
5. After you've created a connection object, you can manually run the KCC to force an update of the replication topology. To do this, in the left pane of the AD Sites and Services dialog box, right-click NTDS Settings, and select All Tasks ➪ Check Replication Topology.
6. In the Check Replication Topology dialog box, click OK.
7. To update your view of the server's connections, in the AD Sites and Services dialog box, select Action ➪ Refresh. The server's current connections are displayed in the right pane.
8. Close Active Directory Sites and Services.

TIP

If you create a connection that duplicates an automatically generated connection, the next time the KCC runs it will delete the duplicate automatically generated connection.

Managing Intersite Replication

The most important aspect of managing intersite replication is the planning you do before you ever implement it. As you know, intersite replication is not automatically configured and performed by Windows 2000—an administrator must manually create and configure various Active Directory components before intersite replication will occur. I've told you about the components involved in intersite replication throughout this chapter so far, but before you rush right out and create them on your network, you need to have a plan.

There are several questions you should ask yourself when planning for intersite replication:

- How many sites do I really need, and what are their boundaries?
- Do I have enough domain controllers and global catalog servers to implement these sites, and to service the clients located in these sites?
- Which protocol should I use for intersite replication, RPC over IP or SMTP?
- Do I need to create site links, or can I use the default IP site link?
- If I need site links, how will I determine the cost to associate with each site link, so that each site link is used appropriately?
- If I need site links, do I also need to create site link bridges, or should I use Active Directory's automatic bridging feature?
- Do I need to designate bridgehead servers, or can any domain controller in the site perform this function?
- Are my operations master roles being performed by the appropriate domain controllers, or do I need to transfer some of these roles to other servers?

Once you've answered these questions, you should have the information you need to solidify your plan for intersite replication. From there, it's just a matter of mechanics, the creating and configuring of the components you will use on your network.

Managing Active Directory Performance

If you have a relatively small network and a lot of bandwidth, why bother managing Active Directory performance? After all, you probably don't need to, right? Wrong. What if you don't have enough domain controllers to service all of your client requests, or if your domain controllers don't have enough RAM or processor power to adequately perform their duties? You do have at least two domain controllers, in case one fails, don't you?

Performance is a common network concern. And it can be a critical issue on large networks, especially on those that are connected by slow WAN links.

Managing Active Directory performance is generally a two-step process. First, you monitor performance of domain controllers and other Active Directory components to determine if there is currently a performance problem, and, if so, to isolate where that problem is occurring. Second, you use this data to help you optimize the performance of Active Directory.

There are several tools you can use to help you manage and monitor Active Directory performance. In addition to the Active Directory management tools you're already familiar with (Active Directory Users and Computers, Active Directory Sites and Services, and Active Directory Domains and Trusts), you can also use System Monitor and Active Directory Replication Monitor to monitor Active Directory performance.

In the next two sections I'll explain how to use these tools to monitor and optimize the performance of Active Directory.

Monitoring Performance of Domain Controllers and Other Active Directory Components

Because all of the Active Directory components I've discussed in this chapter (such as sites, subnets, site links, site link bridges, global catalog servers, and so on) are found on Windows 2000 domain controllers, one approach to monitoring these objects is to monitor the domain controllers themselves. You might also want to monitor Active Directory replication itself.

There are two primary tools you can use to monitor these items. You can use System Monitor to monitor performance of domain controllers and replication. You can also use Active Directory Replication Monitor to monitor replication.

System Monitor counters that you might find helpful for monitoring performance of domain controllers include:

- Memory - Pages/sec
- Network Interface - Bytes Total/sec
- Processor - % Processor Time
- PhysicalDisk - Avg. Disk Queue Length

These counters will help you determine if the system resources, such as memory, disk, processor, and network, are sufficient for the domain controller. In addition, domain controllers have an additional object in System Monitor that is useful for monitoring domain controller operations and replication. The object is named NTDS, and it has numerous counters. A couple of counters that are particularly useful for monitoring replication are:

- NTDS - DRA Outbound Bytes Total/sec
- NTDS - DRA Inbound Bytes Total/sec

These counters measure the amount of replication traffic sent and received by the domain controller. If you want to monitor only intrasite traffic, use counters that measure uncompressed traffic only. To monitor only intersite traffic, use counters that measure compressed traffic only.

CROSS-REFERENCE

Details on how to use System Monitor are presented in Chapter 21.

Active Directory Replication Monitor is a Windows 2000 Server tool specifically designed to monitor Active Directory replication. With Active Directory Replication Monitor you can monitor replication on specific domain controllers, view the replication topology (connections) on a server-by-server basis, view replication statistics for each replication partition on each domain controller, and so on. You can also manually force replication of a partition (or of all partitions on a domain controller) to occur by using this tool.

Active Directory Replication Monitor is not installed by default. You can install Active Directory Replication Monitor by installing the Windows 2000 Support Tools from the Windows 2000 Server compact disc.

STEP BY STEP

INSTALLING ACTIVE DIRECTORY REPLICATION MONITOR

1. Insert your Windows 2000 server compact disc into your computer's CD-ROM drive. When the Microsoft Windows 2000 CD dialog box appears, click Browse This CD.
2. In the right pane, double-click the `SUPPORT` folder. Double-click the `TOOLS` folder. Double-click `SETUP`.
3. The Windows 2000 Support Tools Setup wizard starts. Click Next.
4. In the User Information screen, type your name and organization. Click Next.
5. In the Select An Installation Type screen, select the Typical option. Click Next.
6. In the Begin Installation screen, click Next.
7. Windows 2000 installs the Support Tools. In the Completing the Windows 2000 Support Tools Setup Wizard screen, click Finish.
8. Close the TOOLS dialog box. Close the Microsoft Windows 2000 CD dialog box.

Now that you've installed the Windows 2000 Support Tools, you can use Active Directory Replication Monitor.

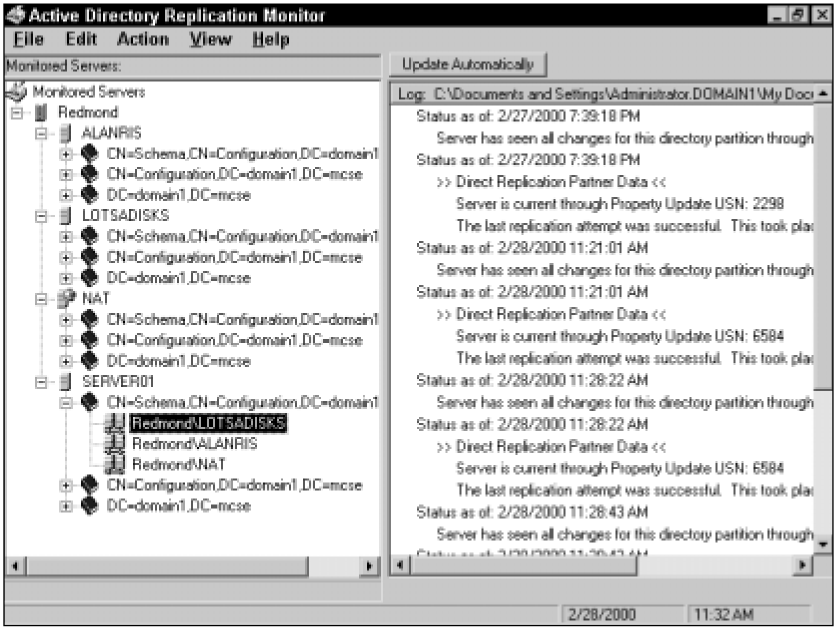
STEP BY STEP

USING ACTIVE DIRECTORY REPLICATION MONITOR

1. Select Start ➪ Run.
2. In the Run dialog box, type **replmon** and click OK.
3. The Active Directory Replication Monitor dialog box appears. Select Edit ➪ Add Monitored Server.
4. The Add Monitored Server wizard starts. Select the "Search the directory for the server to add" option. Then select the domain in which you want to monitor replication from the drop-down list box. Click Next.
5. In the Add Server to Monitor dialog box, click the + next to the site that contains the domain controller you want to monitor. Highlight the domain controller you want to monitor. Click Finish.

STEP BY STEP *Continued*

6. Repeat Steps 3 through 5 until you've added all of the domain controllers you want to monitor. Figure 22-13 shows Active Directory Replication Monitor after four servers have been added. Notice that for each server the three replication partitions are displayed: schema, configuration, and domain. Also notice that when you expand a replication partition, a list of domain controllers to which that partition is replicated is displayed.



```
Monitored Servers
  Redmond
    ALANRIS
      CN=Schema,CN=Configuration,DC=domain1
      CN=Configuration,DC=domain1,DC=mcse
      DC=domain1,DC=mcse
    LOTSADISKS
      CN=Schema,CN=Configuration,DC=domain1
      CN=Configuration,DC=domain1,DC=mcse
      DC=domain1,DC=mcse
    NAT
      CN=Schema,CN=Configuration,DC=domain1
      CN=Configuration,DC=domain1,DC=mcse
      DC=domain1,DC=mcse
    SERVER01
      CN=Schema,CN=Configuration,DC=domain1
        Redmond\LOTSADISKS
        Redmond\ALANRIS
        Redmond\NAT
      CN=Configuration,DC=domain1,DC=mcse
      DC=domain1,DC=mcse
```

```
Log:  C:\Documents and Settings\Administrator.DOMAIN1\My Docu
  Status as of: 2/27/2000 7:39:18 PM
    Server has seen all changes for this directory partition through
  Status as of: 2/27/2000 7:39:18 PM
    >> Direct Replication Partner Data <<
      Server is current through Property Update USN: 2298
      The last replication attempt was successful.  This took plac
  Status as of: 2/28/2000 11:21:01 AM
    Server has seen all changes for this directory partition through
  Status as of: 2/28/2000 11:21:01 AM
    >> Direct Replication Partner Data <<
      Server is current through Property Update USN: 6584
      The last replication attempt was successful.  This took plac
  Status as of: 2/28/2000 11:28:22 AM
    Server has seen all changes for this directory partition through
  Status as of: 2/28/2000 11:28:22 AM
    >> Direct Replication Partner Data <<
      Server is current through Property Update USN: 6584
      The last replication attempt was successful.  This took plac
  Status as of: 2/28/2000 11:28:43 AM
    Server has seen all changes for this directory partition through
```

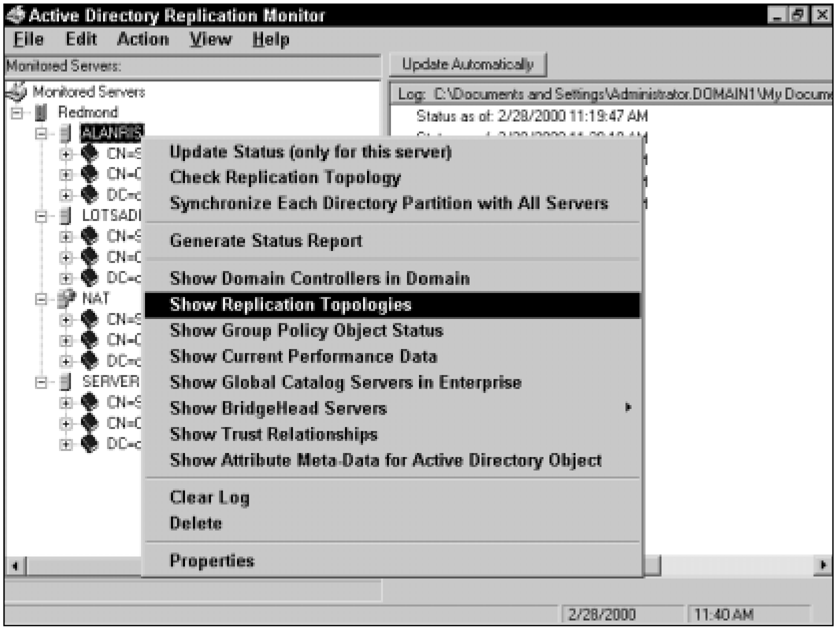
FIGURE 22-13 Monitoring replication partitions and servers

Also notice that when a server is highlighted in the left pane, replication statistics for that server are displayed in the right pane. Finally, notice the globe on the server named NAT. This globe indicates that this server is a global catalog server.

7. To manually force replication to occur on any of the partitions displayed, right-click the partition, and select Synchronize This Directory Partition with All Servers from the menu that appears.
8. In the Synchronizing Naming Context with Replication Partners dialog box, click OK.
9. In the Replication Monitor confirmation dialog box, click Yes to force replication to occur. When notified that the synchronization completed successfully, click OK.

STEP BY STEP *Continued*

10. To view the replication connections (which this tool calls replication topology) for a domain controller, right-click the domain controller, then select Show Replication Topologies from the menu that appears. Figure 22-14 shows selecting this option. Notice all of the tasks you can perform and information you can view for each server by using this tool.
11. In the View Replication Topology dialog box, select View ➪ Connection Objects Only.
12. A graphical representation of the domain controllers you are monitoring is displayed. Right-click any domain controller displayed, and select Show Intra-Site Connections.


Active Directory Replication Monitor
File
Edit
Action
View
Help
Monitored Servers:
Update Automatically
Monitored Servers
Redmond
ALANRIS
CN=S
CN=C
DC=c
LOTSADI
CN=S
CN=C
DC=c
NAT
CN=S
CN=C
DC=c
SERVER
CN=S
CN=C
DC=c
Update Status (only for this server)
Check Replication Topology
Synchronize Each Directory Partition with All Servers
Generate Status Report
Show Domain Controllers in Domain
Show Replication Topologies
Show Group Policy Object Status
Show Current Performance Data
Show Global Catalog Servers in Enterprise
Show BridgeHead Servers
Show Trust Relationships
Show Attribute Meta-Data for Active Directory Object
Clear Log
Delete
Properties
2/28/2000
11:40 AM

Log: C:\Documents and Settings\Administrator.DOMAIN1\My Docum

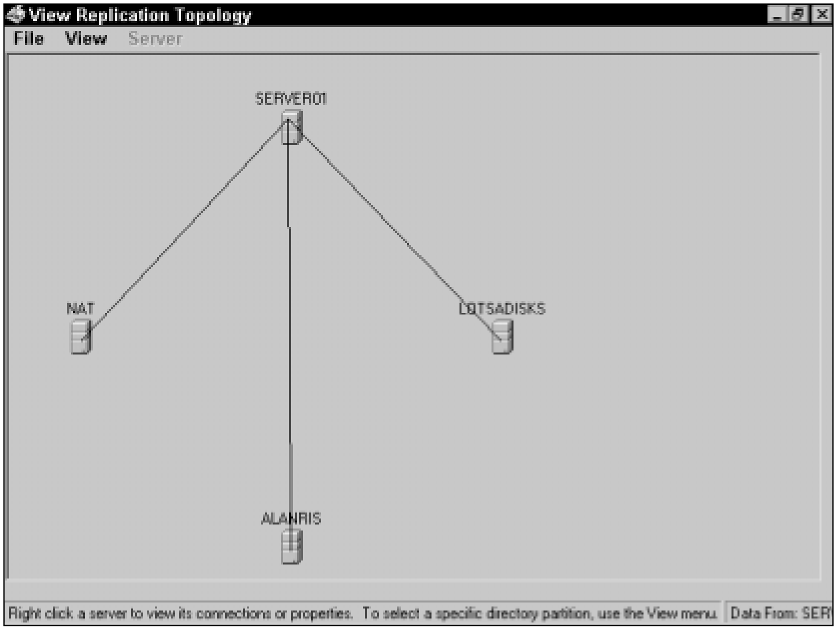
Status as of: 2/28/2000 11:19:47 AM

FIGURE 22-14 Selecting replication menu items

13. Active Directory Replication Monitor displays the connections from the selected domain controller to all other monitored servers in the site to which the domain controller has connections. Figure 22-15 shows the intrasite connections from SERVER01 to three other domain controllers in the site.

    Close the View Replication Topology dialog box.
14. Close Active Directory Replication Monitor.

STEP BY STEP *Continued*



Right click a server to view its connections or properties. To select a specific directory partition, use the View menu. Data From: SER

FIGURE 22-15 Viewing a graphical representation of a server's replication connections

Optimizing Active Directory Performance

Once you've monitored the performance of domain controllers and Active Directory replication on your network, you'll probably know if you have any Active Directory performance problems. If monitoring doesn't indicate any problems, and replication is working correctly (and not excessively impacting other network traffic), you probably have a system that doesn't require further optimization. If you do have some performance problems, however, at least now you probably have a good idea where the problems are.

If performance problems are indicated, here are a few things you might choose to do to optimize Active Directory performance:

- If monitoring indicates a hardware bottleneck on one or more domain controllers (such as memory, disk, or processor), consider upgrading the servers' hardware or replacing the server with a more powerful computer.
- If users at a remote location (that does not have a domain controller) report slow authentication and other Active Directory operations, consider creating a site for the remote location and placing one or more domain controllers, a DNS server, and a global catalog server at the remote site.
- If users within a site report slow authentication and other Active Directory operations, consider adding one or more domain controllers to the site.
- If replication is consuming excessive amounts of network bandwidth, either within a site or between sites, considering scheduling replication to occur less frequently during peak usage hours.
- If you become aware that an inappropriate domain controller is being used for intersite replication, consider designating a more appropriate domain controller as the bridgehead server for that site.

Troubleshooting Active Directory Components, Replication, and Performance

Active Directory is the most complex feature of Windows 2000. Because of this, troubleshooting Active Directory components, replication, and domain controller performance can be a detailed, painstaking task. Sometimes the problem is readily apparent — like when a user can't log on to the domain. Other times, the problem is less apparent, but still an issue. And sometimes a problem will even resolve itself, given a little time.

It's impossible to list all of the Active Directory problems you might encounter on your network, but in Table 22-1 I've listed a few of the problems you're most likely to encounter, along with some recommended solutions for solving these problems.

TABLE 22-1 Active Directory Problems and Solutions

Problem	Possible Cause/Recommended Solution
A user in your Los Angeles site reports that he can't log on using his new user account. You created the user's account 10 minutes ago in your New York site.	The most likely cause of this problem is that the user's account information has not yet been replicated to the Los Angeles site. Either wait for replication to occur, or force replication to occur immediately by using either Active Directory Sites and Services or Active Directory Replication Monitor.
You recently created additional sites, and created subnets for these sites. However, users in the new sites are being authenticated by domain controllers in the original site. In addition, uncompressed replication traffic is being sent across a WAN link between sites.	The most likely cause of this problem is that existing server objects have not been moved to the new sites. Move the server objects for the domain controllers that are physically located in the new sites to the appropriate site by using Active Directory Sites and Services.
Monitoring indicates that processor utilization on one of your domain controllers (that is also a global catalog server, a DNS server, a DHCP server, and a WINS server) is consistently over 70 percent. Users report slow response time from this server.	The possible causes of this problem are: the server doesn't have enough RAM, or a fast enough processor; or the server is overloaded, or both. Possible solutions include: upgrading the server's hardware or replacing the server with a more powerful computer. Or, consider transferring some of the services currently provided by this domain controller to another domain controller or server.
Users in one large site report slow logon authentication and long computer boot times.	The most likely cause of this problem is that the domain controllers in the site are overburdened by client requests. Add one or more additional domain controllers to this site.
You recently disabled automatic bridging and created a site link bridge. However, one of your sites is not receiving all replication updates from the other sites.	The most likely cause of this problem is that the site link to the site not receiving the replication updates is not specified in the site link bridge. Reconfigure the site link bridge to include the site link to the affected site, or create an additional site link bridge, depending on your network and site configuration.
You are unable to create a new domain in the forest after the failure of one your domain controllers.	The most likely cause of this problem is that the failed domain controller performed the domain naming master role. Either bring the failed domain controller back on line, or have another domain controller seize the domain naming master role.

KEY POINT SUMMARY

This chapter introduced several important Windows 2000 Active Directory replication and performance topics:

- There are three replication partitions in Active Directory: the schema partition, the configuration partition, and the domain partition.
- Intrasite replication is Active Directory replication that takes place within a single site. Windows 2000 automatically configures and performs intrasite replication.
- Intersite replication is Active Directory replication between sites. Unlike intrasite replication, intersite replication is not automatically configured and performed by Windows 2000, but must be manually configured by an Administrator.
- There are numerous Active Directory components that affect replication, including sites, subnets, site links, and site link bridges. You can create and manage all of these components by using Active Directory Sites and Services.
- There are five operations master roles: schema master, domain naming master, PDC emulator, relative ID master, and infrastructure master. You can manually transfer these roles to different domain controllers if necessary.
- You can manage intrasite replication by configuring when scheduled replication will occur. You can also create connection objects to manually specify replication partners if needed.
- It’s important to have a comprehensive plan in place before you implement intersite replication.
- There are two primary tools you can use to monitor the performance of Active Directory objects: System Monitor and Active Directory Replication Monitor.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about managing, optimizing, and troubleshooting Active Directory replication and performance. These exercises will also help you prepare for the Directory Services exam:

- **Assessment Questions:** These questions test your knowledge of the Active Directory replication and performance topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenarios, you are asked to evaluate several replication and performance-related situations, and to answer the questions that follow each scenario. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab Exercise:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice creating various Active Directory components.

Assessment Questions

1. You want to create additional sites to manage replication on your Windows 2000 network. What tool should you use to create the sites?

   A. Active Directory Users and Computers

   B. Active Directory Domains and Trusts

   C. Active Directory Sites and Services

   D. Active Directory Replication Monitor

2. You recently created two additional sites on your Windows 2000 network, and created and assigned subnets to those sites. You had 20 existing domain controllers before you created the new sites. Eight of these domain controllers will be used in the two new sites. What should you do to ensure that intersite replication occurs?

A. Move the server objects for the eight domain controllers to their new sites.

B. Add new objects to the Domain Controllers container for each of the eight domain controllers.

C. Change the IP addresses of each of the eight domain controllers so the IP addresses are within the range of IP addresses used by subnets in the new sites.

D. Nothing—Active Directory will automatically move the server objects for the eight domain controllers to their new sites.

3. You decide to add a global catalog server to your site. What tool should you use to cause a domain controller to function as a global catalog server?

   A. Active Directory Users and Computers

   B. Active Directory Sites and Services

   C. `Network and Dial-up Connections` folder

   D. The System application

4. You decide to transfer the infrastructure master role to a different domain controller. There are five domain controllers in the domain. To what domain controller should you *not* transfer the infrastructure master role?

   A. The domain controller that is also the schema master

   B. The domain controller that is located physically close to a router

   C. The domain controller located in the same site as your senior network administrator

   D. The domain controller that also is a global catalog server

5. What is the *minimum* number of sites you must have before you can create a site link bridge?

   A. 1

   B. 2

   C. 3

   D. 4

6. You have fully routed TCP/IP connections between the three sites on your Windows 2000 network. You want to accomplish replication as quickly as possible between these sites. Which protocol should you use for intersite replication?

A. RPC over IP

B. SMTP

C. DHCP Relay Agent

D. RIP Version 2 for Internet Protocol

7. You use two sites on your Windows 2000 network. You decide you want to manually specify a particular domain controller in each site that will be used for intersite replication. What should you do?

   A. Create a site link to connect the two domain controllers.

   B. Designate the desired domain controller in each site as a bridgehead server.

   C. Configure the desired domain controller in each site to be a global catalog server.

   D. Create a new connection object for the desired domain controller in each site.

8. You want to view a graphic representation of the replication topology connections on a specific domain controller. What tool should you use to do this?

   A. Active Directory Users and Computers

   B. Active Directory Sites and Services

   C. Active Directory Replication Monitor

   D. `Network and Dial-up Connections` folder

Scenarios

Managing Active Directory components and replication on your network can be an extremely complex task. For each of the following situations, consider the given facts and answer the question or questions that follow.

1. Users in your large, rapidly expanding site report that searches of Active Directory are becoming slower. What can you do to speed up Active Directory search response time for users?

2. You recently created sites and subnets on your Windows 2000 network. Your company's existing domain controllers will be used in the new sites. What should you do next?

3. You determine that the domain controller performing the infrastructure master role is also a global catalog server. There are 25 domain controllers in the domain. What should you do about this situation, if anything?
4. You recently disabled automatic bridging on your Windows 2000 network and created a site link bridge. Now, all of the domain controllers in a remote site are not receiving all replication updates from other sites.
   a. What is the most likely cause of this problem?
   b. What should you do to resolve the problem?
5. Your company's Seattle site is experiencing rapid growth. Monitoring indicates that utilization of the domain controllers in your Seattle site is increasing as well. What should you do to manage and maintain Active Directory performance as the site continues to grow?
6. Monitoring indicates that processor utilization on one of your company's domain controllers is consistently over 70 percent. This domain controller is also a global catalog server, a DNS server, a DHCP server, and a RIS server. Users are reporting slow response time from this domain controller.
   a. What is the most likely cause of this problem?
   b. What should you do to resolve the problem?
7. You recently created sites and subnets for the new sites. However, when you use System Monitor, you determine that uncompressed replication traffic is still being sent over your WAN links.
   a. What is the most likely cause of this replication problem?
   b. What should you do to resolve the problem?
8. You use Active Directory Replication Monitor to determine that the domain controller in one of your sites that is being used for intersite replication is physically located several subnets away from the router that connects this site to other sites. What should you do to better manage intersite replication?
9. Your company' network has five domain controllers in a single location. You don't use sites. You want to ensure that Active Directory updates are replicated to all five domain controllers as quickly as possible. What should you do to achieve maximum speed of intrasite replication?

Lab Exercise

Lab 22-1 Managing Active Directory Components that Affect Replication

► Directory Services

The purpose of this lab is to provide you with an opportunity to create and configure several Active Directory components that affect replication. First you rename the default site, then you create and configure sites, subnets, site links, and a site link bridge.

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

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.
2. In the left pane of the AD Sites and Services dialog box, click the + next to the Sites container. Right-click the Default-First-Site-Name site, and select Rename from the menu that appears. Type in a new site name of **Seattle** and press Enter.
3. In the left pane of the AD Sites and Services dialog box, right-click the Sites container, and select New Site from the menu that appears.
4. In the New Object – Site dialog box, enter a name of **Denver**. Then highlight a site link object of DEFAULTIPSITELINK. Click OK.
5. Active Directory confirms that the site has been created. Click OK.
6. In the left pane of the AD Sites and Services dialog box, right-click the Sites container, and select New Site from the menu that appears.
7. In the New Object – Site dialog box, enter a name of **Houston**. Then highlight a site link object of DEFAULTIPSITELINK. Click OK.
8. Active Directory confirms that the site has been created. Click OK.
9. In the left pane of the AD Sites and Services dialog box, right-click the Subnets container, and select New Subnet from the menu that appears.

10. The New Object – Subnet dialog box appears. In the Address text box, type **192.168.0.0**. In the Mask text box, type **255.255.255.0**. Then, highlight the Seattle site in the Site Name list box. Click OK.
11. In the left pane of the AD Sites and Services dialog box, right-click the Subnets container, and select New Subnet from the menu that appears.
12. The New Object – Subnet dialog box appears. In the Address text box, type **192.168.101.0**. In the Mask text box, type **255.255.255.0**. Then, highlight the Denver site in the Site Name list box. Click OK.
13. In the left pane of the AD Sites and Services dialog box, right-click the Subnets container, and select New Subnet from the menu that appears.
14. The New Object – Subnet dialog box appears. In the Address text box, type **10.1.1.0**. In the Mask text box, type **255.255.255.0**. Then, highlight the Houston site in the Site Name list box. Click OK.
15. In the left pane of the AD Sites and Services dialog box, click the + next to the Inter-Site Transports container. Then right-click the IP container, and select New Site Link from the menu that appears.
16. In the New Object – Site Link dialog box, type in a name of **Seattle-Denver**. Next, in the "Sites not in this site link" list box, highlight Seattle and Denver. Click Add. Click OK.
17. In the left pane of the AD Sites and Services dialog box, right-click the IP container, and select New Site Link from the menu that appears.
18. In the New Object – Site Link dialog box, type in a name of **Denver-Houston**. Next, in the "Sites not in this site link" list box, highlight Seattle and Denver. Click Add. Click OK.
19. In the left pane of the AD Sites and Services dialog box, right-click the IP container. Select Properties from the menu that appears.
20. In the IP Properties dialog box, clear the check box next to "Bridge all site links." Click OK.
21. In the left pane of the AD Sites and Services dialog box, right-click the IP container. Select New Site Link Bridge from the menu that appears.

22. In the New Object – Site Link Bridge dialog box, type in a name of **Seattle-Denver-Houston**. Then, in the "Site links not in this site link bridge" list box, highlight Seattle-Denver and Denver-Houston. Click Add. Click OK.
23. The site link bridge is created. Close Active Directory Sites and Services.

Answers to Chapter Questions

Chapter Pre-Test

1. The three replication partitions in Active Directory are: the schema partition, the configuration partition, and the domain partition.
2. Intrasite replication is Active Directory replication that takes place within a single site. Windows 2000, by default, automatically performs intrasite replication.
3. Intersite replication is Active Directory replication between sites. Unlike intrasite replication, intersite replication is not automatically configured and performed by Windows 2000, but must be manually configured by an Administrator.
4. The Knowledge Consistency Checker (KCC)
5. Until *subnet objects* are created and assigned to a site, the site has no definition and no functionality — it's just an empty Active Directory object.
6. True
7. The five operations master roles are: schema master, domain naming master, PDC emulator, relative ID master, and infrastructure master.
8. Active Directory Replication Monitor

Assessment Questions

1. **C.** Active Directory Sites and Services is the appropriate tool to create and manage sites.

2. **A.** You must use Active Directory Sites and Services to move the server objects for the eight domain controllers to their new sites.
3. **B.** Use Active Directory Sites and Services to modify the NTDS settings for the server object to configure the server as a global catalog Server.
4. **D.** Microsoft recommends that you *not* transfer the infrastructure master role to the domain controller that also serves as a global catalog server. If you do this (and you have more than one domain controller in the domain), the infrastructure master won't function.
5. **C.** Because you must have a minimum of two site links to create a site link bridge, and because each site link requires a minimum of two sites, you must have a minimum of three site links to create a site link bridge. See Figure 22-7.
6. **A.** RPC over IP and SMTP are the only replication protocols you can use, and RPC is much faster.
7. **B.** The server that is designated as the bridgehead server is used for intersite replication.
8. **C.** Although you can view a list of a specific domain controller's replication connections by using Active Directory Sites and Services, Active Directory Replication Monitor is a better answer because it is the only tool that enables you to view a *graphic* representation of a server's connections.

Scenarios

1. Probably the best thing you can do to speed up searches of Active Directory is to add an additional global catalog server to the site.
2. Use Active Directory Sites and Services to move the server objects (for the existing domain controllers that will be used in the new sites) to the new sites. You may also need to create and configure site links.
3. Either designate a different domain controller to function as the global catalog server (by using Active Directory Sites and Services), or transfer the infrastructure master role to a different domain controller (by using Active Directory Users and Computers or the `ntdsutil.exe` command-line utility).

When more than one domain controller is present in a domain, and the infrastructure master role is performed by the same domain controller that hosts the global catalog, the infrastructure master won't work.

4. The most likely cause of this problem is that the site link to the site not receiving all replication updates is not included in the site link bridge. To resolve this problem, reconfigure the site link bridge to include the site link to the affected site, or create an additional site link bridge, depending on your network configuration.
5. To manage and maintain Active Directory performance, add additional domain controllers (and an additional global catalog server, if appropriate) in the Seattle site. This will maintain current desired performance levels, and prepare for future growth.
6. The most likely cause of this problem is that the server has too many services installed on it, or doesn't have enough RAM or processor power to adequately perform all of its tasks. To resolve the problem, either transfer some of the services currently provided by this server to another domain controller or server, as appropriate, or upgrade the server's hardware.
7. The most likely cause of this problem is that server objects for existing domain controllers have not been moved to the new sites. Move the server objects to the new sites by using Active Directory Sites and Services.
8. Use Active Directory Sites and Services to designate a domain controller that is located on the same subnet as the intersite router as the preferred bridgehead server for the site.
9. Use Active Directory Sites and Services to manually create connection objects between each domain controller and every other domain controller, so that every domain controller has four manually created connection objects.