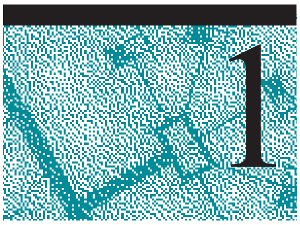
The following document is Chapter 1 of the Concepts and Planning book that is included in the online documentation set that is included on the compact disc and is also available in book format.

CHAPTER 1

Managing Windows NT Server Domains



This chapter presents an overview of the various components of a Microsoft® Windows NT® Server network. The relationships between computers and domains, users and domains, user groups and domains, and between multiple domains are explained, providing a general understanding of how all the pieces fit together.

This chapter introduces the basic concepts (including domain management tasks) required for administering a Windows NT Server domain. For detailed information on these subjects, see the references to the Windows NT Server documentation set that are mentioned throughout. For information on procedures, see online Help.

Directory Services and Domains

Modern network server operating systems track user accounts in a secure and replicated database called a *directory*. The operating system services that facilitate the use of this database are called *directory services*.

The Windows NT Server *domain* is the administrative unit of Windows NT Server Directory Services. Within a domain, an administrator creates one user account for each user. The account includes user information, group memberships, and security policy information.

Through the domain structure, Microsoft Windows NT Server Directory Services provide several key advantages:

- Single user logon

  Network users can connect to multiple servers with a single network logon. Directory Services extend this logon to all Windows NT Server services and server applications.

- Centralized network administration

  A centralized view of the entire network from any workstation on the network provides the ability to track and manage information on users, groups, and resources in a distributed network. This single point of administration for multiple servers simplifies the management of a Windows NT Server-based network.

- Universal access to resources

> One domain user account and password is all the user needs to use available resources throughout the network. Through directory services, account validation is extended to allow seamless user access to multiple network domains.

Although Windows NT Server Directory Services are invisible to you, they respond when you use Windows NT Server commands to manage the user and group accounts in your domain.

Network Building Blocks–An Overview

An understanding of domain components and how they interact is critical to making appropriate decisions when using the domain structure to implement Windows NT Server Directory Services features. The following section provides a brief explanation of the key components and functionality of a Windows NT Server domain.

Windows NT Server Domains

A *domain* is a logical grouping of network servers and other computers that share common security and user account information. Within domains, administrators create one user account for each user. Users then log on once to the domain, not to the individual servers in the domain.

A domain is simply the administrative unit of Windows NT Server Directory Services. The term domain does not refer to a single location or specific type of network configuration. Computers in a single domain can share physical proximity on a small local area network (LAN) or can be located in different corners of the world, communicating over any number of physical connections, including dial-up lines, ISDN, fiber, Ethernet, Token Ring, frame relay, satellite, and leased lines.

Directory Database

The *directory database* stores all security and user account information for a domain. (Other Windows NT documents may refer to the directory database as the “Security Accounts Manager (SAM) database”). The master copy of the directory database is stored on one server and is replicated to backup servers and then synchronized on a regular basis to maintain centralized security. When a user logs on to a domain, Windows NT Server software checks the user name and password against the directory database.

Primary and Backup Domain Controllers

Within a domain, *domain controllers* manage all aspects of user-domain interactions. Domain controllers are computers running Windows NT Server that share one directory database to store security and user account information for the entire domain; they comprise a single administrative unit. Domain controllers use the information in the directory database to authenticate users logging on to domain accounts. There are two types of domain controllers:

- The *primary domain controller* (PDC) tracks changes made to domain accounts. Whenever an administrator makes a change to a domain account, the change is recorded in the directory database on the PDC. The PDC is the only domain server that receives these changes directly. A domain has one PDC.

- A *backup domain controller* (BDC) maintains a copy of the directory database. This copy is synchronized periodically and automatically with the PDC. BDCs also authenticate user logons, and a BDC can be promoted to function as the PDC. Multiple BDCs can exist in a domain.

You create a domain when you install Windows NT Server on a computer and designate that computer as the PDC. There can be as many BDCs as needed in a domain to share the load of authenticating network logons. In a small organization, a PDC and a single BDC in one domain might be all that is required. For information about promoting and demoting domain controllers, see "Promoting and Demoting Domain Controllers" later in this chapter.

Benefits of Domains

Grouping computers into domains provides two main benefits to network administrators and users. Most importantly, the controller servers in a domain form a single administrative unit, sharing security and user account information: Administrators have to manage only one account for each user, and each user needs to use (and remember the password of) only one account. By extending the administrative unit from individual servers to an entire domain, Windows NT Server saves administrators and users time and effort.

The second benefit of domains is user convenience: When users browse the network for available resources, they see the network grouped into domains, rather than seeing all the servers and printers on the whole network at once. This benefit of domains is identical to the Microsoft Windows® for Workgroups and Windows 95 concept of a workgroup.

User Access to Domain Resources

Windows NT Server provides you with many ways to control the actions of users while still letting them use the resources they need. The basis of Windows NT security is that all resources and actions are protected by *discretionary access control*. You can allow some users to connect to a resource or perform an action while preventing others from doing so. For example, you can set different permissions on different files in the same directory.

Rather than being an add-on component, Windows NT Server security is built into the operating system. You can keep files and other resources secure both from users working at the computer where the resource is located and from users connecting to the resource over the network. Security is even provided on basic system functions, such as setting a computer's system clock.

Together, the user account, user rights, and resource permissions provide resource access and restrictions appropriate to each user.

User Accounts Allow Access to Domain Resources

An individual who participates in a domain must have a *user account* to log on to the network and use domain resources such as files, directories, and printers.

An administrator creates a user account by assigning a user name to an account, specifying the user's identification data, and defining the user's rights on the system.

Windows NT Server then assigns a *unique security identifier* (SID) to the new account.

For information about user rights and creating user accounts, see Chapter 2, "Working With User and Group Accounts."

For information about how to create user accounts, see "Creating a New User Account" in User Manager for Domains Help.

User Rights Control Actions by the User

User rights are rules that determine the actions a user can perform on domain controllers, workstations, or member servers. In addition, they control whether a user can log on to a computer directly (locally) or over the network, add users to a workstation or domain group, delete users, and so on. When you assign user rights, those rights apply either to all domain controllers on a domain (what users can do on any PDC or BDC) or to a computer running Windows NT Workstation or a computer running Windows NT Server as a member server (what users can do on that particular computer).

Predefined (built-in) groups have sets of user rights already assigned. Administrators usually assign user rights by adding a user account to one of the predefined groups or by creating a new group and assigning specific user rights to that group. Users who are subsequently added to a group automatically gain all user rights assigned to the group account. Individual users can be given specific user rights; however, most administrators prefer to control actions on a group basis rather than on an individual user basis.

For information about assigning rights to groups, see Chapter 2, "Working With User and Group Accounts."

Permissions Control Access to Domain Resources

Permissions are rules that regulate which users can use objects (such as directories, files, and printers) and in what manner. The owner of an object sets the permissions on the object. Similar to user rights, permissions on an object apply to each member of a group to whom the permissions are granted.

For information about setting permissions on objects, see Chapter 4, "Managing Shared Resources and Resource Security."

Trust Relationships

Although small organizations can store accounts and resources in a single domain, large organizations typically establish multiple domains. With multiple domains, accounts are usually stored in one domain and resources in another domain or domains.

Windows NT Server Directory Services provide security across multiple domains through *trust relationships*. A trust relationship is a link that combines two domains into one administrative unit that can authorize access to resources on both domains.

There are two types of trust relationships:

- In a *one-way trust relationship*, one domain trusts the users in the other domain to use its resources. More specifically, one domain trusts the domain controllers in the other domain to validate user accounts to use its resources. The resources that become available are in the *trusting* domain, and the accounts that can use them are in the *trusted* domain. However, if user accounts located in the trusting domain need to use resources located in the trusted domain, that situation requires a two-way trust relationship.

- A *two-way trust relationship* is two one-way trusts: each domain trusts user accounts in the other domain. Users can log on from computers in either domain to the domain that contains their account. Each domain can have both accounts and resources. Global user accounts and global groups can be used from either domain to grant rights and permissions to resources in either domain. In other words, both domains are trusted domains.

Note

> Using resources located on any domain, trusting or otherwise, is always subject to permissions associated with the resources.

For information about resource permissions, see Chapter 4, "Managing Shared Resources and Resource Security."

For information about creating trust relationships, see "Administering Trust Relationships" later in this chapter.

For information about planning and managing trust relationships, see the *Windows NT Server Resource Kit* version 4.0.

For information about how to create a trust relationship, see "Adding a Trusting Domain" and "Adding a Trusted Domain" in User Manager for Domains Help.

Grouping Users With Similar Needs

Administrators typically group users according to the types and degrees of network access their jobs require. For example, most accountants working at a certain level will probably need access to the same servers, directories, and files. By using *group accounts*, administrators can grant rights and permissions to multiple users at one time. Other users can be added to an existing group account at any time, instantly gaining the rights and permissions granted to the group account.

There can be two types of group accounts:

- A *global group* consists of several user accounts from one domain that are grouped together under one group account name. A global group can contain user accounts from only a single domain—the domain where the global group was created. "Global" indicates that the group can be granted rights and permissions to use resources in multiple (global) domains. A global group can contain only user accounts and can be created only on a domain and not on a workstation or member server.
- A *local group* consists of user accounts and global groups from one or more domains, grouped together under one account name. Users and global groups from outside the local domain can be added to the local group only if they belong to a trusted domain. "Local" indicates that the group can be granted rights and permissions to use resources in only a single (local) domain. A local group can contain users and global groups, but it cannot contain other local groups.

When working with groups, keep the following in mind:

- Global groups are the most efficient way to add users to local groups.
- Global groups can be added to local groups in the same domain, trusting domains, or to computers running Windows NT Workstation or Windows NT Server as a member server in the same or a trusting domain.
- Although a global group can be granted permissions and rights in its own domain, it is best to grant rights and permissions to local groups and use global groups to add user accounts from account domains (trusted) to resource domains (trusting).

Built-in Local Groups and User Rights

Windows NT Server domain controllers contain built-in local groups that determine what users can do on the domain when logged on to domain controllers. Computers running Windows NT Workstation and member servers running Windows NT Server have built-in local groups that determine what users can do on the local computer.

The built-in local groups on domain controllers give administrators a significant head start in managing domain security. Each built-in local group has a predetermined set of rights, which automatically apply to each user account that is added to the group.

The rights assigned to the built-in groups on a domain controller provide sets of abilities for domain users, as characterized by the group names: Administrators, Account Operators, Server Operators, Backup Operators, Print Operators, Users, Guests, and Replicators.

The built-in local groups for workstations and member servers are Administrators, Backup Operators, Power Users, Users, Guests, and Replicators.

For information about the abilities of built-in global and local groups, see Chapter 2, “Working With User and Group Accounts.”

Computers that Can Participate in Domains

In addition to primary and backup domain controllers, a domain contains workstation computers running Windows NT Workstation and computers running Windows NT Server that are not domain controllers (member servers). LAN Manager 2.*x* servers and clients can also participate in a Windows NT Server domain.

Computers Running Windows NT Workstation

For each computer running Windows NT Workstation on your network, you specify whether to have the workstation participate in a domain or in a *workgroup*. A workgroup is a collection of computers that can view each others’ directories over the network but do not share a common directory database. Workgroup members log on to workstation accounts only and share resources between computers in the workgroup. In most cases, you will want each workstation to participate in a domain.

For information about domain interactions with workgroup computers, see “Computers that Can Interact with Domain Computers” later in this chapter.

Member Servers

Computers running Windows NT Server can be configured as *member servers* that do not store copies of the directory database, and therefore do not authenticate accounts or receive synchronized copies of the directory database. These servers are used to run applications dedicated to specific tasks, such as managing print or file servers or high-volume tasks such as running database applications. Member servers can take advantage of several features:

- Support of up to 256 simultaneous Remote Access Service (RAS) connections
- Advanced fault tolerance (disk mirroring/duplexing, RAID 5)
- Macintosh access to Windows NT Server File and Print Services
- Remoteboot server support for MS-DOS and Windows 3.*x* clients

To configure a member server, during installation of Windows NT Server select the **Stand Alone** option for the server type.

You might want to configure a computer as a member server in the following situations:

- If the server performs extremely time-critical tasks and you do not want it to spend time authorizing domain logon attempts or receiving synchronized copies of the domain's directory database. Examples include servers running Microsoft Systems Network Architecture (SNA) Server, Remote Access Service (RAS) servers, and file and print servers.
- If you want the server to have a different administrator or different user accounts from the rest of the servers in a domain. For example, you can have a person dedicated to administering a Microsoft SQL Server database. If you set up the computer running Microsoft SQL Server as a member server, you can allow that person to administer the Microsoft SQL Server database but not have control over the domain's directory database or its other servers.

Member servers can participate in a domain, although participation is not required.

- A member server that participates in a domain does not store a copy of the directory database, but permissions can be set on the server's resources that allow users to connect to the server and use resources. Because the computer itself is a member of the domain, it maintains a trust relationship with the domain and with other domains that the domain trusts. Therefore, resource permissions can be granted for domain global groups and users as well as for local groups and users.
- A member server that does not participate in a domain has only its own database of users, and it processes logon requests by itself. It does not share account information with any other computer and cannot provide access to domain accounts. Only user accounts created at the server itself can be logged on to or given rights and permissions for using the server's resources. These servers have the same types of built-in user and local group accounts as computers running Windows NT Workstation rather than the types of built-in group accounts on Windows NT Server domain controllers.

For information about choosing a server type and setting up a RAS server, see *Windows NT Server Start Here*.

For information about fault tolerance, see Chapter 7, "Protecting Data" and the *Windows NT Server Resource Kit* version 4.0.For information about Services for Macintosh, see the *Windows NT Server Networking Supplement.*

For information about setting up a Remoteboot server, see *Windows NT Server Start Here*.

For detailed information about Windows NT Server Remoteboot Service, see Chapter 11, "Managing Client Administration," and the *Windows NT Server Resource Kit* version 4.0.

LAN Manager 2.x Servers

LAN Manager 2.*x* servers can function in a domain that has a primary domain controller running Windows NT Server. LAN Manager 2.*x* servers can be used as backup domain controllers but cannot be the primary domain controller of a Windows NT Server domain because LAN Manager 2.*x* does not support all the types of information contained in Windows NT Server accounts.

LAN Manager 2.*x* BDCs can validate logon attempts from computers running Windows for Workgroups, Windows 95, or LAN Manager 2.*x* workstation software but cannot validate logon attempts from computers running Windows NT Workstation. (For this reason, don't rely solely on LAN Manager 2.*x* servers as your only BDCs in a Windows NT Server domain.)

Note

LAN Manager 2.*x* BDCs cannot be promoted to primary domain controller of a Windows NT Server domain.

Windows NT Computer Accounts

Each computer running Windows NT Workstation and Windows NT Server that participates in a domain has its own account in the directory database, called a *computer account*. A computer account is created when the computer is first identified to the domain during network setup at installation time.

Secure Communications Channel

When a computer running Windows NT Workstation or Windows NT Server logs on to the network, the Net Logon service on the client computer creates a secure communications channel with the Net Logon service on the server. A *secure communications channel* is created when computers at each end of a connection are satisfied that the computer on the other end has identified itself correctly. Computers identify themselves using their computer accounts. When the secure communications channel has been established, a communications session can begin between the two computers.

To maintain security during the communications session, internal trust accounts are set up between the workstation and the server, the PDC and the BDCs, and between domain controllers on either side of an interdomain trust relationship.

Effects of Computer Accounts on Domain Administration

Computer accounts and the secure channels they provide enable administrators to manage workstations and member servers remotely. They also affect the relationship between a workstation and domain servers and between primary and backup domain controllers:

- The computer account is part of an implicit one-way trust relationship between the client computer and the controllers in its domain. Workstations request logon authentication for a user account from a domain server in the same way a server in a trusting domain requests validation from a server in a trusted domain. This trust relationship enables administrators to select a workstation or member server for administration in the same way they select a domain.
- When the computer account is created, the Domain Admins global group is automatically added to the workstation or member server's Administrators local group. Domain administrators can then use Windows NT Server utilities to remotely manage the computer user environment and manage the computer user and group accounts, including adding domain global groups to the computer's local groups. Additionally, domain administrators can perform any functions on the computer itself that are allowed by the Administrators local group.
- For Windows NT Server domain controllers, computer accounts link BDCs with the PDC and pair up trusting and trusted domains. Server trust accounts created while setting up the secure communications channel allow BDCs to get copies of the master directory database from the PDC. Interdomain trust accounts allow domain controllers in a trusted domain to pass authentication of user accounts through to the trusting domain (see "How User Logons Work," later in this chapter).

For information about how to add a computer to a domain, see "Adding a Computer to the Domain" in Server Manager Help and "joining a Windows NT Domain" in Control Panel Help.

Computers that Can Interact with Domain Computers

Windows NT Server has an open networking architecture that allows flexibility in communicating with other network products. Client computers running operating systems other than Windows NT Workstation or Windows NT Server can interact with computers in a Windows NT Server domain. However, they do not have domain computer accounts and therefore do not have Windows NT Workstation logon security. Their users can have user accounts stored in the directory database, but the computer itself does not have logon security that protects access to its own resources.

Computers running Windows NT Server and Windows NT Workstation can also interact with servers and clients running other operating systems. Various protocols and other software that allows interoperability are either included with Windows NT Server or are available separately.

For information about network interoperability, see the *Windows NT Server Networking Supplement*.

Workgroup Computers

A *workgroup* is an organizational unit of computers (not users) that do not belong to a domain. In a workgroup, each computer tracks its own user and group account information and—in contrast to domain controllers—does not share this information with other workgroup computers.

Workgroup members log on to workstation accounts only and can view directories of other workgroup members over the network.

Computers running Windows NT Workstation, Windows NT Server, Windows for Workgroups, or Windows 95 can be configured to participate in either a domain or a workgroup. When setting up one of these computers for networking, you specify a computer name and a workgroup name. If the workgroup name matches a domain name, the computer name appears in the browse list for that domain and can browse computers running Windows NT Server and Windows NT Workstation, whether participating in a domain or a workgroup. To determine whether the computer participates in a domain or a workgroup, during setup you specify that the computer logs on to either a Windows NT Server domain or a workgroup.

For information about installing workgroup computers, see *Windows NT Server Start Here*.

Windows 95 Clients

Windows 95 has built-in accessibility to Windows NT Server networking. Users who have domain accounts can log on to their accounts the same way Windows NT Workstation users do. Windows 95 user account logons can be validated by both Windows NT Server domain controllers and LAN Manager 2.*x* domain controllers.

MS-DOS Clients

If MS-DOS® client computers are running one of the following components, they can share network resources on the respective servers:

- Microsoft Network Client for MS-DOS (version 3.0) enables computers running MS-DOS to interact with domain controllers and computers running Windows NT Workstation.
- Microsoft LAN Manager for MS-DOS (version 2.2) enables computers running MS-DOS to interact with LAN Manager 2.*x* servers and Windows NT Server domain controllers.

Because computers running MS-DOS cannot store user accounts, they don’t participate in domains the way Windows NT computers do. Each computer running MS-DOS usually has a default domain set for browsing. If an MS-DOS user has a domain account, you can set the browsing domain on the user’s computer to be any domain. It doesn’t have to be the domain containing the user’s account.

For information about Microsoft Network Client for MS-DOS and Microsoft LAN Manager for MS-DOS, see the *Windows NT Server Networking Supplement*.

LAN Manager 2.x Servers and Clients

Windows NT Server interoperates with Microsoft LAN Manager 2.*x* systems. MS-DOS, Windows 3.1, and OS/2 computers running LAN Manager workstation software can connect to servers running Windows NT Server. LAN Manager 2.*x* servers (on both OS/2 and UNIX computers) can also work with servers running Windows NT Server—even in the same domain.

Microsoft LAN Manager for OS/2 version 2.2 is a component of Windows NT Server that enables OS/2 version 1.3*x* computers to interact with LAN Manager 2.*x* servers and computers running Windows NT Workstation and Windows NT Server. If an OS/2 version 1.3*x* system is running these components it can share network resources with the respective servers.

For information about LAN Manager domain interoperability, see “How Windows NT Server Domains Work With LAN Manager Domains” later in this chapter.

Novell NetWare

With NWLink protocol software and Gateway Service for NetWare, you can connect to NetWare file and print resources from computers running Windows NT Server. You can also enable a gateway to share NetWare file and print resources with Microsoft networking clients that have no NetWare client software.

In addition, NetWare client computers can connect to file and print resources and server applications on computers running Windows NT Server.

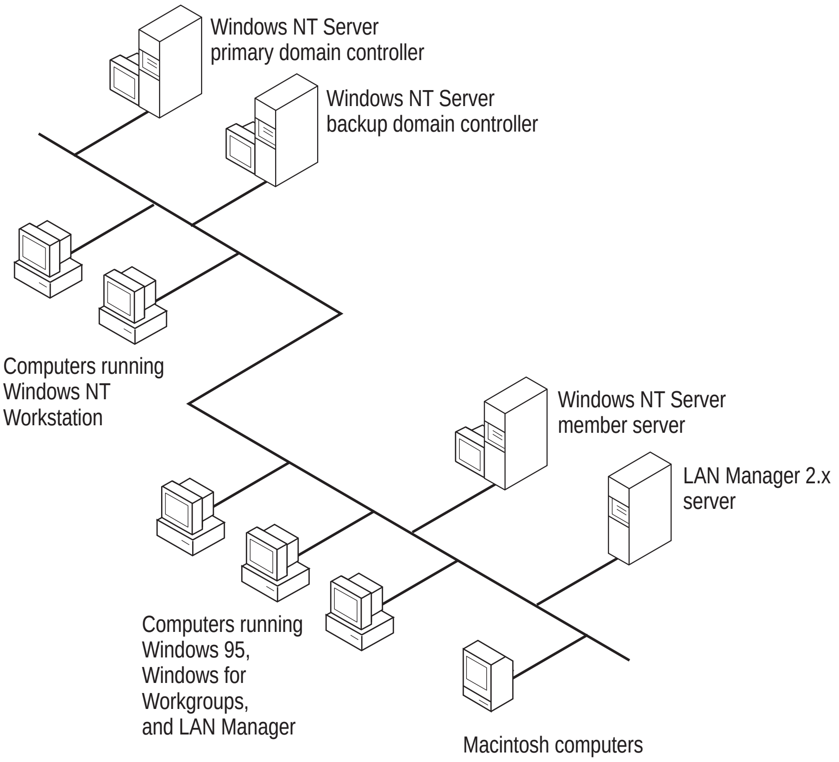
For information about Novell NetWare domain interoperability, see “How Windows NT Server Domains Work With Novell NetWare Domains” later in this chapter.

For information about NWLink protocol and Gateway Service for NetWare, see the *Windows NT Server Networking Supplement*.

Macintosh Clients

Microsoft Windows NT Server Services for Macintosh is a component of Windows NT Server that enables personal computer and Apple Macintosh clients to share files and printers. With Services for Macintosh, one computer running Windows NT Server can act as a server for both Macintosh computers and personal computers, and Macintosh computers can share resources with any client supported by Windows NT Server, such as MS-DOS and LAN Manager client computers.

For information about Windows NT Server Services for Macintosh, see the *Windows NT Server Networking Supplement*.



Windows NT Server domain computers and computers that can interact with them

For more information about network client software installation, see the *Windows NT Server Start Here* book.
For more information about Network Client Administrator, see the *Windows NT Server Networking Supplement*.
For more information about Macintosh workstations and Services for Apple Macintosh, see Chapter 11, “Managing Client Administration.

How User Logons Work

Resources are protected at several levels by different processes, but overall access to a domain or a computer is protected by logon security. This security requires users to identify themselves to the domain or the computer. The user name and password the user types in the **Logon Information** dialog box are checked against the computer directory database if the user is logging on to a user account defined on the computer, or the domain directory database if the user is logging on to a domain user account. Through directory services, authenticated accounts are available for use with all Windows NT Server network services and compatible server applications, such as the BackOffice™ suite of server products. Authentication enables a single user logon in a Windows NT Server domain to additionally use applications such as Microsoft SQL

Server and Microsoft Exchange Server, and network services such as Remote Access Service (RAS), file and print sharing, Internet Information Server (IIS), and Services for Macintosh.

For information about Windows NT Server network services, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

Interactive and Remote Logons

Two logon processes can start logon authentication:

- *Interactive logon* occurs when the user types information in the **Logon Information** dialog box displayed by the computer's operating system. In the **Domain** box, the user selects either the name of a domain or the name of the computer being used for logon, depending on where the user account being logged on to is defined.
- *Remote logon* takes place when a user is already logged on to a user account and makes a network connection to another computer. For example, the user connects to another computer using the **Map Network Drive** dialog box or the **net use** command.

For information about connecting to computers in a non-trusting domain, see "Adding a Local Account" in Chapter 2, "Working With User and Group Accounts."

User Authentication

On a computer running Windows NT Workstation or a member server running Windows NT Server, the Net Logon service processes logon requests for the local computer. On a domain controller, the Net Logon service processes logon requests for the domain.

The Net Logon service initiates the following processes: discovery, secure channel setup, and pass-through authentication.

- *Discovery*: When a computer running Windows NT Workstation or a member server running Windows NT Server starts up, the Net Logon service attempts to locate a domain controller running Windows NT Server in the trusted domain. The Net Logon service on PDCs and BDCs likewise attempts discovery with all trusted domains. Once a domain controller has been discovered, it is used for subsequent user account authentication.
- *Secure communications channel*: The Net Logon services from each computer issue challenges to and receive challenges from each other to verify the existence of their valid computer accounts. When verification is complete, a communication session is set up between the computers and used to pass user identification data.
- *Pass-through authentication*: When a user logs on, the user specifies credentials that identify the user account. When the user account must be authenticated but the computer being used for the logon is not a domain controller in the domain where the user account is defined and is not the computer where the user account is defined, the computer passes the logon information through to a domain controller (directly or indirectly) where the user account is defined.

Pass-through Authentication

Pass-through authentication occurs in the following cases:

- At *interactive logon* when a user logs on to a computer running Windows NT Workstation or a computer running Windows NT Server and the name in the **Domain** box in the **Logon Information** dialog box is not the computer name.

  The logon computer sends the logon request to a domain controller in the domain to which the computer account belongs. The controller first checks the domain name. If the domain name is the domain to which the controller belongs, the controller authenticates the logon credentials against its directory database and passes the account identification information back to the logon computer, allowing the user to connect to resources on both the logon computer and the domain.

Note

If the logon computer is not running Windows NT Workstation or Windows NT Server, domain controller authentication has no effect on the user’s ability to use resources on the logon computer.

If the domain name is not the domain the domain controller belongs to, the domain controller checks to see if the domain is a trusted domain. If so, the domain controller passes the logon request through to a domain controller in the trusted domain. That domain controller authenticates the account user name and password against the domain directory database and passes the account identification information back to the initial domain controller, which sends it back to the logon computer.

If the name in the logon credentials is not the computer name, the name of the domain the computer belongs to, or the name of a domain trusted by the computer's domain, the credentials are considered to belong to an untrusted domain and the interactive logon fails.

- At *interactive logon* when the computer being logged on to is a domain controller but the name in the **Domain** box is not the domain to which the controller belongs.

  The controller checks the domain name to see if it is a trusted domain. (The domain controller does not check for computer name because its directory database contains only domain accounts). If the domain is a trusted domain, the controller passes the logon information to a domain controller in the trusted domain for authentication. If the trusted domain controller authenticates the account, the logon information is passed back to the initial domain controller, and the user is logged on. If the account is not authenticated (is not defined in the trusted domain directory database), the logon fails.

- At *remote logon* (connecting to a computer over the network).

  If the user is logged on to a computer or domain account and then tries to make a network connection to another computer, pass-through authentication proceeds as in interactive logon. The credentials used at interactive logon are used for pass-through authentication unless the user overrides those credentials by typing a different domain or computer name and user name in the **Connect As** box in the **Map Network Drive** dialog box.

  If the user tries to make a network connection to a computer in an untrusted domain, the logon proceeds as if the user were connecting to an account on the remote computer. The computer being connected to authenticates the logon credentials against its directory database. If the account is not defined in the directory database but the Guest account is enabled on the computer being connected to, and if the Guest account has no password set, the user is logged on with guest privileges. If the Guest account is not enabled, the logon fails. For information about the Guest account, see Chapter 2, "Managing User and Group Accounts."

  If the computer being connected to is a BDC in the domain where the user account is defined, but the BDC fails to authenticate the user's password (for example, the password has changed but the BDC is not synchronized at the time the user logs on), the BDC passes the logon request through to the PDC in the same domain.

How Administrators Should Log On

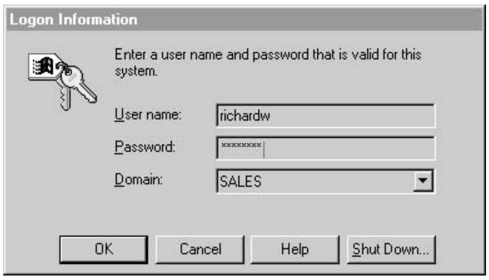
Most network administrators have a dual role. They are both administrators and users of the network. Sometimes they perform network management tasks; at other times they are network users, performing the same tasks as other users.

For this reason, it is a good idea for each administrator to have two domain user accounts. One of these accounts should be in the Administrators local group and is the account the administrator uses when performing network management tasks. The other account should be in the Users local group and is the account the administrator uses at all other times.

If your administrators use two accounts, the network will be more secure. While logged on as a regular user, an administrator cannot accidentally change aspects of the network that only administrators can change. If the administrator introduces a virus, that program will not have the rights of an administrator and cannot modify operating system software.

Logging On at a Computer Running Windows NT Workstation or a Computer Running Windows NT Server as a Member Server

The **Logon Information** dialog box prompts the user for a user name, password, and domain or computer name (**Domain**):



Logon Information

Enter a user name and password that is valid for this system.

User name: richardw

Password: ********

Domain: SALES

User name and **Password** are straightforward; the contents of the **Domain** list depends on whether the computer has a domain computer account.

- If the computer has a domain computer account, the list contains both the computer name and the domain name where the computer account resides, as well as any domains trusted by the computer account's domain; in other words, every domain (including the computer itself) where user accounts can be authenticated.
- If the computer is a member of a workgroup, the list contains only the workstation name (because that is the only place user accounts can be authenticated).

If the computer is a member of a workgroup or a user with a domain account is logging on to an individual computer account, the user selects the computer name—rather than a domain name—in the **Domain** list (in the case of a workgroup computer, a domain name is not available). Then the computer checks its own directory database for the user name and password specified by the user. If a match occurs, the logon is approved and the user's logon information is obtained from the account on the computer.

To log on to a domain, the user selects the name of the domain where the user account resides. This domain is either the same domain as the computer account domain or a domain that is trusted by the computer account domain.

Note

When domains are organized into master user account domains and resource domains, the computer accounts should be stored in a resource domain rather than a user accounts domain, ensuring that the trusted account domain appears in the Domain list.

When the user clicks **OK**, the workstation sends the domain name, user name, and password to a domain controller. The domain controller first checks the domain name and then checks the user name and password against that domain's directory database:

- If the domain name is correct and the user name and password match a domain account, the server notifies the computer that the logon is approved.
- If the domain name is different and the domain controller recognizes the domain as a trusted domain, the controller passes the information to the appropriate domain, which authenticates the logon and sends the information back to the original domain controller.
- If the domain name is different and the domain controller does not recognize the domain, the controller denies domain access.

Cached Logon Information

The first time a user logs on to a domain account from a given computer, a domain controller downloads validated logon information (from the directory database) to the computer. This downloaded information is cached on the computer. On subsequent logons, if a domain controller is not available, the user can log on to the domain account using the cached logon information.

Computers running Windows NT Workstation and Windows NT Server store the information used to authenticate the last several (the default number is ten) users who logged on interactively. The credentials for users who log on to the local computer are also stored in that computer's local directory database.

Logging On at a Windows NT Server Domain Controller

Logging on at a computer running Windows NT Server as a member server is identical to logging on at a computer running Windows NT Workstation, except that servers configured as domain controllers do not maintain a local accounts database separate from the accounts in the directory database. The user must log on to a domain account.

Not everyone with an account in a domain can log on locally at the domain's controller servers. By default, only members of the Administrators, Server Operators, Print Operators, Account Operators, and Backup Operators groups can do so.

For more information about groups and their rights and abilities, see Chapter 2, "Working With User and Group Accounts."

Logging On at Windows 95, Windows for Workgroups, MS-DOS, Macintosh, or LAN Manager 2.x Client Computers

Logons from client computers other than computers running Windows NT Workstation and computers running Windows NT Server as member servers are validated by a domain controller when the user logs on to the network. The extent of the validation is checking that the domain, user name, and password are typed correctly. The client computers do not receive any account information at the workstation that can be cached and used for access to local resources. If domain controllers are unavailable when a user logs on from one of these client computers, the user cannot use network resources that are protected by domain permissions.

For more information about logons and user authentication, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

Deciding on a Domain Model

A *domain model* is a grouping of one or more domains with administration and communications links between them (trust relationships) that are arranged for the purpose of user and resource management.

By properly planning and organizing the domains on your network, you can simplify network administration and ensure that all users can connect to available resources throughout the network. For example, you can set up your domains so that all user accounts and global groups are valid in all domains.

Because one domain can accommodate up to 26,000 users with individual workstations and approximately 250 groups, a single domain is suitable for most applications. To decide how many domains your organization needs, take into account the work structure and number of users. Windows NT Server domain models provide the flexibility needed for different organizations.

In addition, offices can start out with separate domains and can link to each other later or can be added to existing domains.

Your first consideration is the size of your organization because the size of the directory database determines how many domains you need.

Directory Database Size

If you are managing a small or medium organization, you probably do not need to worry about the upper limits of a Windows NT Server domain. However, if you are planning for significant growth, you should keep these numbers in mind.

The limiting factor for the size of a domain is the number of user accounts that can be supported by a single directory database. The maximum recommended size of the directory database file is 40 MB.

A domain consists of user accounts, computer accounts (each computer running Windows NT Workstation or Windows NT Server has a computer account), and group accounts, both built-in and those you create. Each of these objects occupies space in the directory database file. The practical limit for the size of the directory database file depends on the type of computer processor and amount of memory available in the machine being used as the primary domain controller. Microsoft has successfully tested directory database files in excess of 40 MB, and recommends 40 MB as the upper limit. Different types of objects require different amounts of space in the directory database file:

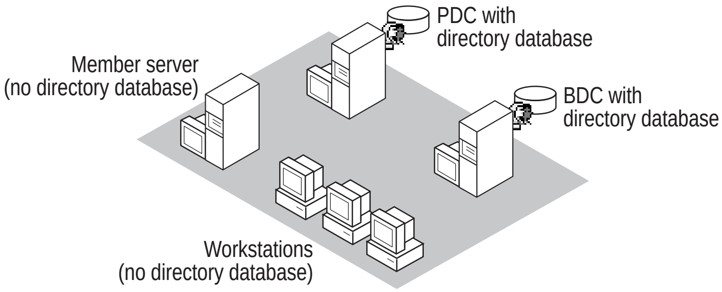
Object	Space Used
User account	1.0K
Computer account	0.5K
Group account	4.0K (average group size = 300 members)

For a single domain, here are some examples of how objects might be distributed:

	User Accounts(1K per account)	Computer Accounts (0.5K per account)	Group Accounts (4K per account)	Total Directory Size
1 workstation per user	2,000	2,000	30	3.12 MB
2 workstations per user	5,000	10,000	100	10.4 MB
2 users per workstation	10,000	5,000	150	13.1 MB
1 workstation per user	25,000	25,000	200	38.3 MB
1 workstation per user	26,000	26,000	250	40 MB
1 workstation per user	40,000	0	0	40 MB

Single Domain Model

In most cases, you can use the single domain model. In this model, the network has only one domain. You create all users and global groups in this domain. The single domain has a PDC with one or more BDCs. The PDC and each BDC can support 2,000 to 2,500 user accounts to validate user logons and provide fault tolerance. The number of accounts could be as high as 5,000, depending on the power of the computer.



Single domain model

The single-domain model is an appropriate choice for organizations that require both centralized management of user accounts and ease of administration. Any member of the Domain Administrators group can administer all network servers and domain accounts on the PDC.

A network can use the single domain model if it has a small enough number of users and groups to ensure good performance (generally up to 26,000). The exact number of users and groups depends on the number of servers in the domain and the hardware of the servers.

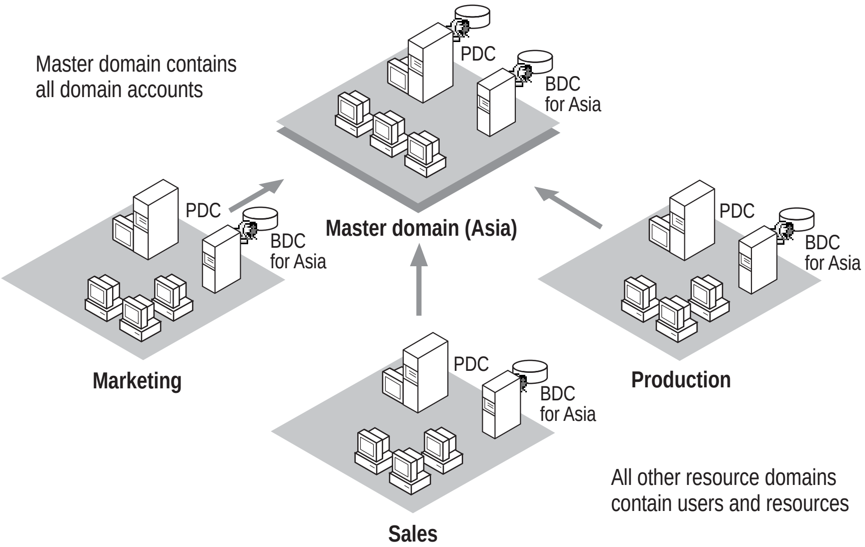
Having a single domain also means that all your network administrators can administer all network servers. Splitting a network into domains enables you to create administrators who can administer only some servers, such as those in their own department.

Single Master Domain Model

When the network does need to be split into domains for organizational purposes, but the network has a small enough number of users and groups, the master domain model might be the best choice. This model gives you both centralized administration and the organizational benefits of multiple domains.

With this model, one domain — the *master domain* — acts as the central administrative unit for user and group accounts. All other domains on the network trust this domain, which means they recognize the users and global groups defined there. If your company has an MIS department that manages your LAN, it is logical to have the MIS department administer the master domain.

All users log on to their accounts in the master domain. Resources, such as printers and file servers, are located in the other domains. Each *resource domain* establishes a one-way trust with the master (account) domain, enabling users with accounts in the master domain to use resources in all the other domains. The network administrator can manage the entire multiple-domain network and its users and resources by managing only a single domain.



Single master domain model

The benefit of the single master domain model is in its flexibility of administration. For example, in a network requiring four domains, it might at first seem most obvious to create four separate user account databases, one for each domain. However, by putting all user accounts in a single directory database on one of the domains and then implementing one-way-trust relationships between these domains, you can consolidate administration of user and computer accounts. You can also administer all resources or delegate these to local administrators. And users need only one logon name and one password to use resources in any of the domains.

This model balances the requirements for account security with the need for readily available resources on the network because users are given permission to resources based on their master domain logon identity.

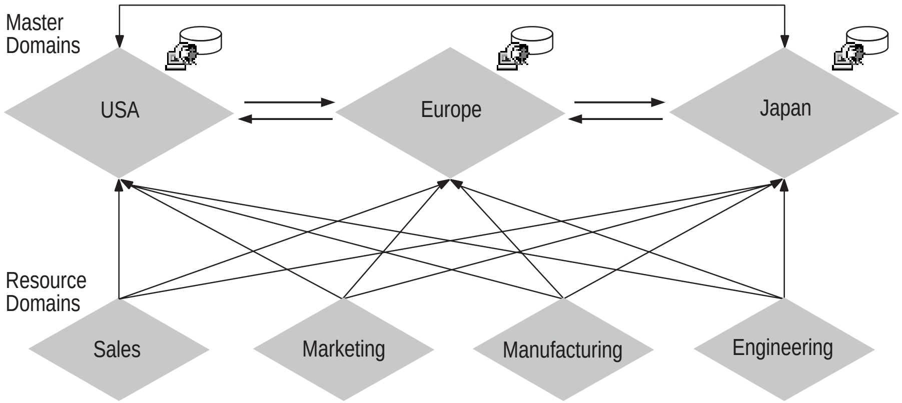
The single master domain model is particularly suited for:

- Centralized account management. User accounts can be centrally managed; add/delete/change user accounts from a single point.
- Decentralized resource management or local system administration capability. Department domains can have their own administrators who manage the resources in the department.
- Resources can be grouped logically, corresponding to local domains.

Multiple Master Domain Model

In the multiple master domain model, there are two or more single master domains. Like the single master domain model, the master domains serve as account domains, with every user and computer account created and maintained on one of these master domains. A company’s MIS groups can centrally manage these master domains. Like the single master domain model, the other domains on the network are called resource domains; they don't store or manage user accounts but do provide resources such as shared file servers and printers to the network.

In this model, every master domain is connected to every other master domain by a two-way trust relationship. Each resource domain trusts every master domain with a one-way trust relationship. The resource domains can trust other resource domains, but are not required to do so. Because every user account exists in one of the master domains, and since each resource domain trusts every master domain, every user account can be used on any of the master domains.



Multiple master domain model. There is one computer account for each user account; therefore, each master domain can contain as many as 26,000 user accounts.

Users log on to the domain that contains their account. Each master domain contains one PDC and at least one BDC.

The multiple master domain model incorporates all the features of a single master domain and also accommodates:

- Organizations of more than 40,000 users. The multiple master domain model is scaleable to networks with any number of users.
- Mobile users. Users can log on from anywhere in the network, anywhere in the world.
- Centralized or decentralized administration.
- Organizational needs. Domains can be configured to mirror specific departments or internal company organizations.
- BDCs can be distributed between sites to facilitate LAN-WAN interactions.

Managing Domains

When you have established one or more domains, you use Windows NT Server utilities to perform required domain management tasks:

- Promoting and demoting domain controllers
- Synchronizing backup domain controllers with the primary domain controller
- Synchronizing all domain servers
- Adding, removing, and renaming domain computers
- Managing domain security, including account policy, audit policy, and trust relationships (with multiple domains)

For information about setting up domain controllers, see *Windows NT Server Start Here*.

For information about managing trust relationships, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

For information about synchronizing domain servers, see “Directory Database Synchronization” later in this chapter.

Promoting and Demoting Domain Controllers

In addition to the primary domain controller (PDC), you should have one or more backup domain controllers (BDCs) per domain.

If the PDC becomes unavailable, a BDC can be promoted to primary domain controller, and the domain continues to function. In such a scenario, the following rules take effect:

- When a BDC is promoted to a PDC, an up-to-date copy of the domain’s directory database is replicated from the old PDC to the new one, and the old PDC is demoted to a BDC.
- If a BDC is promoted to PDC while the existing PDC is unavailable (for example, while it is being repaired), and if the former PDC later returns to service, you must demote the former PDC to BDC. Until it is demoted to a BDC, it will not run the Net Logon service, it will not participate in authentication of user logons, and its icon in the Server Manager window will be dimmed.

Note

Usually, when a BDC is promoted to a PDC, the system automatically demotes the former PDC to a BDC. However, if Server Manager cannot locate the PDC, the PDC is not demoted, and the user receives a message indicating this condition. The user can choose to proceed without demoting the PDC or wait until the PDC can be demoted.

For information about how to promote and demote domain controllers, see “Promoting a Backup Domain Controller to Primary Domain Controller” and “Demoting a Primary Domain Controller to Backup Domain Controller” in Server Manager Help.

Directory Database Synchronization

The directory database is synchronized automatically by Windows NT Server. Based on settings in the registry, the PDC sends timed notices that signal the BDCs to request directory changes from the PDC. The notices are staggered so that all BDCs do not request changes at the same time. When the BDC requests changes, it informs the PDC of the last change it received. Thus the PDC is always aware of which BDC needs changes. If a BDC is up to date, the Net Logon service on the BDC does not request changes.

Storage of Changes in the Change Log

Changes to the directory database consist of any new or changed passwords, new or changed user and group accounts, and any changes in their associated group memberships and user rights.

Changes to the directory database are recorded in the *change log*. The size of the change log determines how long changes can be held. The log holds a certain number of changes. As a new change is added, the oldest change is deleted. When a BDC requests changes, those changes which occurred since the last synchronization are copied to the BDC. Because the change log keeps only the most recent changes, if a BDC does not request changes in time, the entire directory database must be copied to that BDC. For example, if a BDC is offline for a time, more changes can occur during that time than can be stored in the change log.

Partial and Full Synchronization

The automatic, timed replication to all domain BDCs of only those directory database changes that have occurred since the last synchronization is called *partial synchronization*. You can use Server Manager to force a partial synchronization of all BDCs in the domain. For example, if a new user is added to the domain and is in great need of certain resources, you can perform a partial synchronization to get the new user's account added to all BDCs as soon as possible.

If needed, you can use Server Manager to manually force a partial synchronization of a particular BDC with the PDC. For example, if access is denied because of a problem with the BDC computer account password (as evidenced by "access denied" messages in the event log), a partial synchronization of the BDC with the PDC fixes the password problem and reestablishes a secure channel.

Sending a copy of the entire directory database to a BDC is called *full synchronization*. Full synchronization is performed automatically when changes have been deleted from the change log before replication takes place (as described in the preceding example) and when a new BDC is added to a domain.

The default Net Logon Service settings for the timing of updates (every five minutes) and the size of the change log (holds about 2000 changes) ensure that full synchronization will not be required under most operating conditions.

Note

Full synchronization over a slow WAN link is time consuming and expensive. To avoid the occurrence of an unplanned full synchronization, you can increase the size of the change log.

For information about setting the size of the change log, see the *Windows NT Network Guide in the Resource Kit* version 4.0.

Synchronizing Domain Controllers

In Server Manager, the **Computer** menu command for synchronizing changes, depending on the type of computer that is selected:

- When the primary domain controller is selected, the **Synchronize Entire Domain** command is available on the **Computer** menu. This command copies the latest directory database changes from the PDC to all the BDCs in the domain. S**ynchronize Entire Domain** initiates synchronization of all BDCs without waiting for completion of the synchronization in progress.

- When a backup domain controller is selected, the **Synchronize With Primary Domain Controller** command is available on the **Computer** menu. This command copies the latest directory database changes to the selected BDC only.

For information about setting the size of the change log, see the *Windows NT Server Resource Kit*.

For information about how to synchronize domain controllers, see “Synchronizing a Backup Domain Controller with the Primary Domain Controller” and “Synchronizing All Servers of the Domain” in Server Manager Help.

Adding, Renaming, Moving, and Removing Domain Computers

A domain is created by installing Windows NT Server and designating the computer as a domain controller. Other computers can then be added to the domain.

Before a computer running Windows NT Workstation or Windows NT Server can be a domain member and participate in domain security, it must be added to the domain. When a computer is added to a domain, Windows NT Server creates an account for the computer. If the added computer is a backup domain controller, it requests a copy of the domain directory database.

When you remove a computer running Windows NT Workstation or a computer running Windows NT Server from a domain, the computer’s account is removed. To add a computer to another domain, a new computer account must be created and then the computer can join that domain.

Note

To remove a backup domain controller from a domain, you must delete the computer account and reinstall Windows NT Server on that computer, indicating the new domain.

Adding a Domain Workstation or Server Computer

To add a computer to a domain, you must be logged on to a user account that has the appropriate user rights.

With the appropriate rights, users can add workstations and servers to domains during or after installation:

- Once a domain is created, a member of Administrators or Account Operators local groups can add a backup domain controller to the domain. Primary and backup domain controllers can be added only during installation.

  Note

  A primary domain controller cannot be added to an existing domain.

- During installation of Windows NT Server, a member of the Administrators or Account Operators group, or a user who has the Add workstation to domain right, can add a computer running Windows NT Server to a domain as a member server.

- During installation of Windows NT Workstation, a member of the Administrators or Account Operators group, or a user who has the Add workstation to domain right, can add a computer running Windows NT Workstation to a domain.
- After installation, a member of the Administrators or Account Operators group, or a user who has the “Add workstation to domain” right, can add an existing computer running Windows NT Workstation or a member server to a domain using the Network option in Control Panel on the computer being added.
- After installation, a member of the Administrators or Account Operators group, or a user that has the “Add workstation to domain” right can use the **Add To Domain** command in Server Manager to add a computer account to the domain’s security database. Then a user at the computer allows the computer to *join the domain* by typing the domain name in the Network option in Control Panel on the computer being added.

Note

Take care to protect the security of an added computer name. Until the intended computer joins the domain, it is possible for a user to give a different computer that computer name, and then have it join the domain using the computer account you have just created. If the added computer is a backup domain controller, when it joins it receives a copy of the domain’s security database.

For information about how to add a computer to a domain, see “Adding a Computer to the Domain” in Server Manager Help.

For information about rights, see Chapter 2, “Working With User and Group Accounts.”

For instructions on installing Windows NT Server or Windows NT Workstation, see *Windows NT Server Start Here*.

Removing a Computer from a Domain

You can remove workstations, backup domain controllers, and member servers from a domain, but you cannot remove the primary domain controller until you promote a backup domain controller to primary domain controller.

When you remove a computer running Windows NT Workstation or member server from a Windows NT Server domain, you delete the computer’s account from the directory database, and the computer cannot participate in domain security. Once the computer account is removed from the domain, a user of the computer must remove the domain name using the Network option in Control Panel. Then the user can add a different domain name or a workgroup name.

Warning

To remove a backup domain controller from a domain, you must delete the computer account and reinstall Windows NT Server or Windows NT Workstation on that computer, indicating the new domain. Do not continue to use a backup domain controller that has been removed from a domain until you have reinstalled the operating system.

For information about how to remove a computer from a domain, see “Removing a Computer from the Domain” in Server Manager Help.

Changing the Computer Name of a Workstation or Server

To change a computer name, first add the computer to the domain as a new computer account. Then change the computer name at the workstation or server using the Network option in Control Panel. From your computer, you can then remove the old computer account from the domain.

If you are changing the name of a backup domain controller, make sure the new computer name is reflected in the database before deleting the old computer account from the directory database. Use the primary domain controller or another backup domain controller to synchronize the directory database.

For information about how to “Adding a Computer to Domain” and change a computer name, “Changing a Computer Name” in Server Manager Help.

For information about how to synchronize domain controllers, see “Synchronizing a Backup Domain Controller with the Primary Domain Controller” in Server Manager Help.

Changing the Name of a Domain

To change the name of a Windows NT Server domain, reenter the domain name on each server and workstation in the domain and then reestablish existing trust relationships. The domain security identifier (SID) does not change.

You can use this procedure to change the domain name on all computers within a domain. You cannot use it to move a domain controller from one domain to another. Also, you cannot use this procedure to split a domain into two separate domains or to join two separate domains into a single domain.

For information about how to change a domain name, see “Removing a Computer from the Domain” in User Manager for Domains Help.

Moving a Computer to a Different Domain

A backup domain controller cannot change domains unless Windows NT Server is reinstalled on it. Member servers and computers running Windows NT Workstation can change domains without requiring Windows NT to be reinstalled.

To move a workstation or member server from one Windows NT Server domain to another, remove the computer from the old domain and add it to the new one.

For information about how to “Removing a Computer from the Domain” and “Adding a Computer to the Domain” in Server Manager Help.

Managing Domain Security Policies

Windows NT Server and Windows NT Workstation security policy settings can provide different levels of security for user actions on domain controllers and on workstations and member servers. Domain security policy should be worked out in advance as part of planning your domain.

When administering domains, security policy applies to the primary and backup domain controllers in the domain (they share the same security policy). When administering a computer running Windows NT Workstation or a computer running Windows NT Server, security policy applies only to that computer.

You can define three security policies:

- The *Account policy* controls how passwords are used by user accounts.
- The *Audit policy* controls what types of events are recorded in the security log (which you can view in Event Viewer if you are logged on as a member of the Administrators group).
- The *Trust Relationships policy* controls which domains are trusted and which domains are trusting domains. This policy is not used in the Single Domain model and is not available when administering a computer running Windows NT Workstation or a computer running Windows NT Server as a member server.

A fourth security policy, the *User Rights policy*, is applied to groups or users and affects the activities allowed on either an individual workstation or member server, or on all domain controllers in a domain.

For information about the User Rights security policy, see Chapter 2, “Working With User and Group Accounts.”

For information about trust relationships, see “Administering Trust Relationships,” later in this chapter.

For information about planning domains and creating trust relationships in multiple-domain models, see the Windows NT Networking Guide in the *Windows NT Server Resource Kit* version 4.0.

Setting User Password (Account) Policy

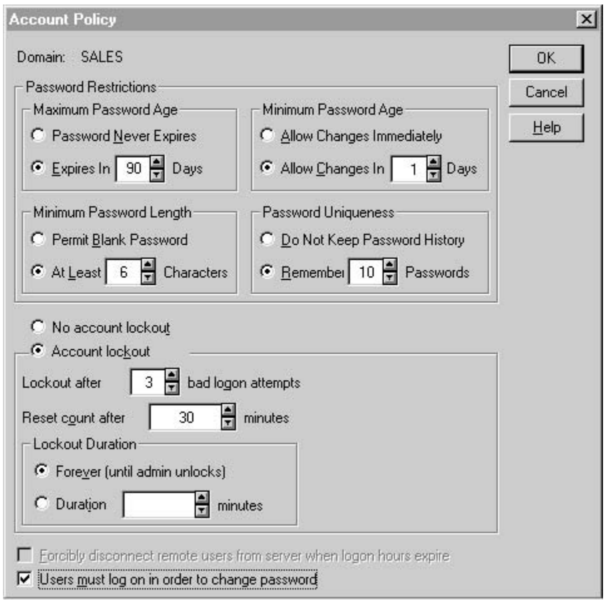
The *Account policy* controls how passwords must be used by all user accounts for a computer or domain and also determines the *account lockout* policy.

Password restrictions include password expiration limits, whether a password can be changed and when a change is required, whether each new password must be unique from former passwords, and how long a password can be.

The account lockout feature enables you to make Windows NT Server more secure from intruders who try to log on by guessing the passwords of existing user accounts. When account lockout is enabled, a user account becomes locked if a number of incorrect logon attempts occur within a specified amount of time. Locked accounts cannot log on. A locked account remains locked until an administrator unlocks it or until a specified amount of time passes. By default, account lockout is disabled.

Note

The account lockout feature is not available in Windows NT version 3.1 or LAN Manager version 2.*x*.



Domain: SALES

Password Restrictions

Maximum Password Age
- ○ Password Never Expires
- ● Expires In 90 Days

Minimum Password Age
- ○ Allow Changes Immediately
- ● Allow Changes In 1 Days

Minimum Password Length
- ○ Permit Blank Password
- ● At Least 6 Characters

Password Uniqueness
- ○ Do Not Keep Password History
- ● Remembei 10 Passwords

- ○ No account lockout
- ● Account lockout

Lockout after 3 bad logon attempts

Reset count after 30 minutes

Lockout Duration
- ● Forever (until admin unlocks)
- ○ Duration minutes

□ Forcibly disconnect remote users from server when logon hours expire

☑ Users must log on in order to change password

There are four password parameters you define in the Account Policy dialog box.

Parameter	Description
Maximum Password Age	The period of time a password can be used before the system requires the user to change it.
Minimum Password Age	The period of time a password must be used before the user is allowed to change it. If you select the Allow Changes Immediately option, then under Password Uniqueness you should select the Do Not Keep Password History option.
Minimum Password Length	The fewest characters a password can contain.
Password Uniqueness	The number of new passwords that must be used by a user account before an old password can be reused. If you enter a uniqueness value here (for example, Remember 4 Passwords), then under Minimum Password Age you should specify an age value (for example, Allow Changes In 7 Days).

If you select Account Lockout, you should also set the following parameters.

Parameter	Meaning

Lockout After — The number of incorrect logon attempts that will cause the account to be locked. The range is 1 to 999.

Reset Count After — The maximum number of minutes that can occur between any two bad logon attempts. The range is 1 to 99999.

For example, if Lockout After is 5 bad logon attempts, and Reset Count After is 30 minutes, then 5 bad logon attempts, each 29 minutes apart, would cause lockout.

Lockout Duration — Select Forever to cause locked accounts to remain locked until an administrator unlocks them. Select Duration and type a number to cause accounts to remain locked for the specified number of minutes.

The **Forcibly Disconnect Remote Users From Server When Logon Hours Expire** option interacts with the logon hours defined for a user account. If the option is selected, a user account that exceeds the time set in the Logon Hours dialog box is disconnected from all connections to any server in the domain. The user receives a warning message a few minutes prior to expiration of the logon hours.

If this option is cleared, the user will not be disconnected when Logon Hours has been reached, but no new connections are allowed and a warning message is sent every 10 minutes.

When **Users Must Log On In Order To Change Password** is selected, users cannot change their own passwords when they expire—they must get help from an administrator. When this option is cleared, users can change their own passwords when they expire without help from an administrator.

Changes to account policy affect each user on the computer or domain at the next logon.

For information about how to set account policy, see “Managing the Account Policy” in User Manager for Domains Help.

For information about setting logon hours, see Chapter 2, “Working With User and Group Accounts.”

Setting the Audit Policy

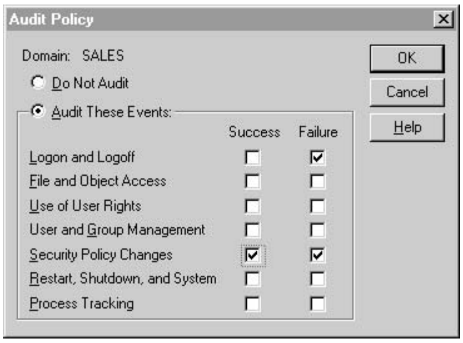
Through auditing, you can track selected activities of users. On a domain controller, the Audit policy determines the amount and type of security logging Windows NT Server performs on all domain controllers in the domain. On workstations or member servers, the Audit policy determines the amount and type of security logging performed on the individual computer.

Windows NT can record a range of event types—from a system-wide event such as a user logging on, to an attempt by a particular user to read a specific file. Both successful and unsuccessful attempts to perform an action can be recorded.

Use the Audit policy to select the types of security events that will be audited. When such an event occurs, an entry is added to the computer’s security log. Use Event Viewer in Administrative Tools on the Start menu to view the security log.

Setting up auditing on files, directories, and printers is a two-part process: After you enable auditing for the domain and select the events to audit, you can then apply audit security to files, directories, and printers using the Security tab on the respective object’s property sheet. For information about using auditing as a resource security measure, see Chapter 4 “Managing Shared Resources and Resource Security.”

When administering domains, the Audit policy applies to the security log of the primary and backup domain controllers in the domain because they share the same Audit policy. When administering a computer running Windows NT Workstation or a computer running Windows NT Server as a member server, this policy applies only to the security log of that computer.



Domain: SALES

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	☐	☑
File and Object Access	☐	☐
Use of User Rights	☐	☐
User and Group Management	☐	☐
Security Policy Changes	☑	☑
Restart, Shutdown, and System	☐	☐
Process Tracking	☐	☐

The following table describes the types of events that can be audited.

Type of event	**Description**
Logon and Logoff	A user logged on or off or made a network connection.
File and Object Access	A user opened a directory or a file that is set for auditing in File Manager, or a user sent a print job to a printer that is set for auditing in Print Manager.
Use of User Rights	A user used a user right (except those rights related to logon and logoff).
User and Group Management	A user account or group was created, changed, or deleted. A user account was renamed, disabled, or enabled; or a password was set or changed.
Security Policy Changes	A change was made to the User Rights, Audit, or Trust Relationships policies.
Restart, Shutdown, and System	A user restarted or shut down the computer, or an event has occurred that affects system security or the security log.
Process Tracking	These events provided detailed tracking information for things like program activation, some forms of handle duplication, indirect object accesses, and process exit.

Because the security log size is limited, select the events to be audited carefully, and consider the amount of disk space you are willing to devote to the security log. The maximum size of the security log is defined in Event Viewer.

For information, see “Managing the Audit Policy” in User Manager for Domains Help; “Viewing Event Logs”, “Searching for Events”, and “Viewing Event Details” in

Event Viewer Help; and "To add a user or group to a permissions or auditing list" in Windows NT Help.

For information about the security log and using the Event Viewer, see Chapter 9, "Monitoring Events."

Administering Trust Relationships

By grouping computers into domains, network administrators and users benefit in two major ways:

- Servers in a domain form a single administrative unit, sharing security and user account information, thereby saving administrators and users time and effort.
- Users browsing the network for available resources see the network grouped into domains rather than as individual servers and printers on the whole network. (This benefit of domains is identical to the Microsoft Windows for Workgroups and Windows 95 concept of a workgroup.)

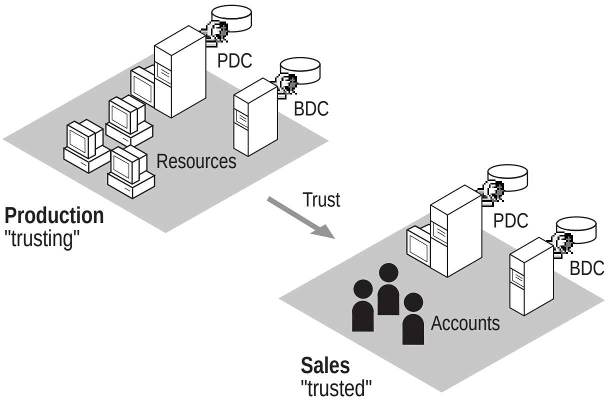
Trust relationships move the convenience of centralized administration from the domain level to the network level. By establishing trust relationships between the domains on your network, you enable user accounts and global groups to be used in domains other than the domain where these accounts are located. You need to create each user account only once, and because directory services enable synchronization of all security data in the directory database, the account can be given access to any computer on your network—not just the computers in one domain.

Trust relationships are created only between Windows NT Server domains. When administering member servers, computers running Windows NT Workstation, or a LAN Manager 2.*x* domain, the **Trust Relationships** command is unavailable.

The following diagram illustrates a trust relationship between two domains that contain both resources and accounts.

Note

The arrows in diagrams showing trust relationships always point *from the resources* that can be used *to the accounts* that are trusted to use them.



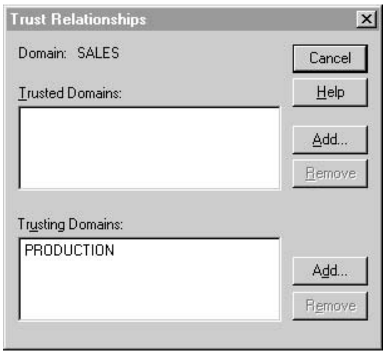
One-way trust relationship

In the preceding diagram, user accounts from the Sales domain can use resources in the Production domain. The effect of this trust is that users from Sales can log on to their domain and receive access to servers in the Production domain, and they can do so from any workstation in either domain. Users from Sales can be added to local groups in the Production domain. Users in Production, however, cannot belong to local groups in the Sales domain, log on to the Production domain from Sales workstations, nor connect to servers in the Sales domain.

One common scenario for a one-way trust is for a domain containing only accounts to be trusted by one or more resource domains. That trust configuration results in all accounts being trusted to use all resources.

Creating a Trust Relationship Between Two Domains

To create trust relationships, you use the **Trust Relationships** command on the **Policies** menu in User Manager for Domains. Creating a one-way trust relationship requires two steps: first one domain (the domain that is to be the *trusted* domain) must add a second domain (the domain that is to be the *trusting* domain) to the list of domains that trust it. Then the trusting domain must add the trusted domain to the list of domains that it trusts. Because the trust relationship is not yet established, these two steps might need to be performed by separate administrators.



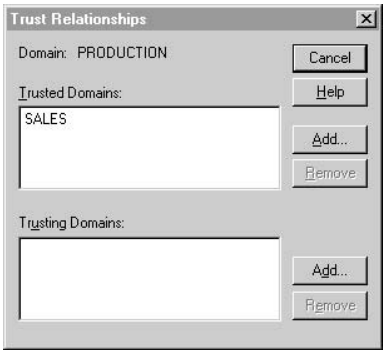
Trust Relationships

Domain: SALES

Trusted Domains:

Trusting Domains:
PRODUCTION

It is best to establish the **Trusting Domain** relationship first, followed by the **Trusted Domain** relationship. This order allows the password used for setting up the relationship to be verified immediately when the relationship is first used.



Trust Relationships

Domain: PRODUCTION

Trusted Domains:
SALES

Trusting Domains:

For detailed information about trust relationships, and strategies for planning trust relationships between the domains of a network, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

For information about how to create a trust relationship, see “Adding a Trusting Domain” and “Adding a Trusted Domain” in User Manager for Domains Help.

Removing a Trust Relationship Between Two Domains

To remove a trust relationship, you must remove both halves of the trust. From the trusting domain, remove the trusted domain. From the trusted domain, remove the trusting domain.

Integrating Windows NT Server With Existing Systems

Microsoft Windows NT Server integrates well with existing network systems, including Novell NetWare and LAN Manager. Windows NT Server provides the software you need to establish communication between your computers running Windows NT Server and other network computers and resources. However, because so many choices of protocols and services exist, you need to know your organization’s requirements before installing Windows NT Server.

For two computers to communicate on a network, they must share at least one network protocol. Before installing Windows NT Server, you’ll need to know the requirements of your organization.

For information about understanding how various protocols and services work, see the *Windows NT Server Networking Supplement.*

For step-by-step procedures for installing the correct software components, see *Windows NT Server Start Here*.

Local User Accounts

If your network currently has servers with network operating systems other than Windows NT, such as LAN Manager 2.*x*, Novell NetWare, or IBM LAN Server, you can use *local user accounts* to facilitate network access between users of these systems and users with Windows NT Server domain accounts.

Local user accounts cannot be used to log on interactively at a computer running Windows NT Server as a member server or Windows NT Workstation, but in most other ways are just like regular user accounts: They can connect to computers running Windows NT Server or Windows NT Workstation over the network, can be placed in global and local groups, and can be assigned resource permissions and user rights. The one exception is that local accounts created in one domain cannot be used in domains that trust that domain—the use of each local account is limited to one domain.

You create and use local accounts in a domain in two types of situations:

- To allow users from other Windows NT Server domains to connect to LAN Manager 2.*x* servers in this domain
- To allow users whose user accounts are in untrusted domains or domains not running Windows NT Server to connect to computers running Windows NT Server and Windows NT Workstation in this domain.

You create a local account in the same way you create regular user accounts, except that while creating the account, use the **Account** button in the **New User** dialog box in User Manager for Domains to designate it as a local account.

For information about creating local user accounts, see Chapter 2, “Managing User and Group Accounts.”

How Windows NT Server Works With LAN Manager

Windows NT Server maintains compatibility with servers running LAN Manager at the same time it expands and enhances the LAN Manager feature set. Instead of four types of servers, there are three Windows NT Servers; instead of requiring a user account for each domain, users can have a single network-wide logon. Similarly, Windows NT Server security features build on those of LAN Manager.

A significant difference between LAN Manager and Windows NT Server systems is that LAN Manager does not recognize trust relationships, and therefore does not allow local groups. To enable user access to resources on LAN Manager servers in your domain, you must create local user accounts for all users in your domain who need to use the resources.

Workstations do not need updated software to make the transition from a LAN Manager to a Windows NT Server domain. However, to ensure that the correct domain validates the logon request, MS-DOS LAN Manager clients must be running LAN Manager version 2.1a or above. When clients run software prior to LAN Manager 2.1, the domain name is not passed and is instead broadcast throughout the network until a server recognizes the logon name. Not only does performance suffer, but the user may have accounts in several domains and may not be validated by the correct domain controller.

Administering Microsoft LAN Manager Servers

When you administer Microsoft LAN Manager 2.1 or later servers, a few Server Manager functions are unavailable or work slightly differently from Windows NT computers.

Server Manager function	**Performance with Microsoft LAN Manager 2.x**
Administering the list of alert recipients	The Server and Alerter services on that server must be stopped and restarted before the changes will take effect. Since the Server service can only be restarted locally, this action must be performed at that server.
Configuring service startup	In the Services dialog box, the Startup button is unavailable.
Promoting a server to primary domain controller	A LAN Manager 2.*x* server cannot be promoted to primary domain controller of a domain containing a Windows NT Server PDC.

Synchronizing a server with the primary domain controller	When a LAN Manager 2.*x* server is selected, the Synchronize With Primary command reestablishes the computer account password on both that server and the primary domain controller. You can do this only for LAN Manager 2.*x* servers that are members of domains with LAN Manager 2.*x* primary domain controllers. You cannot use Server Manager to synchronize a LAN Manager 2.*x* server with a Windows NT Server primary domain controller.
Directory replication	Server Manager cannot administer the LAN Manager 2.*x* replication service. A LAN Manager 2.*x* export server cannot replicate to Windows NT import computers. However, a Windows NT export server can replicate to LAN Manager 2.*x* servers (including LAN Manager for UNIX Systems 2.*x* servers). Usually, Windows NT and LAN Manager 2.*x* export servers will not coexist in the same domain.

When administering a Microsoft LAN Manager 2.*x* domain using Server Manager, the **Servers**, **Workstations**, and **All** commands on the **View** menu are unavailable.

How Windows NT Server Works With Novell NetWare

Windows NT Server provides the transport protocol software needed to communicate with NetWare computers and the gateway service that enables servers and workstations on a Windows NT Server domain to use resources on NetWare network servers and a migration path from NetWare to Windows NT Server.

Windows NT Workstation and Windows NT Server include client software to support connections to servers running NetWare. With the Client Service for NetWare in Windows NT Workstation and the Gateway Service for NetWare in Windows NT Server, users can use file and print resources on servers running NetWare 2.*x* through 4.*x*.

In addition to acting as client software for NetWare, the Gateway Service provides access to NetWare servers for Microsoft network client computers that are not running NetWare client software. Computers without NetWare client software can connect to NetWare resources as if they were shared on a computer running Windows NT Server. Administrators can control which users can establish a gateway and which resources can be shared over the gateway.

Also, File and Print Services for NetWare enables a computer running Windows NT Server to function as a NetWare 3.12-compatible file and print server. Computers running NetWare client software can use file and print resources and advanced server applications on the same multipurpose computer running Windows NT Server. This feature enables NetWare users to integrate Windows NT Servers without incurring the high expense of reconfiguring their desktops and networks.

For information about NetWare networks, see the *Windows NT Server Networking Supplement*.

How Services for Macintosh Integrates Macintosh Computers

Where Apple Macintosh computers exist on a network, you can use Services for Macintosh to allow personal computer and Macintosh clients to share files and printers. Services for Macintosh is a thoroughly integrated component of Microsoft Windows NT Server. You can set up Services for Macintosh during installation, or you can add it later.

With Services for Macintosh, Macintosh computers need only the Macintosh operating system to function as Windows NT Server clients. No other software is required, although optional user authentication module software is available if you want to provide a secure logon to Windows NT Server.

For applications that have versions for both the personal computer and Macintosh, users of both versions can work on the same data file using Services for Macintosh. When Macintosh users view directories on the server containing these files, they see the files represented by the appropriate icon. For example, a person using a personal computer version of Microsoft Excel can create a spreadsheet file and store it on the server in a shared directory that also is configured as a Macintosh-accessible volume. A Macintosh user who opens that folder sees the file represented by the Macintosh icon that represents a Microsoft Excel spreadsheet.

Macintosh and personal computer users can send print jobs to any printer attached to a computer running Windows NT Server, as well as to PostScript printers that register themselves as a LaserWriter on the AppleTalk network.

All Macintosh computers that can use AppleShare (the Apple networking software for the Macintosh) can use Services for Macintosh.

User accounts for Macintosh users are created and stored in the same way as accounts for personal computer users. One aspect of Windows NT Server user accounts, the user’s *primary group*, applies only to Services for Macintosh. The user’s primary group is the group the user works with the most, and it should be the group with which the user has the most resource needs in common. When a user creates a folder on a server, the user becomes the owner. The owner’s primary group is set as the group associated with the folder. The administrator or owner can change the group associated with the folder.

For information about using Services for Macintosh, see the *Windows NT Server Networking Supplement*.

Network Protocols and Services that Provide Connectivity

In addition to the specific software for interactions with Novell NetWare and Microsoft LAN Manager networks, and for using Apple Macintosh and MS-DOS client computers in Windows NT domains, Windows NT Server provides the protocols and network services that allow information exchange between Windows NT Server-based computers and most other networks, including UNIX networks and the Internet.

For information about protocols and services that are available with Windows NT Server, see *Windows NT Server Start Here*.

For information about specific network connectivity, see the *Windows NT Server Networking Supplement*.

Connectivity with IBM Mainframe and AS/400 Hosts

Microsoft System Network Architecture (SNA) Server is an optional solution that provides a gateway connection between personal computer LANs or WANs and IBM mainframe and AS/400 hosts. SNA Server can use a variety of physical connection types to connect to the host. On the client side, personal computer LANs or WANs need only TCP/IP (Transmission Control Protocol/Internet Protocol), IPX (internetworking packet exchange), or NetBEUI protocols to use the SNA gateway, all of which are provided by Windows NT Server.

An SNA gateway eliminates the need for SNA software running on the host to manage a communications port for each personal computer connection. Instead, personal computers connect over a LAN to the SNA server; the SNA server requires only one connection to the host.

For information about Microsoft SNA Server, see the *Windows NT Networking* Guide in the *Windows NT server Resource Kit* version 4.0.