Enterprise

CHAPTER

Managing Windows NT Directory Services

10

About Chapter 10

This chapter defines and explains Windows NT Directory Services. After a brief overview, trust relationships between domains are discussed extensively. Included in this section are key terms as well as step-by-step instructions for creating one-way and two-way trusts. The chapter then explains the logon process and the part the NetLogon Service plays in this process. Pass-through authentication and synchronization of BDCs with the PDC are also explored.

Next, Chapter 10 outlines the four domain models: the single domain model, the single master domain model, the multiple master domain model, and the complete trust domain model. And finally, the chapter discusses how groups can be used to manage a large number of users in a multiple domain environment.

This chapter includes a review activity on planning as well as two hands-on labs. In the first lab you implement one-way and two-way trust relationships between two domains. In the second, you plan a Directory Services architecture and trust relationship for a given situation. Chapter 10 is optional if you're preparing for the Workstation or Server exams, but essential if you're preparing for the Enterprise exam. This chapter maps to the "Plan the implementation of a directory services architecture" objective in the Planning section in the Enterprise exam's objectives.

Overview of Windows NT Directory Services

Windows NT Directory Services refers to the architecture, features, functionality, and benefits of Windows NT domains and trust relationships. Windows NT Directory Services (often referred to simply as Directory Services), as implemented in Windows NT 4.0, is not X.500-compliant. However, Microsoft plans to release a new version of Windows NT Directory Services, called the *Active Directory*, that will be X.500-compliant in a future release of Windows NT.

The primary benefits of Directory Services, as implemented in NT 4.0, include the following:

- A single user account logon and password are used to gain access to all shared resources on the network. In a Windows NT Directory Services environment, users are not required to remember different user names and passwords for each network resource that they access.
- User and group accounts, as well as shared network resources, can be managed from a central location. Administrators are not required to log on to multiple computers to manage accounts and shared resources.

exam preparation pointer

The concepts presented in this chapter form the foundation for a large portion of the Windows NT Server 4.0 Enterprise exam. Don't even *think* about attempting to pass this exam until you've completely mastered trusts, domain models, and using groups in a multiple domain environment.

In the Directory Services architecture, domains contain logical groupings of user and group accounts, computers, and shared resources. A large company might have more than one domain in its Directory Services architecture. The next section examines how trust relationships are used to manage interaction between multiple domains.

Trust Relationships

To manage the interaction between multiple domains, trust relationships are necessary. *Trust relationships* enable users from one domain to access shared resources located in other domains.

Without trust relationships, the benefits of single user account logon and centralized administration would not be possible. If no trust relationship exists between two domains, users would have to have user accounts (and passwords) in both domains to access shared resources in both domains.

The terminology used to discuss trusts is sometimes confusing, so the next section is dedicated to explaining and clarifying these terms. Once you've mastered the terminology, trust concepts are much easier to understand.

Trust Terminology

Two primary terms are used to refer to a trust relationship between two domains: trusting domain and trusted domain.

Trusting domain—The *trusting domain* is the domain that has *resources* to share with user accounts in the trusted domain. The trusting domain trusts the trusted domain.

Trusted domain—The *trusted domain* is the domain that contains the *user accounts* that want to access resources in the trusting domain. The trusted domain is trusted by the trusting domain.

exam preparation pointer

This terminology is used extensively in Microsoft product documentation and on the Microsoft Certified Professional exams. Memorize these terms so that you are clear as to which domain contains the resources and which domain contains the user accounts.

A trust relationship between two domains is depicted in diagrams by using an arrow to point from the trusting (resource) domain to the trusted (accounts) domain. Remember that the arrow points toward the accounts domain.

Figure 10-1 depicts a trust relationship between the EAST domain and the WEST domain. The EAST domain is the trusted domain, and the WEST domain is the trusting domain. Notice that the arrow points toward the EAST domain, where the user accounts are stored. Users from the EAST domain are able to access shared resources on computers located in the WEST domain.

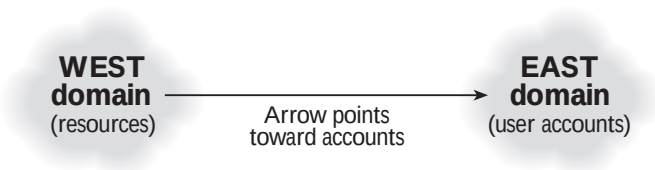


FIGURE 10-1 The WEST domain trusts the EAST domain

Many people are confused by the arrows used to depict trust relationships. It often seems more natural to have the arrow point toward the shared resource, because the resource is the object that users want to access. The opposite is true. The arrow points away from the resource, and the arrow points toward the user accounts. Always follow the arrow to determine the location of the user accounts.

One-way Trusts

When a single trust relationship exists between two domains, it is called a *one-way* trust.

Figure 10-1 is an example of a one-way trust, in which the WEST domain trusts the EAST domain. In this example, users from the EAST domain are able to access resources in both the EAST and WEST domains. However, the trust is one-way only, and, therefore, users in the WEST domain are able to access resources in the WEST domain only.

It is necessary to configure both domains to establish a trust relationship. Only an Administrator can establish a trust relationship.

Steps to create a one-way trust

Creating a one-way trust is a two-part process. In the first part of the process you configure the trusted domain to allow the trusting domain to trust it. In the second part, you configure the trusting domain to trust the trusted domain.

TO CREATE A ONE-WAY TRUST, FOLLOW THESE STEPS:

Part 1 On a computer in the domain that will be the trusted domain, that is, the domain that contains the user accounts, perform the following steps:

1. Select Start ⩾ Programs ⩾ Administrative Tools (Common) ⩾ User Manager for Domains (*not* User Manager).
2. In the User Manager dialog box, select Policies ⩾ Trust Relationships.
3. In the Trust Relationships dialog box, click the Add command button next to the Trusting Domains list box.
4. In the Add Trusting Domain dialog box, type the name of the trusting domain and an initial password to create the trust relationship. (The other domain will enter this password when the trust relationship is configured on its PDC.) Confirm the password.

   Figure 10-2 shows the Add Trusting Domain dialog box for the EAST domain. In these steps, the EAST domain is being configured to allow WEST domain to trust it. (The EAST domain will be the trusted domain, and the WEST domain will be the trusting domain.)

   Click OK.

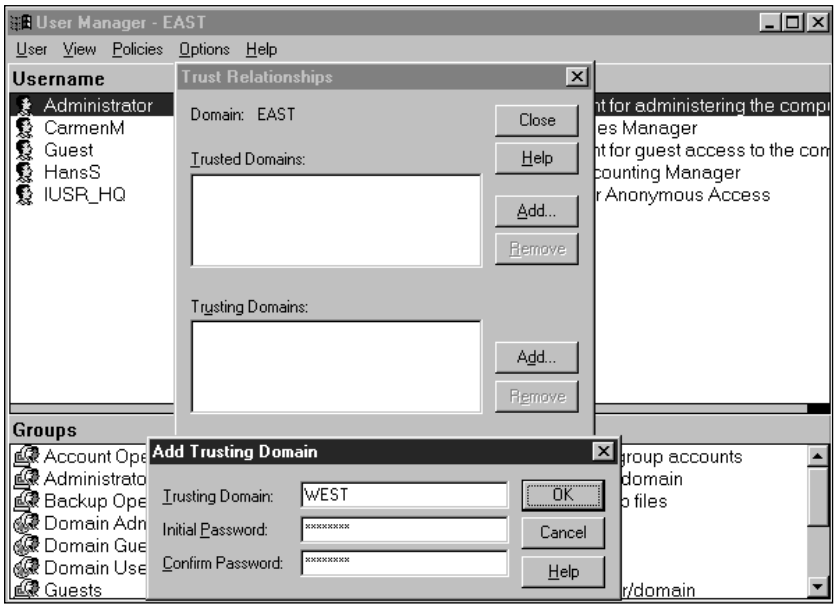


FIGURE 10-2 **Configuring the trusted domain**

5. In the Trust Relationships dialog box, the name of the trusting domain that you entered in Step 4 appears in the Trusting Domains list box.

Figure 10-3 shows the Trust Relationships dialog box for the EAST domain. Notice that the WEST domain is listed in the Trusting Domains list box. This means the EAST domain allows the WEST domain to trust it.

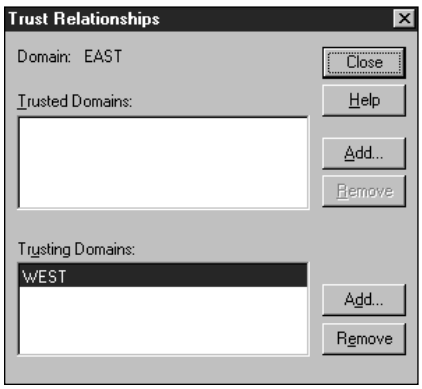


FIGURE 10-3 **Completing the configuration of the trusted domain**

Click the Close command button.

6. Exit User Manager for Domains.

Part 2 On a computer in the domain that will be the trusting domain, that is, the domain that contains the resources, perform the following steps:

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager for Domains (*not* User Manager).
2. In the User Manager dialog box, select Policies ➪ Trust Relationships.
3. In the Trust Relationships dialog box, click the Add command button next to the Trusted Domains list box.
4. In the Add Trusted Domain dialog box, type the name of the trusted domain and the password to create the trust relationship. (The password is the password that was entered in Step 4 in Part 1 of this process.) Click OK.
5. After a few moments a dialog box appears, as shown in Figure 10-4. Notice that the trust relationship has been successfully established. Click OK.

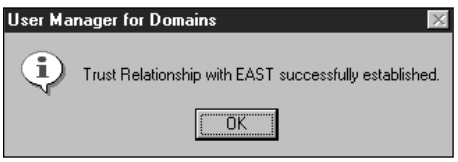


FIGURE 10-4 **Trust relationship established**

6. The Trust Relationships dialog box reappears, as shown in Figure 10-5. Notice that the EAST domain is listed in the Trusted Domains list box. This means the WEST domain trusts the EAST domain.

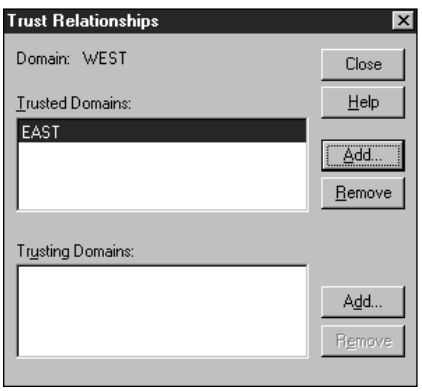


FIGURE 10-5 **The WEST domain trusts the EAST domain**

Click the Close command button.

7. Exit User Manager for Domains.

tip **I recommend you always configure the trusted domain first, and then configure the trusting domain when establishing a trust relationship. If you configure the domains in the reverse order, the dialog box shown in Figure 10-6 will be displayed. The trust relationship will usually be established within a few minutes.**

FIGURE 10-6 Result of configuring domains in reverse order when establishing a trust

Two-way Trusts

Sometimes it is advantageous to configure two domains to trust each other. For example, you may want to permit users from two different domains to access resources located in both domains.

When two domains trust each other, the configuration is referred to as a *two-way trust*. A two-way trust is really two one-way trusts, and is depicted in diagrams by two arrows between the two domains.

Figure 10-7 shows a two-way trust. Notice that a two-way trust is depicted as two one-way trusts. In this example, a two-way trust exists between the SALES domain and the SERVICE domain. Both domains contain user accounts and resources.

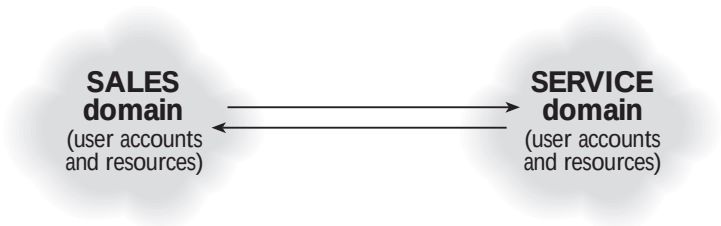


FIGURE 10-7 A two-way trust

As with one-way trusts, you must configure both domains to establish a two-way trust relationship.

Steps to create a two-way trust

Assume you want to create a two-way trust between two domains in your company, the SALES domain and the SERVICE domain.

Creating a two-way trust between the SALES domain and the SERVICE domain is a three-step process, as the following section explains.

TO CREATE A TWO-WAY TRUST, FOLLOW THESE STEPS:

1. Configure the SALES domain to allow the SERVICE domain to trust it. To do this, follow the steps in Part 1 in the "Steps to create a one-way trust." Figure 10-8 shows the SALES domain configured to allow the SERVICE domain to trust it.

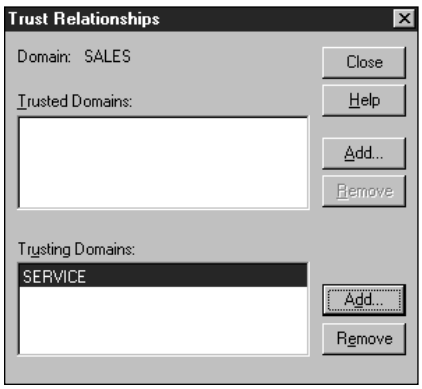


FIGURE 10-8 **First step in creating a two-way trust**

2. Configure the SERVICE domain to trust the SALES domain, and also to allow the SALES domain to trust the SERVICE domain. To do this, follow the steps in Part 2 in the "Steps to create a one-way trust," and then perform the steps in Part 1 in the "Steps to create a one-way trust." Figure 10-9 shows the SERVICE domain configured to trust the SALES domain, and also to allow the SALES domain to trust it.
3. Configure the SALES domain to trust the SERVICE domain. To do this, follow the steps in Part 1 in the "Steps to create a one-way trust." This completes the creation of a two-way trust between the SALES domain and the SERVICE domain. The SALES domain now trusts the SERVICE domain, and the SALES domain allows the SERVICE domain to trust it, as shown in Figure 10-10.

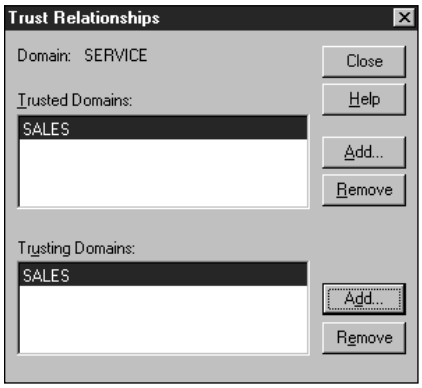


FIGURE 10-9 **Second step in creating a two-way trust**

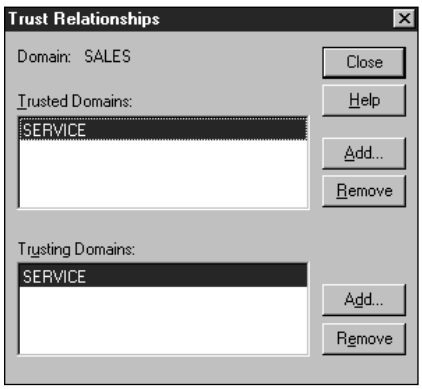


FIGURE 10-10 **Two-way trust established between the SALES domain and the SERVICE domain**

Trusts Are Non-transitive

Trust relationships between domains are *non-transitive*, which means that trusts apply *only* to the domains they are established between (they do not extend to other domains. For example, suppose that the A domain trusts the B domain. Further suppose that the B domain trusts the C domain. Figure 10-11 shows these trust relationships.

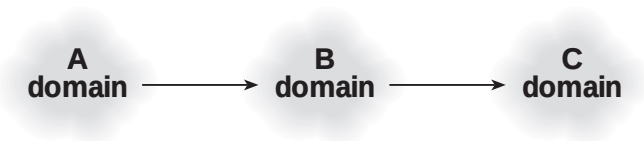


FIGURE 10-11 **Trusts between the A, B, and C domains**

At first glance, it might appear that user accounts in the C domain are able to access resources in the A domain. This is *not* the case. A trust relationship does not exist between the A domain and the C domain. Therefore, users in the C domain *can't* access resources in the A domain.

To enable users in the C domain to access resources in the A domain, a trust must be established between the A domain and the C domain. Figure 10-12 shows the three domains after the additional trust is established. Notice that the A domain now trusts the C domain. Users in the C domain can now access resources in the A domain.

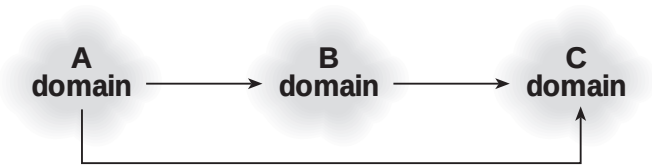


FIGURE 10-12 Trust established between the A domain and the C domain

Logging On

When a user logs on to a Windows NT computer or domain, the logon process is managed by the NetLogon Service. The following sections explain the purpose and function of this service, and provide several detailed examples of the logon process.

The NetLogon Service

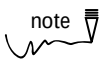
The *NetLogon Service* is installed automatically during the installation of Windows NT. The service is configured, by default, to start automatically every time Windows NT is booted.

The NetLogon Service in Windows NT is responsible for managing the logon process, pass-through authentication, and synchronization of the *backup domain controllers* (BDCs) with the *primary domain controller* (PDC) within a domain.

The logon process

To understand the nuances of the logon process, it's helpful to have an understanding of the Windows NT *Security Accounts Manager* (SAM) database.

Windows NT assigns every user account, group account, and computer account a unique *security identifier* (SID). All account information, including user names, passwords, group memberships, and SIDs are stored in a domain database called the SAM database. This database is created originally on the domain's PDC (and on each local Windows NT computer that is a non-domain controller). The SAM is stored in the *<winntroot>*\System32\Config folder.



Several terms are used to refer to the domain SAM. The most commonly used terms include Windows NT Directory Services database, Directory Services database, domain directory database, and directory database. All of these terms are interchangeable and refer to the Security Accounts Manager (SAM) database. I've tried to use *SAM* to refer to the Security Accounts Manager (SAM) database on all non-domain controllers, and the term *Directory Services database* to refer to the common Security Accounts Manager (SAM) database on domain controllers.

Here's how SIDs, the SAM, and the NetLogon Service interact when you log on to a Windows NT Workstation computer using a local user account:

- You begin the logon process by pressing Ctrl + Alt + Delete. The Logon Information dialog box appears, prompting you to enter a user name and password. If the Windows NT Workstation computer is a member of a domain, an additional Domain drop-down list box is displayed. In the Domain drop-down list box, you can choose to log on using a user account from the domain or using a user account on the local computer. In this example, you are logging on using a user account on the local computer.
- When you click OK in the Logon Information dialog box, Windows NT provides your logon information (user name, password, and domain/local computer name) to the NetLogon Service. The NetLogon Service determines whether you are logging on using a user account on the local computer or a user account from the domain. In this example, you are logging on using a user account on the local computer. The NetLogon Service queries the local SAM to determine if your user account and

password is valid. If your user name and password are validated, the NetLogon Service retrieves your user account's SID, and the SIDs for each group of which you are a member. The NetLogon Service combines your user and group SIDs to create an *access token*.

- The NetLogon Services completes the logon process for you.

For the rest of the logon session, Windows NT uses your access token to determine whether you can access resources. Every time you attempt to access a resource (such as a folder or a printer), Windows NT compares the SIDs in your access token to the SIDs contained in the *access control list* (ACL) for the resource you want to access. If the SIDs in your access token are listed in the ACL for the resource, you are granted access to the resource.

Anytime a user logs on to a Windows NT computer using a user account that is *not* contained in the local computer's SAM, pass-through authentication is used to validate the user.

Pass-through authentication

Pass-through authentication enables a user to log on to a Windows NT computer by using a user account from the domain or from a trusted domain. Without pass-through authentication, the single user account logon/single password feature of Directory Services would not be possible.

Pass-through authentication occurs when a user account can't be validated by the NetLogon Service on the local computer. The NetLogon Service on the local computer forwards (passes-through) the logon request (and logon information) to the NetLogon Service on a Windows NT Server domain controller for validation. The domain controller validates the user account and passes the appropriate SIDs back to the NetLogon Service on the local computer to which the user is logging on. The NetLogon Service on the local computer completes the user's logon and creates the user's access token. The following examples show how pass-through authentication works.

Example 1: Logging on by using a user account from the domain Assume a user logs on to a Windows NT Workstation computer, which is a member of the WEST domain, by using a user account from the WEST domain. Figure 10-13 depicts this scenario.

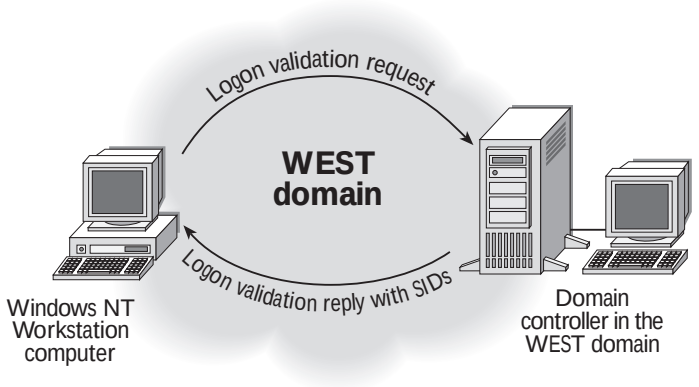


FIGURE 10-13 **Pass-through authentication in a single domain environment**

- The user enters a user name, password, and domain name in the Logon Information dialog box.
- The local NetLogon Service determines that the user account is not in the local computer's SAM, and forwards (passes-through) the logon request to a domain controller (in the WEST domain) for validation.
- The NetLogon Service on the domain controller verifies the user account and password, and retrieves the user and group SIDs for that user account from the Directory Services database.
- Then the NetLogon Service on the domain controller passes the SIDs to the NetLogon Service on the Windows NT Workstation computer, where the local NetLogon Service completes the logon process for the user.

Example 2: Logging on using a user account from a trusted domain

Assume a user who normally works in a company's Dallas office is visiting the company's Seattle office. This user logs on to a Windows NT Workstation computer in the SEATTLE domain by using a user account from the DALLAS domain. The SEATTLE domain trusts the DALLAS domain. Figure 10-14 depicts this scenario.

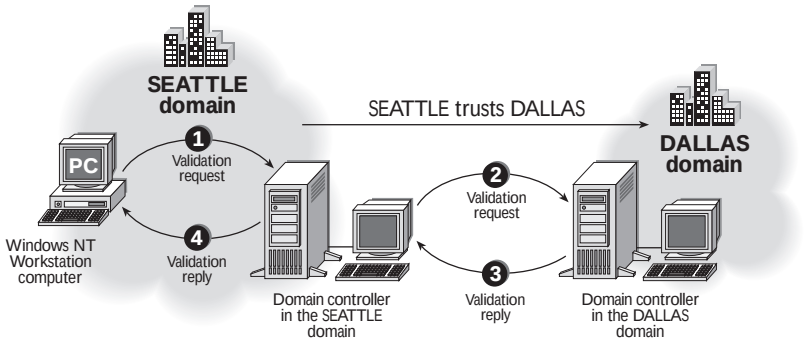
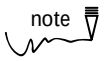


FIGURE 10-14 **Pass-through authentication across a trust relationship**

Here are the steps that take place to authenticate the user when the user logs on across a trust:

- The user begins the logon process at the Windows NT Workstation computer located in the SEATTLE domain by entering a user name, password, and domain name in the Logon Information dialog box. (The user enters a domain name of DALLAS to indicate which domain contains the user's account.) The local NetLogon Service determines that the user account is not in the local computer's SAM, and forwards (passes-through) the logon request to a domain controller in the SEATTLE domain for validation.
- The NetLogon Service on the domain controller in the SEATTLE domain forwards (passes-through) the logon request to a domain controller in the DALLAS domain for validation.
- The NetLogon Service on the domain controller in the DALLAS domain verifies the user account and password, and retrieves the user and group SIDs for that user account from the Directory Services database. Then the NetLogon Service on the DALLAS domain controller passes the SIDs to the NetLogon Service on the SEATTLE domain controller.
- The NetLogon Service on the SEATTLE domain controller passes the SIDs to the NetLogon Service on the Windows NT Workstation computer, where the local NetLogon Service completes the logon process for the user.



In Windows NT, all pass-through authentication requests and validation replies are sent over the network in an encrypted format. User names and passwords are never sent over the network in clear (unencrypted) text. This security feature discourages unauthorized persons from using network analyzer-type tools in an attempt to gather password and user account information on a Windows NT network.

Synchronization of BDCs with the PDC

Another function of the NetLogon Service is to periodically copy Directory Services database update information from the PDC to each BDC in the domain. This process is called *synchronization*.

To begin the synchronization process, the PDC notifies each BDC that the Directory Services database on the PDC has been updated. Each BDC then contacts the PDC to obtain the changes necessary to update the BDC's copy of the PDC's Directory Services database.

Managing the synchronization process is covered in more detail in Chapter 11.

Directory Services Architecture

Domains are the basic unit that comprise Directory Services architecture. They contain logical groupings of user and group accounts, computers, and shared resources. Domains can be structured and combined in various architectures, called *domain models*.

Many factors must be considered when planning a Directory Services architecture. Some of these factors include the total number and location of users in the organization; the number, types, and location of computers and shared resources; whether centralized or decentralized network management is desired; and the needs of departments within the organization. The Directory Services architecture an organization chooses must meet the needs and characteristics of that organization.

There are four domain models: the single domain model, the single master domain model, the multiple master domain model, and the complete trust domain model. An organization can choose any one of these four models, or it can implement a hybrid combination of two or more models.

Single Domain Model

The *single domain model* is the most straightforward of the four domain models. It consists of one domain and does not use trust relationships. All user accounts, group accounts, computer accounts, and shared resources are contained in a single domain.

The single domain model is ideal for the small- to medium-sized organization that wants to use centralized network administration. It can by used by organizations that have multiple locations. Although many organizations choose to implement multiple domains when they have multiple locations, it is not a requirement.

The single domain model does have limitations. It can accommodate a maximum of 40,000 user accounts. However, if the domain contains computer accounts and an appropriate number of group accounts, the practical limitation for a single domain is about 26,000 user accounts. If an organization has more than 26,000 user accounts, it should use another domain model. Another limitation of the single domain model is that browsing can be slow if there are a large number of shared resources, or if shared resources are in geographically diverse locations connected by slow WAN links.

Single Master Domain Model

The *single master domain model* consists of one master domain that contains all user accounts and one or more domains that contain shared resources. This domain model uses one-way trusts from each resource domain to the master domain.

Figure 10-15 depicts the single master domain model. Notice the one-way trust relationships between the domains. The master domain is the trusted domain, and the resource domains are the trusting domains. All user accounts are contained in the master domain.

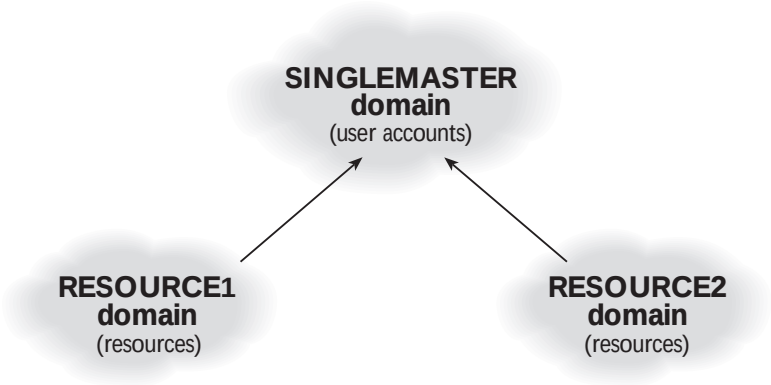


FIGURE 10-15 The single master domain model

The single master domain model is ideal for small- to medium-sized organizations that want to subdivide administration of resources along geographic or departmental lines. This model enables user accounts to be managed centrally, but provides for regional or departmental control over shared resources.

The single master domain model, like the single domain model, is limited to a maximum of 40,000 user accounts.

concept link 

For more information on how to determine the number of user accounts, computer accounts, and group accounts that a domain can accommodate, see Chapter 11.

Multiple Master Domain Model

The *multiple master domain model* consists of two or more master domains that contain user accounts and any number of domains that contain shared resources. In this model, a two-way trust is used between each of the master domains, and one-way trusts are used from each resource domain to each and every master domain.

Figure 10-16 depicts the multiple master domain model. Notice the configuration of trust relationships in the diagram.

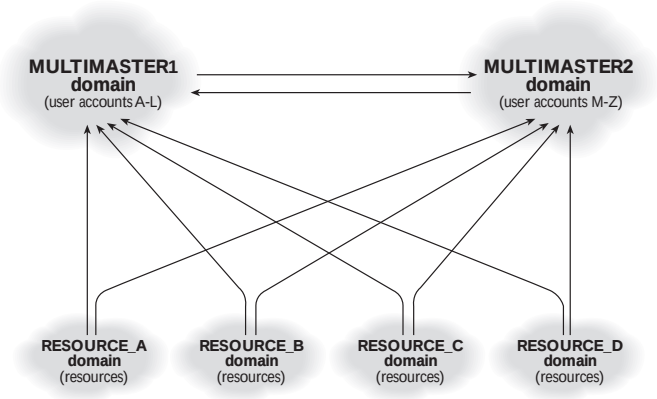


FIGURE 10-16 **The multiple master domain model**

There are various ways to distribute user accounts among the two or more master domains. You can distribute user accounts by any of the following:

- Division or department
- Geographic location, such as by city or region
- Alphabetically, by user account name or by the user's actual name
- Using any hybrid combination of the aforementioned

The multiple master domain model can be scaled to match any size organization. There is no practical limitation on the number of user accounts an organization can have, because an additional master domain can always be added.

Because of the two-way trust that exists between the master domains, user account administration can be centralized, or it can be distributed among multiple administrators. In the multiple master domain model, management of shared resources can be distributed by geographic location or by department.

This domain model is the preferred model by the majority of large organizations, because of its practicality and scaleability.

Complete Trust Domain Model

The *complete trust domain model* is a decentralized model that consists of two or more domains that contain user accounts and shared resources. A two-way trust relationship exists between each and every domain.

Figure 10-17 depicts the complete trust domain model. Notice the configuration of trust relationships in the diagram.

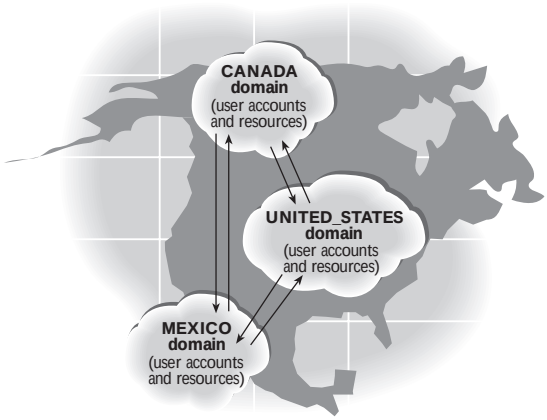


FIGURE 10-17 **The complete trust domain model**

Figure 10-17 shows a total of three domains and six trust relationships. This looks fairly easy to manage upon first glance, but as the number of domains increases, the number of trusts also increases—often to an excessive number. The number of trust relationships required to implement this domain model can be computed by using the formula $n \times (n - 1)$, where n equals the number of domains. A complete trust domain model consisting of four domains requires twelve trust relationships, a complete trust domain model consisting of five domains requires twenty trust relationships, and a complete trust domain model consisting of ten domains requires ninety trust relationships.

Organizations that require decentralized management of user accounts and shared resources can choose the complete trust domain model. However, because of the excessive number of trusts required, this model is *not* recommended.

Besides the number of trusts involved, another drawback of this model is that managers of shared resources must trust administrators of other domains to place only appropriate users in each global group that has permissions to the shared resources they manage.

Because multiple domain environments often involve many users, it's imperative that you understand how to place users into groups appropriately and manage these groups to streamline the administration of your network.

Using Groups to Manage Users in a Multiple Domain Environment

The easiest way to manage many users in a multiple domain environment is through groups. Groups enable the administrator to assign rights and permissions to multiple users efficiently.

concept link 

Groups were introduced and discussed in detail in Chapter 7. If it's been a while since you studied Chapter 7, you may want to refresh your understanding of how group accounts are used.

Groups are commonly used in the following way in a multiple domain environment:

- First, *user accounts* are placed into a *global group* in the trusted domain.
- Next, this global group, which can cross trust relationships to other domains, is made a member of a *local group* in the trusting domain.
- Finally, the local group in the trusting domain is assigned *permissions to a shared resource* in the trusting domain, so that all of the local group's members can access the shared resource.

Figure 10-18 shows how groups are used in a multiple domain environment. Notice the flow of the process: user accounts are made members of a global group in the CALIFORNIA domain. This global group can cross the trust to the ILLINOIS domain. Then the global group is made a member of a local group in the ILLINOIS domain, which is then assigned permissions to a shared printer in the ILLINOIS domain.

Keep in mind that local groups can be assigned permissions only to resources within a single domain. However, global groups can cross trust relationships to other domains. Occasionally a single user account within a domain may be made a member of a local group in another domain. This is possible because user accounts, like global groups, can also cross trust relationships to other domains.

To cement your understanding of how groups can be used to manage users in multiple domain environments, two example applications are presented in the following section.

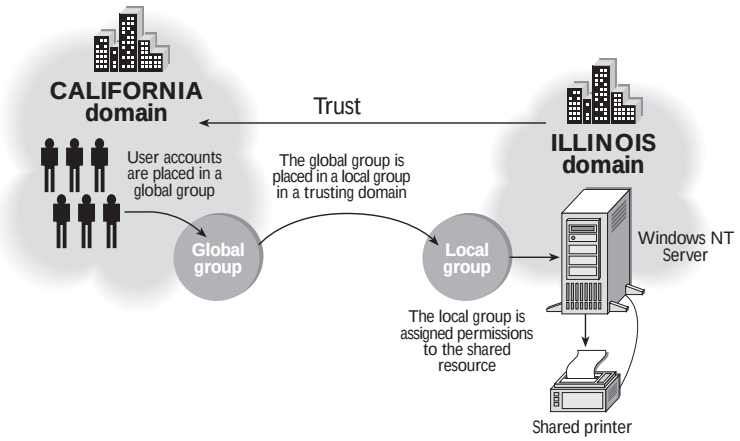


FIGURE 10-18 **Using groups to manage users in a multiple domain environment**

Example 1: Using Global Groups and Built-in Groups in a Single Master Domain Model

Assume you are an administrator of a Windows NT network that uses the single master domain model. Your organization's domain model is shown in Figure 10-19. Notice the trust relationships between the resource domains and the master domain. Also notice the location of the user accounts.

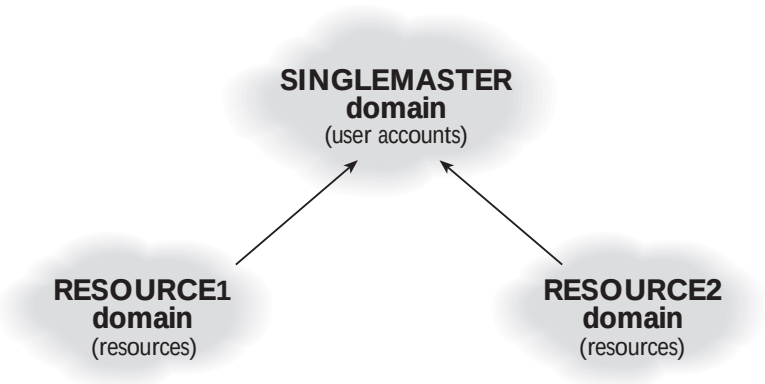


FIGURE 10-19 **Domain model for Example 1**

Table 10-1 shows the distribution of domain controllers, member servers, and Windows NT Workstation computers (that are members of their respective domains) in each of the three domains.

TABLE 10-1 COMPUTER DISTRIBUTION IN EXAMPLE 1

DOMAIN	*# DOMAIN CONTROLLERS*	*# MEMBER SERVERS*	*# NT WORKSTATIONS*
SINGLEMASTER	3	10	50
RESOURCE1	2	5	100
RESOURCE2	2	2	100

You have been assigned the job of creating a single global group that has rights to restore files to all domain controllers, all member servers, and all Windows NT Workstation computers in all three domains.

You accomplish this task by doing the following:

- Creating one global group, called Restore, in the SINGLEMASTER domain. You assign the appropriate user accounts to this global group.
- Placing the Restore global group in the Backup Operators built-in local group (which has the rights to *restore* as well as backup files) in the SINGLEMASTER, RESOURCE1, and RESOURCE2 domains. (This enables members of the Restore global group to restore files to all of the domain controllers in all three domains.)
- Placing the Restore global group in the Backup Operators built-in local group on *each* member server in the SINGLEMASTER, RESOURCE1, and RESOURCE2 domains. (This enables members of the Restore global group to restore files to all of the member servers in all three domains.)
- Placing the Restore global group in the Backup Operators built-in local group on *each* Windows NT Workstation computer in the SINGLEMASTER, RESOURCE1, and RESOURCE2 domains. (This enables members of the Restore global group to restore files to all of the Windows NT Workstation computers in all three domains.)

Example 2: Using Global Groups and Built-in Groups in a Multiple Master Domain Model

Assume you are the lead administrator of a Windows NT network that uses the multiple master domain model. Your company's domain model is shown in Figure 10-20. Notice the trust relationships between the resource domains and the master domains. Also notice the location of the user accounts.

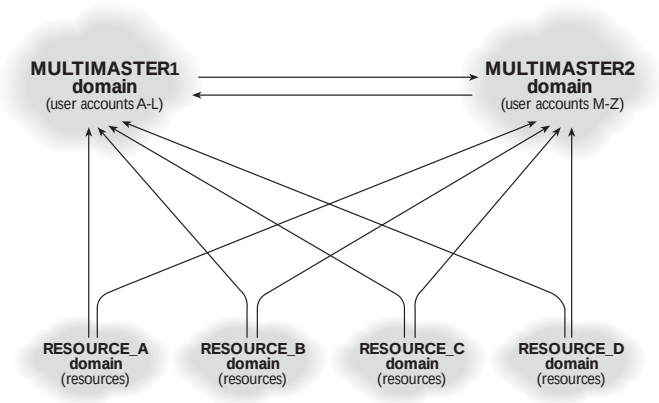


FIGURE 10-20 **Domain model for Example 2**

Table 10-2 shows the distribution of domain controllers, member servers, and Windows NT Workstation computers (that are members of their respective domains) in each of the six domains.

TABLE 10-2 COMPUTER DISTRIBUTION IN EXAMPLE 2

DOMAIN	*# DOMAIN CONTROLLERS*	*# MEMBER SERVERS*	*# NT WORKSTATIONS*
MULTIMASTER1	6	2	25
MULTIMASTER2	6	2	75
RESOURCE_A	3	3	100
RESOURCE_B	4	11	400
RESOURCE_C	2	7	300
RESOURCE_D	2	9	350

You have decided that your company needs a global group in each master domain that has rights to restore files to all domain controllers, all member servers, and all Windows NT Workstation computers in all six domains. You accomplish this rather large task by doing the following:

- Creating a global group called Master1Restore in the MULTIMASTER1 domain, and creating another global group called Master2Restore in the MULTIMASTER2 domain. You assign the appropriate user accounts to these global groups.
- Placing the Master1Restore and the Master2Restore global groups in the Backup Operators built-in local group (which has the rights to *restore* as well as backup files) in the MULTIMASTER1, MULTIMASTER2, RESOURCE_A, RESOURCE_B, RESOURCE_C, and RESOURCE_D domains. (This enables members of the Master1Restore and Master2Restore global groups to restore files to all of the domain controllers in all six domains.)
- Placing the Master1Restore and the Master2Restore global groups in the Backup Operators built-in local group on *each* member server in the MULTIMASTER1, MULTIMASTER2, RESOURCE_A, RESOURCE_B, RESOURCE_C, and RESOURCE_D domains. (This enables members of the Master1Restore and Master2Restore global groups to restore files to all of the member servers in all six domains.)
- Placing the Master1Restore and the Master2Restore global groups in the Backup Operators built-in local group on *each* Windows NT Workstation computer in the MULTIMASTER1, MULTIMASTER2, RESOURCE_A, RESOURCE_B, RESOURCE_C, and RESOURCE_D domains. (This enables members of the Master1Restore and Master2Restore global groups to restore files to all of the Windows NT Workstation computers in all six domains.)

These two examples highlight the use of global groups and built-in local groups in a multidomain environment. They also point out that in a Windows NT network, each member server and each Windows NT Workstation computer has its own SAM, and because of this fact, the local groups on each of these computers must be configured individually.

Key Point Summary

This chapter explained managing Windows NT Directory Services. The following points illuminate the major issues:

- Windows NT Directory Services (Directory Services) is a Microsoft catchall phrase that refers to the architecture, features, functionality, and benefits of Windows NT domains and trust relationships. The primary benefits of Directory Services include a single user account logon and password, and centralized management of user and group accounts. In the Directory Services architecture, domains contain logical groupings of user and group accounts, computers, and shared resources.
- Trust relationships enable users from one domain to access shared resources located in other domains. In a trust relationship between two domains, the trusting domain is the domain that contains the shared resources, and the trusted domain is the domain that contains the user accounts. A trust relationship is depicted in diagrams by an arrow that points from the trusting (resource) domain to the trusted (user accounts) domain. Remember that the arrow points toward the accounts domain.
- When a single trust relationship exists between two domains, it is called a *one-way trust*. Both domains must be configured by an Administrator in order to establish a trust relationship. Trusts are configured in Windows NT by using User Manager for Domains. The trusted domain should be configured first, and then the trusting domain.
- When two domains trust each other, it is called a *two-way trust*. A two-way trust is really two one-way trusts, and is depicted in diagrams by two arrows between the two domains. As with one-way trusts, both domains must be configured by an Administrator in order to establish the two-way trust relationship.
- Trust relationships are non-transitive—they apply only to the domains they are established between. If the A domain trusts the B domain, and the B domain trusts the C domain, user accounts in the C domain *can't* access resources in the A domain because no trust exists between the A domain and the C domain.

- When a user logs on to a Windows NT computer or domain, the logon process is managed by the NetLogon Service. The NetLogon Service is responsible for managing not only the logon process, but pass-through authentication and synchronization of the BDCs with the PDC, as well.
- In the logon process, a user enters a user name, password, and domain name in the Logon Information dialog box. The local NetLogon Service determines whether the user account is located in the local computer's Security Accounts Manager (SAM) database. If the user account is found to be valid by the local SAM, the NetLogon Service retrieves the user account's security identifier (SID), and the SIDs for each group that the user is a member of. The NetLogon Service combines the user and group SIDs to create an access token, and then completes the logon process for the user.
- Anytime a user logs on to a Windows NT computer using a user account that is *not* contained in the local computer's SAM, pass-through authentication is used to validate the user. Pass-through authentication enables a user to log on to a Windows NT computer by using a user account from the domain or from a trusted domain.
- When a user account can't be validated on the local computer, the NetLogon Service on the local computer forwards (passes-through) the logon request to the NetLogon Service on a Windows NT Server domain controller for validation. The domain controller either validates the user account and passes the appropriate SIDs back to the local NetLogon Service to complete the logon process; or, if the user account resides in a trusted domain, the domain controller forwards (passes-through) the logon request to the NetLogon Service on a Windows NT Server domain controller in the trusted domain for validation. The NetLogon Service on the trusted domain's domain controller validates the user account and passes the appropriate SIDs back to the NetLogon Service on the trusting domain's domain controller, which, in turn, passes the SIDs back to the NetLogon Service on the local computer so that the user's logon can be completed.
- Domains are the basic unit that comprise Directory Services architecture. Domains can be structured and combined in various architectures, called domain models. Many factors must be considered when planning a

Directory Services architecture, including the number and location of users; the number, types, and location of computers and shared resources; whether centralized or decentralized network management is desired; and the needs of departments within the organization. There are four domain models: the single domain model, the single master domain model, the multiple master domain model, and the complete trust domain model.

- The *single domain model* consists of one domain and does not use trust relationships. All user accounts and shared resources are contained in a single domain. A single domain can accommodate a maximum of 40,000 user accounts; but has a practical limitation of about 26,000 user accounts, assuming that each user has a Windows NT computer.
- The *single master domain model* consists of one master domain that contains all user accounts *and* one or more domains that contain shared resources. This domain model uses one-way trusts from each resource domain to the master domain. This model is ideal for small- to medium-sized organizations that want to mange user accounts centrally but also provide for regional or departmental control over shared resources. The single master domain model, like the single domain model, is limited to 40,000 user accounts.
- The *multiple master domain model* consists of two or more master domains that contain user accounts *and* any number of domains that contain shared resources. A two-way trust is used between each of the master domains, and one-way trusts are used from each resource domain to each and every master domain. This model can be scaled to match any size organization, and has no practical limitation on the number of user accounts, because an additional master domain can always be added. Because of the two-way trust that exists between the master domains, user account administration can be centralized, or it can be distributed among multiple administrators. Management of shared resources is generally distributed by geographic location or by department.
- There are various ways to distribute user accounts among two or more master domains: by division or department, by geographic location, alphabetically, or by using any hybrid combination of the aforementioned.
- The *complete trust domain model* is a decentralized model that consists of two or more domains that contain user accounts and shared resources.

A two-way trust relationship exists between each and every domain. The number of trusts required to implement this model can be computed by using the formula $n \times (n-1)$, where n equals the number of domains. Because of the excessive number of trusts required, this model is not recommended.

- The easiest way to manage many users in a multiple domain environment is by using groups. Groups enable the administrator to assign rights and permissions to multiple users efficiently. Groups are commonly used in the following way in a multiple domain environment:
  - First, user accounts are placed into a global group in the trusted domain.
  - Next, this global group, which can cross trust relationships to other domains, is made a member of a local group in the trusting domain.
  - Finally, the local group in the trusting domain is assigned permissions to a shared resource located in the trusting domain, so that all of the local group's members can access the shared resource.
- Local groups can be assigned permissions only to resources within a single domain.
- In a Windows NT network, each member server and each Windows NT Workstation computer has its own SAM, and because of this fact, the local groups on each of these computers must be configured individually.

Applying What You've Learned

Now it's time to regroup, review, and apply what you've learned in this chapter.

The questions in the Instant Assessment section that follows bring to mind key facts and concepts. The review activity tests your ability to plan network administration in a multiple master domain environment. The hands-on lab exercises reinforce what you've learned and give you an opportunity to practice some of the tasks tested by the Enterprise exam.

Instant Assessment Questions

1. What is Windows NT Directory Services?
2. What are the primary benefits of Windows NT Directory Services?
3. In a trust relationship, which domain is the trusting domain and which domain is the trusted domain?
4. What is a single trust relationship between two domains called?
5. What is the trust relationship of two domains that trust each other called?
6. What Windows NT tool must you use to create a trust relationship?
7. What does the fact that trust relationships are non-transitive mean?
8. Briefly describe the logon process when a user logs on to a Windows NT Workstation computer by using a local user account.
9. What Windows NT feature enables a user to log on to a Windows NT computer using a user account from the domain or from a trusted domain?
10. Briefly describe how pass-through authentication works when a user logs on to a Windows NT Workstation computer, which is a member of a domain, using a user account from the domain.
11. The NetLogon Service periodically replicates Directory Services database update information from the PDC to each BDC in the domain. What is this process called?
12. What factors should be considered when planning a Directory Services architecture?
13. Which domain model consists of two or more master domains that contain user accounts *and* any number of domains that contain shared resources?
14. Which domain model consists of one master domain that contains all user accounts *and* one or more domains that contain shared resources?
15. Which domain model consists of one domain and does not use trust relationships?
16. Which domain model is a decentralized model that consists of two or more domains that contain user accounts and shared resources, and between each domain a two-way trust exists? (Hint: This model can require an excessive number of trust relationships and is not recommended.)

17. You are the administrator for a small company (2,000 users) that wants to use centralized administration of its Windows NT network. You do not require any departmental or geographical control of shared resources. Which domain model would you use?

18. You are the administrator for a large company (60,000 users) that wants to use distributed network administration for the user accounts and shared resources that make up your Windows NT network. Which domain model would you use?

19. Briefly describe how groups are commonly used to manage users in a multiple domain environment.

T/F

20. Both domains must be configured in order to establish a trust relationship. _____

concept link  **For answers to the Instant Assessment questions see Appendix D.**

Enterprise

Review Activity

Planning network administration in a multiple master domain environment exercise

You manage the administrators of a Windows NT network that uses the multiple master domain model. Your company's domain model is shown in Figure 10-21.

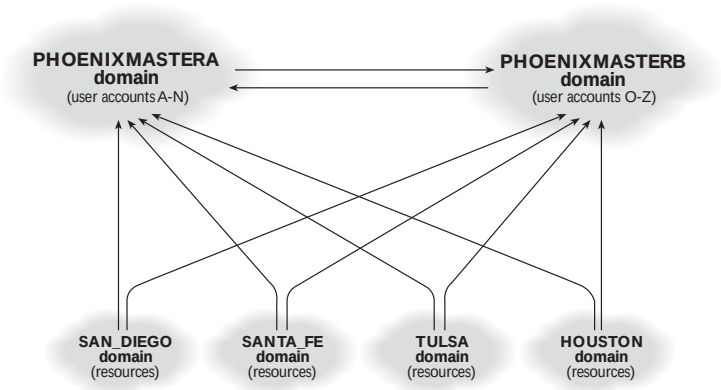


FIGURE 10-21 **Your company's domain model**

Table 10-3 shows the distribution of domain controllers, member servers, and Windows NT Workstation computers (that are members of their respective domains) in each of your company's six domains.

TABLE 10-3 YOUR COMPANY'S COMPUTER DISTRIBUTION

DOMAIN	*# DOMAIN CONTROLLERS*	*# MEMBER SERVERS*	*# NT WORKSTATIONS*
PHOENIXMASTERA	3	2	40
PHOENIXMASTERB	3	2	25
SAN_DIEGO	2	3	150
SANTA_FE	2	6	50
TULSA	2	5	50
HOUSTON	2	4	200

As your company's budding Windows NT guru, your job, should you choose to accept it, is to create a global group in each master domain and use existing built-in local groups to enable specific users in the PHOENIXMASTERA and PHOENIXMASTERB domains to fully administer users, groups, and shared resources on all Windows NT computers in all six domains.

The following may help you to plan a solution to this task:

New global group in PHOENIXMASTERA domain: _____

New global group in PHOENIXMASTERB domain: _____

Built-in local group in each domain in which you will place the two new global groups:_____

Built-in local group on every member server in all six domains in which you will place the two new global groups: _____

Built-in local group on every Windows NT Workstation computer in all six domains in which you will place the two new global groups: _____

concept link 

For answers to the Review Activity see Appendix D.

Hands-on Lab Exercises

The following hands-on lab exercises provide an excellent opportunity for you to apply many of the concepts about managing Windows NT Directory Services that you've learned in this chapter.

Lab 10.15 *Implementing a trust relationship*

Enterprise

This lab is optional, but only because it requires an additional Intel-based computer with a 486/33 processor, 16MB of RAM, and 500MB — 1GB available hard disk space. You will also need a VGA monitor and graphics card and mouse. A CD-ROM drive for the second computer would be nice, but it's not absolutely necessary if you don't mind taking the CD-ROM drive out of your first computer and installing it in the second for the NT installation portion of this lab. This lab also requires that you use two network adapters and the appropriate cabling to connect the two computers.

I can't suggest strongly enough that you go through whatever pain is necessary to beg, borrow, rent, or purchase a second computer to use in this lab (a 486 can be obtained fairly inexpensively), and t**he benefit you'll receive from experiencing trusts and groups in a multiple domain environment will pay off big when you take the Enterprise exam.**

The objective of this lab is to give you hands-on experience with implementing and testing one-way and two-way trust relationships between two domains.

This lab consists of the following five parts:

Part 1: Installing Windows NT Server 4.0 on a second computer

Part 2: Configuring a one-way trust

Part 3: Testing a one-way trust

Part 4: Configuring a two-way trust

Part 5: Testing a two-way trust

Part 1: Installing Windows NT Server 4.0 on a second computer

First install MS-DOS on the second computer's hard drive, and load the drivers for the CD-ROM drive. Make sure that the Windows NT Server compact disc is in the CD-ROM drive.

You will need one blank, 3.5-inch high-density floppy disk for this lab exercise.

Follow the steps below carefully to perform the installation of Windows NT Server 4.0.

Pre-copy phase

1. Change the default drive to your CD-ROM drive by typing in the CD-ROM drive letter followed by a colon (for example, **D:**), and press Enter.
2. Type **cd i386**, and then press Enter.
3. Type **winnt /b**, and then press Enter. (This command instructs Setup to perform the `Winnt.exe` installation without creating the Setup Boot Disk set.)
4. When Windows NT Setup asks you to enter the path where NT files are located, press Enter.
5. Setup copies files to your hard disk. (This process takes a few minutes. How about a stretch break or a fresh cup of coffee?)
6. When the Windows NT Server Setup screen appears, press Enter to restart your computer and continue Windows NT Setup.

Phase 0

1. After a minute or two, when the Windows NT Server Setup screen appears, press Enter to set up Windows NT now.
2. Setup displays a screen showing any mass storage devices, such as SCSI adapters, CD-ROM drives, and so on. Some older IDE controllers will not be displayed here, but they will still function and be recognized by NT. Specify additional devices by making changes on this screen if necessary. When you have completed all necessary changes, press Enter to continue.
3. The Windows NT Licensing Agreement screen appears. Read the licensing agreement, pressing PgDn to view additional screens of the agreement. When you reach the bottom of the agreement, press F8 to continue setup.
4. Windows NT Server Setup displays a screen listing your computer's hardware and software components. Make any changes necessary. When you are finished, highlight "The above list matches my computer," and press Enter.

5. If you have a previous version of Microsoft Windows installed on your computer, Setup displays a screen stating that it detected a previous version. If this screen appears, press **N** to install Windows NT Server in a different directory.
6. Windows NT Server Setup displays a screen showing your computer's hard disk partitions. Highlight the partition on which you want to install Windows NT Server, then press Enter. (Make sure the partition you choose has at least 124MB free.)
7. Windows NT Server Setup asks you to select the type of file system you want on this partition. Highlight "Leave the current file system intact <no changes>," and press Enter.
8. Windows NT Server Setup displays the location where it will install the NT Server files. In the highlighted area, edit the text so that it reads: **\WINNTSRV**. (Don't type in the period at the end.) Then press Enter.
9. Windows NT Server Setup offers to examine your hard disk for corruption. Press Enter to enable this. (This takes a few minutes.)
10. Windows NT Server Setup displays a screen that indicates this portion of Setup is complete. If you have a floppy disk inserted in drive A:, remove it now. Then press Enter to restart your computer and to continue with setup.

Phase 1

1. After your computer reboots and the Windows NT Server Setup dialog box finally appears, click Next to continue.
2. Type in your name, press Tab, and then type in the name of your organization. Click Next to continue.
3. Type in the ten-digit CD key number from the back of your Windows NT Server compact disc case (press Tab after you enter the first three digits). Click Next to continue.
4. Select a Licensing Mode for the server. Select "Per Server for:" and enter the number of client licenses you purchased. Click Next to continue.
5. When prompted to type in a name for your computer, type **PDCMAINOFFICE**. Click Next to continue.
6. Select Primary Domain Controller in the Server Type window. Click Next to continue.
7. Type **password** when prompted to enter an administrator password. Press Tab. Confirm the password by retyping it. Click Next to continue.
8. Windows NT Server Setup asks you if you want to create an Emergency Repair Disk. Accept the Yes default. Click Next to continue.

9. Windows NT Server Setup displays a screen prompting you to Select Components. Add any components that you want to install, but do *not* deselect any components that are selected by default. Click Next to continue.

Phase 2

1. Windows NT Server Setup displays a window indicating that Phase 2, Installing Windows NT Networking, is about to begin. Click Next to continue.
2. Accept the default check in the box next to "Wired to the network." Click Next to continue.
3. Accept the default check in the box next to "Install Microsoft Internet Information Server." Click Next to continue.
4. Windows NT Server Setup displays the Network Adapters box. Click Start Search. Your network adapter should then appear in the Network Adapters box.

   If your network adapter did not appear, click Select from list. If your network adapter is shown in the list, highlight it and click OK.

   If your network adapter is not on the list, and you have a driver disk from its manufacturer, highlight any network adapter and click Have Disk. Setup then prompts you to insert this disk. Insert the disk and click OK. Highlight your network adapter from the list and click OK.

   You should now have your network adapter displayed in the Network Adapters box. Click Next to continue.
5. Windows NT Server Setup displays the Network Protocols list box. Deselect NWLink IPX/SPX Compatible Transport. Ensure that the TCP/IP Protocol is the only protocol selected (it will have a gray check in the check box). Click Next to continue.
6. Windows NT Server Setup displays the Network Services list box. Accept all of the defaults selected in this window. Click Next to continue.
7. Click Next to continue and to have Setup install the selected components.
8. Setup prompts you to enter your network adapter card settings. (This screen may not appear for some network adapters.) Verify that the settings shown match the ones that you used when you installed and configured your network adapter. Make changes only as needed. Click Continue to continue.
9. A TCP/IP Setup warning screen appears. If you are on a network that has a DHCP server, click Yes. Otherwise, click No.

10. The Microsoft TCP/IP Properties dialog box appears if you clicked No in the previous step. *If you are on a network that uses TCP/IP, or if you are connected to the Internet, obtain an IP address, subnet mask, and default gateway from your network administrator.* Otherwise, type an IP address of: **192.168.59.6** and a subnet mask of: **255.255.255.0**.

Do *not* use this IP address if you are on a network that uses TCP/IP, or if you are connected to the Internet.

11. Leave the Default Gateway blank. Click OK to continue.
12. Windows NT Server Setup displays a screen showing network binding information. Click Next to continue.
13. Click Next to start the network.
14. Windows NT Server Setup prompts you enter a domain name. Type **MAINOFFICE** as your domain name. Click Next to continue.

Phase 3

1. Click Finish to continue the setup process.
2. Accept the defaults selected in the Microsoft Internet Information Server 2.0 Setup dialog box. Click OK to continue.
3. Click Yes to create the directory.
4. Accept the default directories in the Publishing Directories dialog box by clicking on OK.
5. Click Yes to create the directories.
6. Click OK in the Microsoft Internet Information Server 2.0 Setup dialog box.
7. Click SQL Server in the Install Drivers dialog box to highlight it. Click OK to continue.
8. In the drop-down list box under the Time Zone tab, click your time zone to highlight it. Optionally, you may also click the Date & Time tab and set the correct date and time. When you are finished click Close to continue.
9. Setup displays a screen indicating that it has found your video display adapter. Click OK in the Detected Display dialog box to continue.
10. Adjust the display settings to suit your preferences. Click Test. The Testing Mode dialog box appears. Click OK to test. When the Testing Mode dialog box reappears, click Yes if you saw the test bitmap. When the Display Settings dialog box appears, click OK to continue. Click OK in the Display Properties dialog box to complete the installation. (This takes a few minutes.)
11. When prompted, label and insert a blank 3.5-inch floppy disk into drive A:. Setup formats and makes this disk into your Emergency Repair Disk. Click OK to continue. (This takes a couple of minutes.)

12. Windows NT Setup displays a window indicating that Windows NT 4.0 is successfully installed. Remove your newly created Emergency Repair Disk from drive A: (and save it for future use). Also remove the compact disc from your CD-ROM drive. Then click Restart Computer to reboot and start Windows NT Server. The setup is complete. Continue on to Part 2.

Part 2: Configuring a one-way trust

In this section you create users in the MAINOFFICE domain, and configure the LAB domain to trust the MAINOFFICE domain.

Boot both of your computers to Windows NT Server. Log on as Administrator to each one.

Perform the following steps on the computer you named PDCMAINOFFICE (the second computer):

1. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
2. Select User ≥ New User.
3. In the New User dialog box, type the following bolded information in the appropriate text boxes:

   User name: **CarmenM**

   Full name: **Carmen Martinez**

   Description: **Corporate Sales Manager**

   Password: **password**

   Confirm password: **password**

   Clear the check box next to User Must Change Password at Next Logon. Select the check box next to Password Never Expires. Click the Add command button.
4. In the New User dialog box, type the following bolded information in the appropriate text boxes:

   User name: **HansS**

   Full name: **Hans Schmidt**

   Description: **Corporate Accounting Manager**

   Password: **password**

   Confirm password: **password**

   Clear the check box next to User Must Change Password at Next Logon. Select the check box next to Password Never Expires. Click the Add command button. Click the Close command button.
5. In the User Manager dialog box, select Policies ≥ Trust Relationships.

6. In the Trust Relationships dialog box, click the Add command button next to the Trusting Domains list box (this is the text box at the bottom of the dialog box).
7. In the Add Trusting Domain dialog box, type the following bolded information in the appropriate text boxes:

   Trusting domain: **LAB**

   Initial password: **password**

   Confirm password: **password**

   Click OK.
8. In the Trust Relationships dialog box, PDCLAB appears in the Trusting Domains list box. Click the Close command button.
9. Exit User Manager for Domains.

Perform the following steps on the computer named PDCLAB (the first computer):

1. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager for Domains.
2. In the User Manager for Domains dialog box, select Policies ➪ Trust Relationships.
3. In the Trust Relationships dialog box, click the Add command button next to the Trusted Domains list box (this is the list box toward the top of the dialog box).
4. In the Add Trusted Domain dialog box, type the following bolded information in the appropriate text boxes:

   Domain: **MAINOFFICE**

   Password: **password**

   Click OK.
5. A message appears, indicating that a trust relationship with MAINOFFICE has been successfully established. Click OK.
6. In the Trust Relationships dialog box, notice that MAINOFFICE appears in the Trusted Domains list box. Click the Close command button.
7. Exit User Manager for Domains. Continue on to Part 3.

Part 3: Testing a one-way trust

In this section you verify that the LAB domain trusts the MAINOFFICE domain by assigning a user from the MAINOFFICE domain permissions to a printer in the LAB domain, and by logging on to the PDC in the LAB domain by using a user account from the MAINOFFICE domain. In addition, you attempt to log on to the

PDC in the MAINOFFICE domain by using a user account from the LAB domain, but fail, verifying that the MAINOFFICE domain does *not* trust the LAB domain.

Perform these steps on the computer named PDCLAB (the first computer):

1. Select Start ➢ Settings ➢ Printers.
2. In the Printers dialog box, highlight the printer you created in Lab 6.8. Select File ➢ Properties.
3. In the printer's Properties dialog box, click the Security tab.
4. On the Security tab, click the Permissions command button.
5. In the Printer Permissions dialog box, click the Add command button.
6. In the Add Users and Groups dialog box, click the down arrow in the List Names From drop-down list box. Select MAINOFFICE from the list that appears. Click the Show Users command button. Scroll down the list in the Names list box and highlight CarmenM. Click the Add command button. Click OK.
7. In the Printer Permissions dialog box, notice that MAINOFFICE\CarmenM now appears in the Name list box. She has permissions to print to the printer. (You have just verified that the LAB domain trusts the MAINOFFICE domain by successfully assigning CarmenM, a user in the MAINOFFICE domain, permissions to a printer in the LAB domain.) Click OK.
8. In the printer's Properties dialog box, click OK.
9. Close the Printers dialog box.
10. Select Start ➢ Shut Down.
11. In the Shut Down Windows dialog box, select the radio button next to "Close all programs and log on as a different user." Click the Yes command button.
12. Press Ctrl + Alt + Delete to log on.
13. Click OK in the Important Notice dialog box.
14. In the Logon Information dialog box, type the user name, **HansS,** and the password, **password**. Select MAINOFFICE in the Domain drop-down list box. Click OK.
15. If the Welcome to Windows NT screen appears, click the Close command button.
16. Because HansS, a user in the MAINOFFICE domain, is successful in logging on at the PDC in the LAB domain, you have verified that the LAB domain trusts the MAINOFFICE domain.
17. Select Start ➢ Shut Down.
18. In the Shut Down Windows dialog box, select the radio button next to "Close all programs and log on as a different user." Click the Yes command button.

Perform the following steps on the computer named PDCMAINOFFICE (the second computer):

1. Select Start ➪ Shut Down.
2. In the Shut Down Windows dialog box, select the radio button next to "Close all programs and log on as a different user." Click the Yes command button.
3. Press Ctrl + Alt + Delete to log on.
4. In the Logon Information dialog box, click the down arrow in the Domain drop-down list box. Notice that only the MAINOFFICE domain is listed. (This is because the MAINOFFICE domain does *not* trust the LAB domain.) Click the Cancel command button. You have verified that the MAINOFFICE domain does *not* trust the LAB domain. Continue to Part 4.

Part 4: Configuring a two-way trust

In this section you configure the MAINOFFICE domain to trust the LAB domain. (This completes the creation of a two-way trust between the LAB and MAINOFFICE domains.)

Perform these steps on the computer named PDCLAB (the first computer):

1. Press Ctr + Alt + Delete to log on.
2. Click OK in the Important Notice dialog box.
3. In the Logon Information dialog box, type in a user name of **Administrator**, a password of **password**, and select the LAB domain from the Domain list box. Click OK.
4. Select Start ➪ Programs ➪ Administrative Tools (Common) ➪ User Manager for Domains.
5. In the User Manager dialog box, select Policies ➪ Trust Relationships.
6. In the Trust Relationships dialog box, click the Add command button next to the Trusting Domains list box (the list box toward the bottom of the dialog box).
7. In the Add Trusting Domain dialog box, type the following bolded information in the appropriate text boxes:

   Trusting domain: **MAINOFFICE**

   Initial password: **password**

   Confirm password: **password**

   Click OK.
8. In the Trust Relationships dialog box, notice that MAINOFFICE appears in the Trusting Domains list box. Click the Close command button.

9. Exit User Manager for Domains.

Perform the following steps on the computer named PDCMAINOFFICE (the second computer):

1. Press Ctrl + Alt + Delete to log on.
2. In the Logon Information dialog box, type in a user name of **Administrator**, a password of **password**, and select the MAINOFFICE domain. Click OK.
3. Select Start ≥ Programs ≥ Administrative Tools (Common) ≥ User Manager for Domains.
4. In the User Manager dialog box, select Policies ≥ Trust Relationships.
5. In the Trust Relationships dialog box, click the Add command button next to the Trusted Domains list box (this list box is located near the top of the dialog box).
6. In the Add Trusted Domain dialog box, type in a domain of **LAB** and a password of **password**. Click OK.
7. After a few moments a dialog box appears, indicating that a trust relationship with the LAB domain has been successfully established. Click OK.
8. In the Trust Relationships dialog box, notice that the LAB domain appears in the Trusted Domains list box. The MAINOFFICE domain is now configured to trust the LAB domain. Click the Close command button.
9. In the User Manager dialog box, select Policies ≥ User Rights.
10. In the User Rights Policy dialog box, select Log on locally from the Right drop-down list box. Click the Add command button.
11. In the Add Users and Groups dialog box, double-click the Everyone group in the Names list box. Click OK. (This step enables all users from both the LAB and MAINOFFICE domains to log on locally to this computer.)
12. In the User Rights Policy dialog box, click OK.
13. Exit User Manager for Domains. Continue to Part 5.

Part 5: Testing a two-way trust

In this section, you verify that the MAINOFFICE domain trusts the LAB domain by logging on to the PDC in the MAINOFFICE domain by using a user account from the LAB domain. (You already verified that the LAB domain trusts the MAINOFFICE domain.)

Perform the following steps on the computer named PDCMAINOFFICE (the second computer):

1. Select Start ➪ Shut Down.
2. In the Shut Down Windows dialog box, select the radio button next to "Close all programs and log on as a different user." Click the Yes command button.
3. Press Ctrl + Alt + Delete to log on.
4. In the Logon Information dialog box, type in a user name of **MikeCo**, a password of **newuser**, and select the LAB domain. Click OK.
5. A Logon Message appears, indicating that you are required to change your password at first logon. Click OK.
6. In the Change Password dialog box, type in a new password of **password** and confirm the new password. Click OK.
7. A Change Password dialog box appears, indicating that your password has been changed. Click OK.
8. If a Welcome to Windows NT dialog box appears, click the Close command button.

   Because you were able to log on successfully to the PDC in the MAINOFFICE domain by using a user account from the LAB domain (MikeCo), you verified that the MAINOFFICE domain trusts the LAB domain.

Lab 10.16 *Planning a Directory Services architecture*

Enterprise

The objective of this lab is to give you hands-on experience in planning a Directory Services architecture and trust relationships in given situations.

In each of the following exercises, your job is to:

1. Plan the appropriate Directory Services architecture for the given scenario (single domain model, single master domain model, multiple master domain model, or complete trust domain model).
2. Plan the appropriate trust relationships for the scenario.

Exercise 1 An international marketing firm called Worldwide Promotions, Inc., based in New York City, is planning to roll out Windows NT 4.0 in all of its offices worldwide.

Table 10-4 lists Worldwide Promotions' offices, and the number of users at each office.

TABLE 10-4 WORLDWIDE PROMOTIONS, INC.

OFFICE LOCATION	*NUMBER OF USERS*
New York City	500
Paris	150
London	100
Seattle	100
Mexico City	50
Total Users	900

A Windows NT network will be installed at each location, and all offices will be connected to the New York City office via a high-speed, digital leased line. The company plans to standardize by using Windows NT Server on all of its servers, and by using Windows NT Workstation on all client computers.

The company's Management Information Systems (MIS) department is located in the New York City office, and wants to manage all of the user accounts in all five locations. On-site network managers at each of the other four offices will manage the security for local network resources at their own respective offices.

Worldwide Promotions maintains a critical database in the New York City office that all users from all locations need to be able to access.

1. Which Directory Services architecture would you choose for this situation?
2. What trust relationships would you use in this situation, if any?

(You might want to draw out your Directory Services architecture design and trust relationships on a piece of scratch paper.)

Exercise 2 An international import company called Import International, Ltd., based in Toronto, Canada, is planning to roll out Windows NT 4.0 in all of its offices worldwide.

Table 10-5 lists Import International, Ltd.'s offices, and the number of users at each office.

TABLE 10-5 IMPORT INTERNATIONAL, LTD.

OFFICE LOCATION	*NUMBER OF USERS*
Toronto	9,000
Los Angeles	8,000
Tokyo	7,000
Rio de Janeiro	6,000
Miami	6,000
Bombay	3,000
Johannesburg	3,000
Sydney	2,000
Hong Kong	1,000
Bangkok	1,000
Total Users	46,000

High-speed, digital leased lines connect the locations, as shown in Figure 10-22.

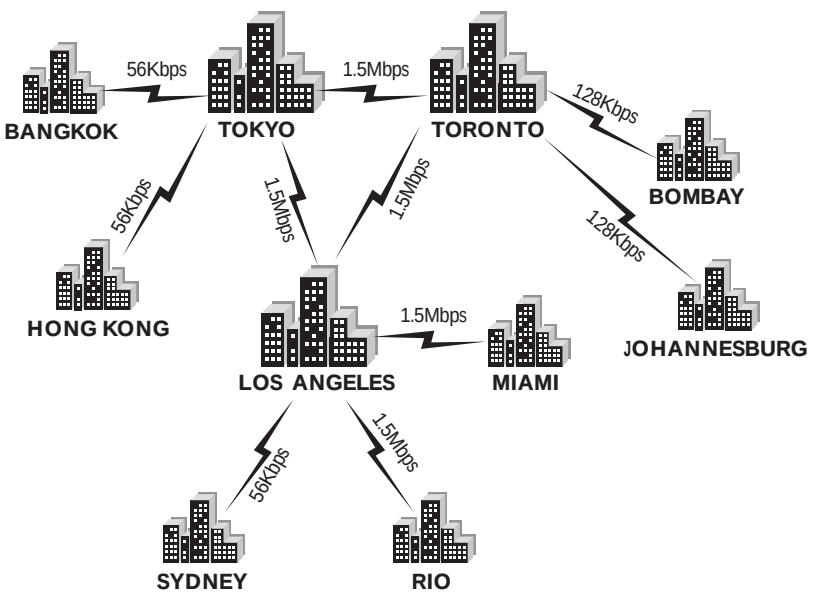


FIGURE 10-22 **Leased lines connecting Import International, Ltd.'s ten offices**

A Windows NT network will be installed at each location. Import International plans to standardize by using Windows NT Server on all of its servers, and by using Windows NT Workstation on all client computers.

The company's Data Processing and Computer Services department is located in the Toronto office and wants to manage all of the user accounts for all ten locations. On-site network managers at each of the other nine offices will manage the security for local network resources at their own respective offices.

Personnel travel frequently and log on to computers in various offices when traveling. Users must be able to log on using a single user account from a computer in any Import International office.

Import International maintains three critical databases: one in Toronto, one in Los Angeles, and one in Tokyo. All users from all locations need to be able to access all three of these databases.

1. Which Directory Services architecture would you choose for this situation?
2. What trust relationships would you use in this situation, if any?

(You might want to draw out your Directory Services architecture design and trust relationships on a piece of scratch paper.)

For answers to this lab see Appendix D.