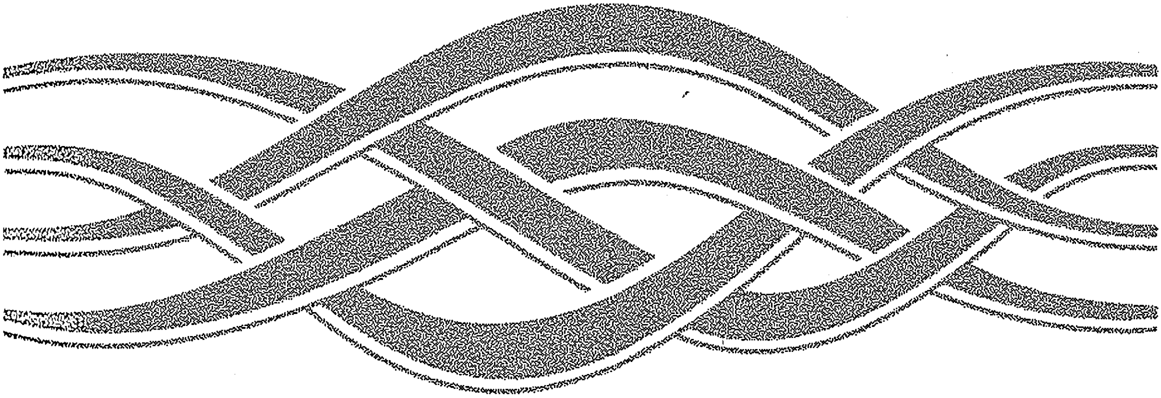
Microsoft®

Concepts and Planning



Microsoft® Windows NT® Server

Concepts and Planning

Microsoft® Windows NT® Server

Version 4.0

Microsoft Corporation

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation.

© 1985-1996 Microsoft Corporation. All rights reserved.

Microsoft, MS, MS-DOS, Windows, Windows NT, and BackOffice are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Microsoft.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Document No. 69940-0696
Printed in the United States of America.

Contents

Welcome

The *Windows NT Server Concepts and Planning* guide is for new and experienced administrators of small networks and advanced users of operating systems. Use this book to implement and optimize Windows NT® Server.

Windows NT Server Concepts and Planning provides information on the following topics:

- Managing domains
- User and group accounts
- User work environments
- File systems and security
- Print servers
- Data protection
- Monitoring performance, events, and your network
- Client administration
- Licensing
- Registry
- Running applications for other operating systems on Windows NT Server

This book assumes that you have already installed Windows NT Server as described in *Windows NT Server Start Here*.

For information about implementing Windows NT Server on larger networks, see the *Windows NT Server Resource Kit* version 4.0.

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.

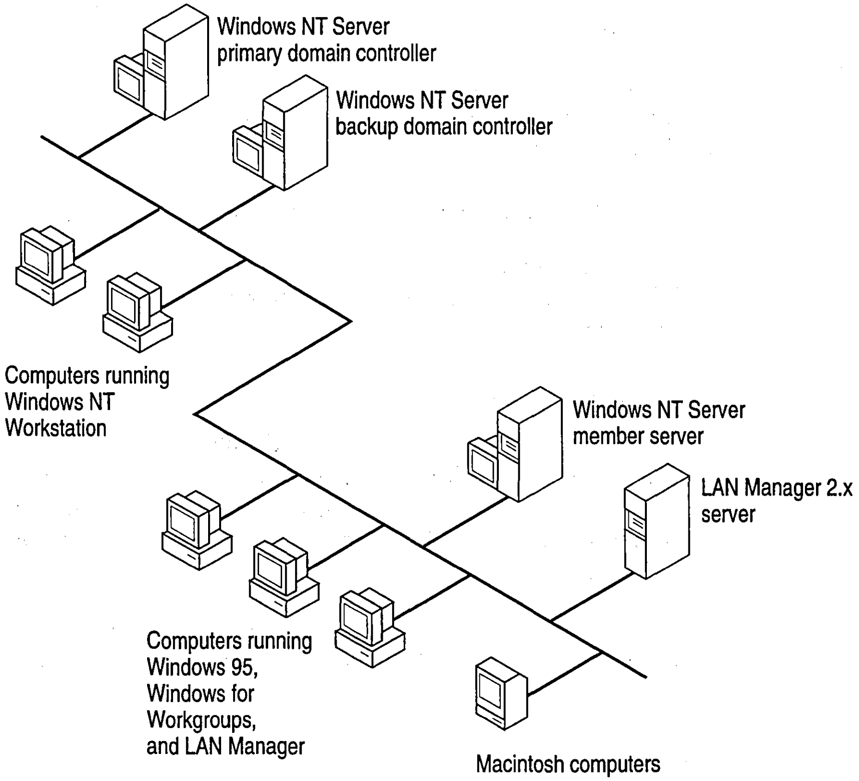
For information about Novell NetWare domain interoperability, see "How Windows NT Server Domains Work With Novell NetWare Domains" later in this chapter.

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 primary domain controller
Windows NT Server backup domain controller
Computers running Windows NT Workstation
Windows NT Server member server
LAN Manager 2.x server
Computers running Windows 95, Windows for Workgroups, and LAN Manager
Macintosh computers

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

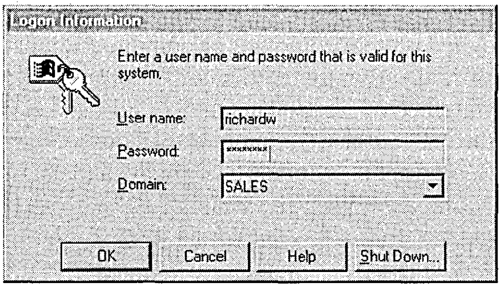
Most network administrators have a dual role. They are both administrators and users of the network. Sometimes they perform network management tasks; at other times they are network users, performing the same tasks as other users.

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:

- Organizations with many small branch offices
- Large organizations
- Security for sensitive information

In addition, expansion is easy. 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:

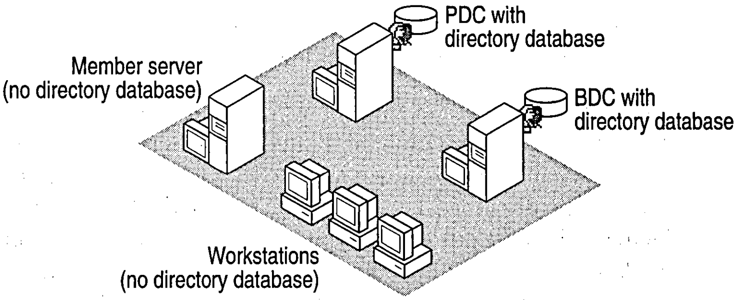
Object	Space Used
User account	1.0K
Computer account	0.5K
Group account	4.0K (average group size = 300 members)

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.


PDC with directory database
Member server (no directory database)
BDC with directory database
Workstations (no directory database)

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.

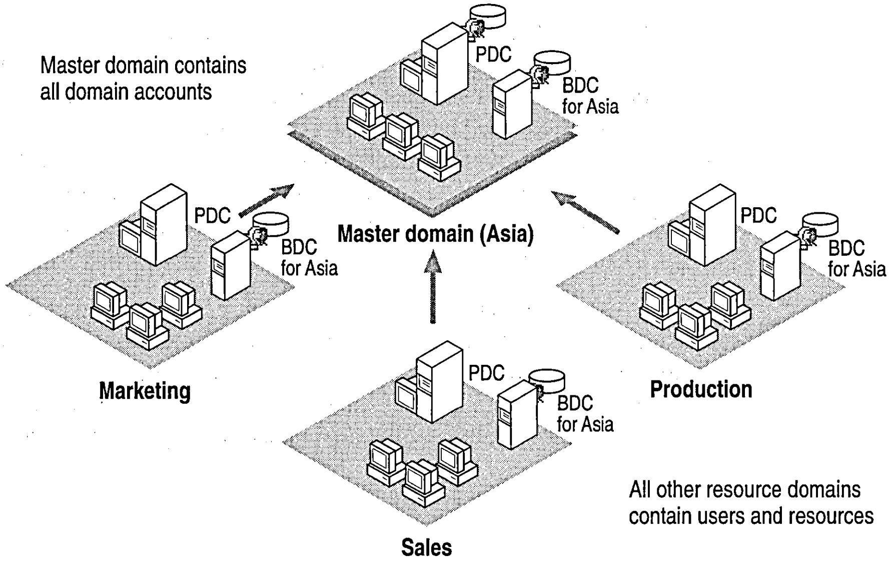
Having a single domain also means that all your network administrators can administer all network servers. Splitting a network into domains enables you to create administrators who can administer only some servers, such as those in their own department.

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.

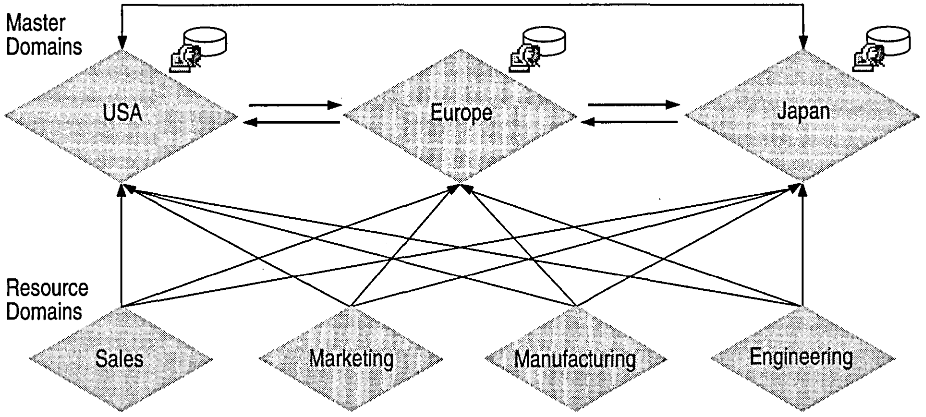
The single master domain model is particularly suited for:

- 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. **Synchronize 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.

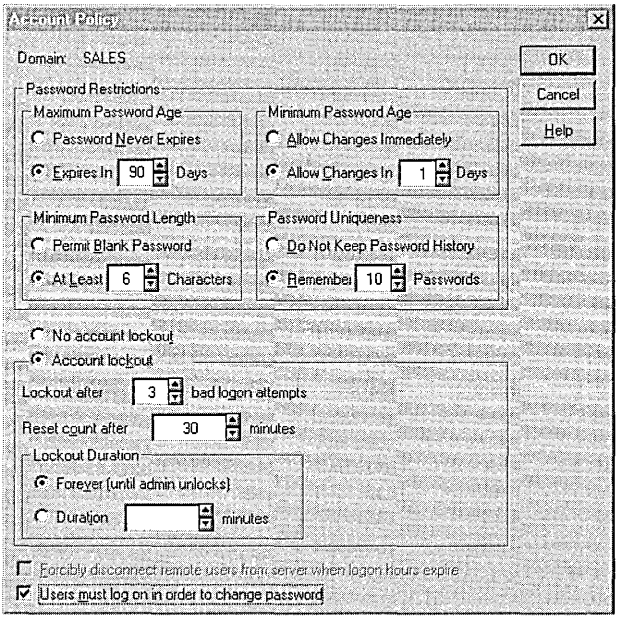
Setting User Password (Account) Policy

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
● Remember 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

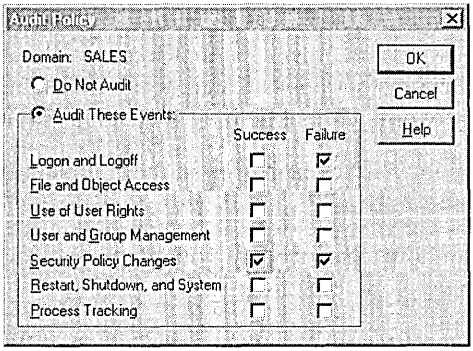
Through auditing, you can track selected activities of users. On a domain controller, the Audit policy determines the amount and type of security logging Windows NT Server performs on all domain controllers in the domain. On workstations or member servers, the Audit policy determines the amount and type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

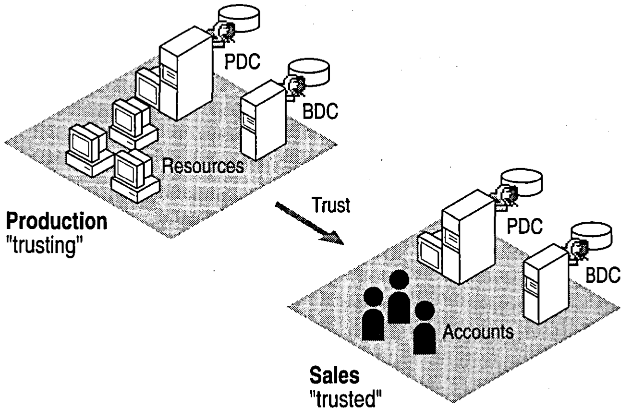
- Servers in a domain form a single administrative unit, sharing security and user account information, thereby saving administrators and users time and effort.
- Users browsing the network for available resources see the network grouped into domains rather than as individual servers and printers on 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.



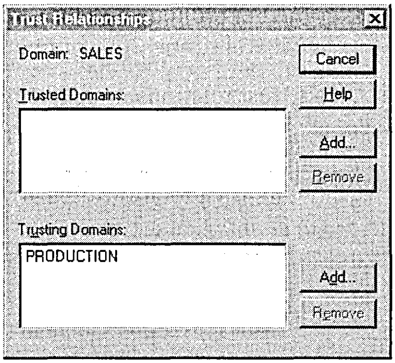
One-way trust relationship

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.



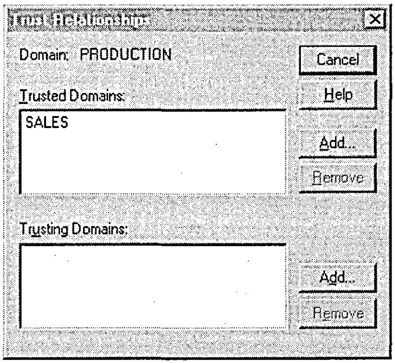
Trust Relationships

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.



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. For example, Windows NT Server builds on the LAN Manager domain model but simplifies domain administration. Instead of four types of servers, there are three; 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.

CHAPTER 2

Working With User and Group Accounts

User and group accounts enable users to participate in a domain and to access its resources. Rights and permissions granted to user accounts and group accounts provide the appropriate amount of freedom and restrictions that an organization's various resources require.

Managing user accounts and groups involves careful planning, but the procedures for administering accounts are simple and straightforward. In most cases, these procedures are identical for domain accounts and for workstation accounts.

Managing User Accounts

Each person who will regularly use the network and participate in a domain must have a *user account* in a domain on the network. The user account contains information about the user, including name, password, various optional entries that determine when and how users log on and how their desktop settings are stored.

Domain Accounts and Workstation Accounts

Computers running Windows NT Workstation and member servers (computers running Windows NT Server that are not domain controllers) maintain user accounts, groups, and security policies separate from those of the domain. The built-in accounts on such computers provide built-in rights on the computer that parallel the rights afforded by these same built-in accounts on the domain level.

When a domain controller is configured, its built-in accounts provide the administrator with certain administrative rights. When a workstation or member server is configured, its built-in accounts provide the administrator with administrative rights. To achieve the appropriate level of control over a workstation, member server, or domain, the administrator decides which user accounts to add to the various built-in groups.

Management Utilities: User Manager and User Manager for Domains

A computer's operating system determines the type of accounts you can manage, as well as the utility you use to manage them:

- On computers running Windows NT Workstation, you manage the accounts of that workstation only, and you use the User Manager utility.
- On computers running Windows NT Server, you manage accounts on the local domain or on any workstation, member server, or other domain to which you have access. To do so, you use the User Manager for Domains utility.
- You can install User Manager for Domains on a computer running Windows NT Workstation or Windows® 95 using Client-based Administration Tools. With User Manager for Domains installed on the client computer, you can administer domain controllers and other workstations from that computer.

For information about using Client-based Network Administration Tools, see Chapter 11, "Managing Client Administration."

For information about using User Manager for Domains on client computers, "To install Client-based Network Administration Tools on a computer running Windows NT Workstation" and "To install Client-based Network Administration Tools on a computer running Windows 95" in Network Client Administrator Help.

Using a Low-Speed Connection

Some domains and computers might communicate with your computer across a connection that has relatively low transmission rates. For example, slow transmission can occur on a domain controller that is connected to your computer using a Remote Access Service (RAS) connection, overseas connection, or connection that is saturated with other high-volume tasks that should not be interrupted with User Manager for Domains tasks. To reduce delays in the display of user accounts, groups, or computers, select **Low Speed Connection**.

For more information, see "Using Low Speed Connection" in User Manager for Domains Help.

Refreshing the View

When User Manager for Domains first displays a domain or a computer, it receives the information necessary to create the user account and the group lists. Information displayed by User Manager for Domains is automatically updated at fixed intervals. However, if you need to make sure the displayed information is current, use the **Refresh** command on the **View** menu.

Note When **Low Speed Connection** is selected, the **Refresh** command is unavailable.

Domain User Accounts

A *domain user account* contains information that defines a user to a Windows NT Server domain controller. In User Manager for Domains, you can establish, delete, or disable domain user accounts. You can also set security policies and add user accounts to groups.

Contents of a User Account

When creating a user account, you provide several pieces of information that determine how the account can be used. The following table shows the contents of each user account:

Account element	Description
User name	The unique name the user types when logging on; often a combination of parts of the user's first and last names.
Full name	The user's full name.
Description	Any text describing the user or user account.
Password	The user's secret password.
Logon hours	The hours during which the user is allowed to log on. This setting affects both being able to log on to the network and being able to access servers. Whether users are forced to log off when their logon hours expire is determined by a setting in the domain's account security policy. For more information, see "Managing Logon Hours" later in this chapter.
Logon workstations	The computer names of the Windows NT computers that the user can work from. By default, the user can use any workstation, but you can limit this if you want.
Expiration date	A future date when the account automatically becomes disabled; it is useful to ensure that accounts for temporary employees or students are not unnecessarily kept active.

(continued)

Account element	Description
Home directory	A directory that is private to the user. An administrator creates this directory, and the user controls access to it.
Logon script	A batch file or executable file that runs automatically when the user logs on.
Profile	The path to a folder containing information that is retained to create the user's desktop environment between logons, such as program groups, network connections, and screen colors, and settings determining what aspects of the environment the user can change. For information about user profiles, see Chapter 3, "Managing User Work Environments."
Account type	The account type is either global or local. Most accounts you create will be global accounts. For information about local accounts, see "Adding Local User Accounts" later in this chapter. This option is available only on Windows NT Server domains.

In addition, several conditions affect the user with respect to their unique domain or local computer password. These conditions can be selected or cleared by the administrator or account operator for the domain controller or by the administrator for a workstation or member server containing user accounts.

Account condition	Default	Comments
User Must Change Password at Next Logon	Selected	If selected, the user will be forced to change the password the next time he or she logs on. The setting changes to On when the user's password reaches the maximum password age as set for the domain in Account Policy. Once the password is changed, the setting changes to Off.
User Cannot Change Password	Cleared	If selected, the user cannot change his or her own password. This restriction is useful for shared accounts. It does not apply to administrators.
Password Never Expires	Cleared	If selected, this user account ignores the password expiration policy set for the domain, and the password never expires. This is used for accounts that represent services, such as the Replicator service. It is also useful for accounts for which you want the password to never change, such as guest accounts.
Account Disabled	Cleared	If selected, this account is disabled and cannot be logged on to. It is not removed from the database, but no one can log on to the account until you enable it again.

Security Identifier (SID)

A user or group account includes a *security identifier* (SID), a unique number that identifies the account. Every account on your network is issued a unique SID when the account is first created. Internal processes in Windows NT refer to an account's SID rather than the account's user or group name. If you create an account, delete it, and then create an account with the same user name, the new account will not have the rights or permissions previously granted to the old account because the accounts have different SID numbers.

Domain Names

On some Windows NT Server screens (such as in User Manager for Domains), a domain name precedes the user name. The domain name indicates where the user's account was created and where it resides within the overall domain structure. For example, user JohnL from the Sales domain might appear as SALES\JohnL.This name would distinguish him from a different JohnL in another domain (such as ENGINEERING\JohnL).

Built-in Domain and Workstation User Accounts

Two built-in user accounts are created automatically when Windows NT Server or Windows NT Workstation is installed: the Administrator account and the Guest account.

Built-in Administrator User Account

The Administrator account is the one you use when you first set up a new domain controller, member server, or workstation. You use this account before you create an account for yourself. The Administrator user account is a member of the Administrators local group on a domain controller, workstation, or member server. The Administrator account can never be deleted, disabled, or removed from the Administrators local group, ensuring that you never lock yourself out of the computer by deleting or disabling all the administrative accounts. This feature sets the Administrator account apart from other members of the Administrators local group.

The built-in Administrator account gives a user automatic rights to perform domain management tasks on a domain controller or on a workstation or member server that resides within that domain or a trusting domain. During Setup, the domain administrator or MIS person who sets up the domain PDC is prompted for a password to the Administrator account. This password should be guarded carefully, not only for security purposes but also because if the password is forgotten or the person who knows the password becomes unavailable, the built-in Administrator account is unusable. The password can be changed but it does not expire.

The user who sets up a workstation can assign a password to the Administrator account, or leave it blank. In the latter case, anyone can use the account without a password.

After the PDC is set up, the built-in Administrator account can be renamed, but it can never be deleted or disabled.

Tip Following installation, it is a good idea to create an additional administrative account with administrative-level abilities and reserve the built-in Administrator account for emergency purposes. When each administrative user has a separate account, their actions can be audited on the individual user account name as opposed to the Administrator account.

For information about built-in groups and rights, see "Using Groups to Assign User Abilities" later in this chapter.

For information about auditing, see Chapter 9, "Monitoring Events."

For information about installing a PDC, see *Windows NT Server Start Here.*

Built-in Guest Account

The Guest account is used for logons by people who do not have an actual account on the computer or domain or in any of the domains trusted by the computer's domain. A user whose account is disabled (but not deleted) can also use the Guest account. The Guest account does not require a password and can be used for two types of guest logons: *local guest logons* and *network guest logons.* You can configure each domain and computer to allow both types of guest logon, only one type, or neither type. The Guest account is disabled by default when Windows NT Server or Windows NT Workstation is installed, but you can reenable it.

You can set rights and permissions for the Guest account just like any user account. By default, the Guest account is a member of the built-in Guests group, which allows a user to log on to a workstation or member server (the right to log on locally) only. Rights other than this one, as well as any permissions, must be granted to the Guests local group by an Administrator or Account Operator.

Guests have no predefined rights on a domain controller.

A *local guest logon* takes effect when a user logs on interactively at a computer running Windows NT Workstation or at a member server running Windows NT Server and specifies Guest as the user name in the **Logon Information** dialog box. Because the Guest account on these computers (but not on domain controllers) has the built-in right to log on locally, the guest user can then work at that computer (subject to the rights and permissions you have granted the Guest account) and use it to access the network.

A *network guest logon* takes effect at a computer that uses the Guest account when a user has logged on interactively to either a domain account or a local computer account (as in the case of a workgroup member) and tries to connect to the computer that uses the Guest account:

- A computer running Windows NT Workstation in either a workgroup or a domain
- A member server
- A domain controller
- A LAN Manager 2.*x* client computer

In the case of a workgroup, the computer name is treated as a domain name by the computer being accessed. The computer being connected to might not recognize the user's account for any of the following reasons:

- The domain specified as containing the user's account is not trusted and the user does not have an account in the domain or in the directory database of the computer being accessed. This case always applies to a workgroup computer because workgroup computers do not use trust relationships, and the computer being connected to treats the computer name as a domain name.
- The domain specified as containing the user's account is trusted but the user does not have an account in the trusted domain.
- The domain is the same as the domain of the computer being connected to and the user does not have an account in the domain or in the directory database of the computer being connected to (if it is not a domain controller).

A network guest logon is approved only if the Guest account of the destination computer is enabled and has no password set. The guest user then has all rights, permissions, and group memberships on the computer that are granted to the Guest account, even though the guest user has not specified Guest as his or her user name.

Tip To allow local guest logons but not network guest logons, enable the Guest account, but revoke its Access This Computer From Network user right in User Manager for Domains.

To allow network guest logons but not local guest logons, enable the Guest account, and revoke its Log On Locally user right. (Be sure Guest has the Access This Computer From Network right).

For information about how to manage user accounts, see "Managing Properties for One User Account" in User Manager for Domains Help.

For information about logon validation, see Chapter 1, "Managing Windows NT Server Domains."

For information about configuring computers while installing Windows NT Server or Windows NT Workstation, see *Windows NT Server Start Here.*

Adding New Domain User Accounts

To create additional user accounts or modify existing accounts, use User Manager for Domains.

When adding a user account you will be asked to provide a user name, which can be up to 20 characters. It must be unique to the domain or computer being administered. It can contain any uppercase or lowercase characters except the following:

" / \ [ ] : ; | = , + * ? < >

A user name cannot consist solely of periods (.) and spaces.

Be consistent in the way you enter user names because when Windows NT presents lists of user accounts, they are usually sorted by the user names. It is a good idea to establish a standard for user names, such as a shortened combination of the first and last names (JeffHo for Jeff Howard).

You will also be asked to provide the user's full name. It is a good idea to establish a standard for full names so that they always begin with either the last name (Howard, Jeff) or the first name (Jeff Howard). The full name can also affect the sort order because the user account list in the User Manager for Domains window can optionally be sorted by full name instead of user name.

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

Adding Several Accounts at One Time

User accounts can contain a lot of information. Typing that information for each user can take a lot of time, but with Windows NT Server Directory Services there are ways you can make creating user accounts easier. You can create a new account by copying an existing account and just changing the user name, full name, and initial password, and any other information that must be changed. You can also create one or more *template accounts*. These accounts are not used by real users but serve only as bases for the real accounts you create. For greater security, you can disable your template accounts to ensure that no user can log on using them. The copies that you make are enabled by default.

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

Selecting User Accounts

The user account list in the **User Manager for Domains** window includes all user accounts of the displayed domain. One or more user accounts can be selected from this list:

- You can copy, delete, rename, or modify the properties of a selected user account or create a new group that contains that account.
- You can modify or delete multiple user accounts at the same time.
- You can modify the properties of a group, delete a group, or create a new group containing the selected accounts.

Note When **Low Speed Connection** is selected, the **Select Users** command is unavailable.

For more information, see "Selecting User Accounts", "Managing Properties for One User Account" and "Managing Properties for Multiple User Accounts" in User Manager for Domains Help.

Copying Existing Accounts

It is often quicker and more convenient to copy an existing user account than to create a new one. By copying, you ensure that the group memberships and many other properties are copied to the new account.

When a user account is copied, the description, group memberships, logon hours, logon workstations, and account information are copied exactly.

To have the system automatically enter the account user name into the home directory path, use %USERNAME%. For more information, see "Using %USERNAME% in the Home Directory Path" later in this chapter.

- The user name, full name, and password boxes of the new account are blank and must be entered. The **User Cannot Change Password** and **Password Never Expires** check boxes are copied.

Note When copying an account that is a member of the Administrators local group, the **User Cannot Change Password** setting is not copied.

- Usually, the **User Must Change Password At Next Logon** check box is selected, regardless of its setting in the original account. However, if the **User Cannot Change Password** check box is copied as selected, then the **User Must Change Password At Next Logon** check box is cleared.
- The **Account Disabled** check box is always cleared, regardless of the setting in the original user account. You can create a new user account, configure it as needed, disable it, and then use it as a template. You can quickly make numerous copies of a disabled template account.

User Manager for Domains does not copy rights and permissions granted to a user account. However, it is recommended that these be provided only to groups and not granted directly to user accounts. Because the group memberships of the original account are copied to the new user account, the new user account will usually have the same abilities and access to resources as the original account.

For information about how to copy user accounts, see "Copying a User Account" in User Manager for Domains Help.

For information about creating and copying user profiles, see Chapter 3, "Managing User Work Environments."

Specifying a Home Directory

A *home directory* contains a user's files and programs; it can be assigned to an individual or be shared by many users. Because home directories collect user files in one location, they make it easy for an administrator to back up user files and delete user accounts. You specify a home directory by adding a directory path to the user account. Home directories must be added to a shared directory with appropriate access.

The home directory is a user's default directory for the **File Open** and **Save As** dialog boxes, for the command prompt, and for all applications that do not have a working directory defined.

User Manager for Domains automatically applies directory permissions if it creates the home directory. When one user account is being administered and a new home directory is created, that user is granted Full Control. When two or more user accounts are being administered and a new home directory is created, Full Control is granted to Everyone.

User Manager for Domains does not automatically apply permissions if the directory already exists. In this case, you must apply the permissions using Windows NT Explorer.

If the user account does not specify a home directory, the default home directory for upgraded computers is \USERS\DEFAULT on the user's local drive where Windows NT is installed. If Windows NT Workstation or Windows NT Server has been installed for the first time, the default home directory is the root of the drive where Windows NT is installed. (To change the default home directory to a shared network directory or to another local directory on the user's workstation, use User Manager for Domains.)

- When administering the user accounts of a domain, you should assign *network* home directories. User Manager for Domains automatically creates that home directory. If it cannot, a message instructs you to create the directory manually.
- When administering the user accounts of a workstation or member server, you should assign *local* home directories. User Manager for Domains automatically creates that home directory at that computer. If it cannot, a message instructs you to manually create the directory.
- If you are administering a domain and you specify a local path for the home directory, User Manager for Domains will not create the home directory.

For information about how to add home directories, see "Managing the User Environment" in User Manager for Domains Help.

Managing the User Environment Profile

A *user profile* consists of work environment settings that are loaded by the system during logon for a given user. These settings include all the user-specific settings of a user's Windows environment, such as screen colors, network connections, printer connections, mouse settings, shortcuts, window size and position. User profiles are identified by the user name.

Local user profiles are created automatically on the computer at logon the first time a user logs on to a computer running Windows NT Workstation or Windows NT Server. Each user's individual user profile is available to that user on successive logons at that computer.

Roaming user profiles are available on computers running Windows NT Workstation or Windows NT Server. To enable roaming user profiles, an administrator enters a user profile path into the user account. The first time the user logs off, the local user profile is copied to that location. Thereafter, the server copy of the user profile is downloaded each time the user logs on (if it is more current than the local copy). Both the local and server copies are updated each time the user logs off.

Mandatory user profiles are roaming profiles that are created for the user and cannot be changed by the user. When the user logs off, the local user profile is not saved and a copy of the local user profile is not copied to the server. User profiles are also available on computers running Windows 95; however, a user profile created on Windows 95 is not available to the user on a computer running Windows NT and vice versa, even if the user profile is stored on a server.

For information about how to add user profiles, see "Managing the User Environment" in User Manager for Domains Help

For information about creating and managing mandatory and roaming user profiles, see Chapter 3, "Managing User Work Environments."

Specifying a User Profile Location

In the **User Environment Profile** dialog box, assign a roaming or mandatory profile to a user account by typing its full path and user profile folder name in the **User Profile Path** box.

\\server\share\profile name

For information about adding a user profile location, see "Managing the User Environment" in User Manager for Domains Help.

For information about creating and managing user profiles, see Chapter 3, "Managing User Work Environments."

Using %USERNAME% in the Home Directory Path

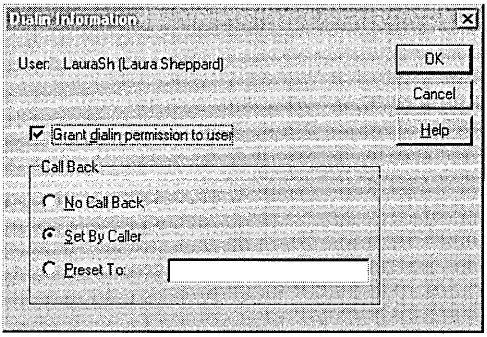
In the **Home Directory** box, %USERNAME% can be substituted for the last entry in the path. The system later substitutes the user name of the user account. This substitution is useful when multiple user accounts are selected.

For example, you have selected eight user accounts. In the **Home Directory** box, you might select **Connect**, specify a drive letter of **K**, select the **To** box, and type **\\\\SALES\\home\\%username%**. When you choose **OK** to save the User Environment Profile, the actual user name will be substituted for each %USERNAME% entry.

For information about logon scripts and about creating and managing user profiles, see Chapter 3, "Managing User Work Environments."

Managing Dial-in Information

Windows NT Server provides domain-based security for RAS users. To enable users to use RAS to dial in to domain accounts from remote computers, you use the **Dialin Information** dialog box in User Manager for Domains to add dialin information to their user accounts, including call-back options and permission to use dial-in facilities.


Dialin Information

User: LauraSh (Laura Sheppard)

☑ Grant dialin permission to user

Call Back

○ No Call Back

● Set By Caller

○ Preset To:

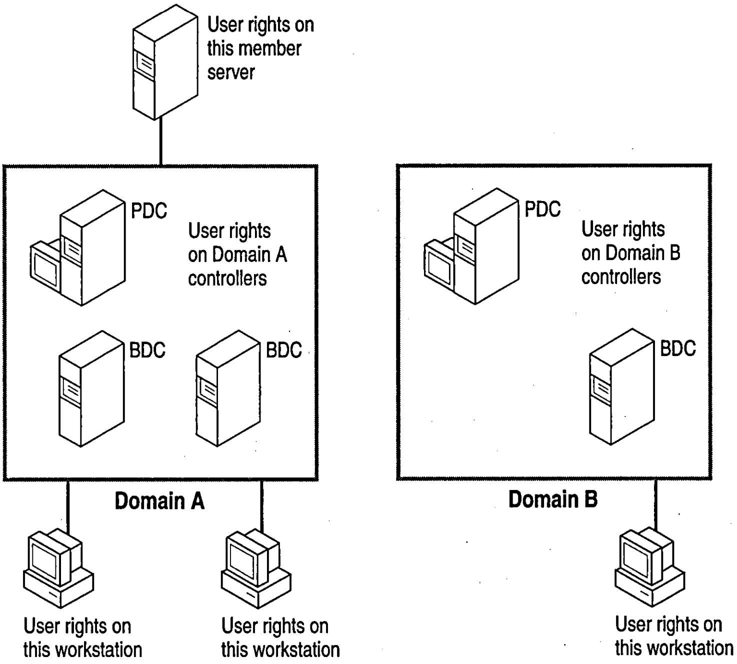
For information about using RAS and installing RAS servers, see the *Windows NT Server Networking Supplement.*

Managing the User Rights Policy

A *right* authorizes a user to perform certain actions on a computer system, such as backing up files and directories, logging on to a computer interactively, or shutting down a computer system. Rights exist as capabilities for using either domain controllers at the domain level or workstations or member servers at the local level. Rights can be granted to groups or to user accounts, but are best reserved for use by groups. Rights also can be granted to the special built-in groups Everyone, Interactive, and Network (for more information about these groups, see "Special Groups" later in this chapter). A user who logs on to an account that belongs to a group to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights to perform an action, an attempt to carry out that action is blocked by Windows NT Server (if the attempt is made on a domain controller or member server) or by Windows NT Workstation (if the attempt is made on a workstation computer).

Note Rights apply to the system as a whole and are different from permissions, which apply to specific objects. A *permission* is a rule associated with an object (usually a directory, file, or printer), and it regulates which users can have access to the object and in what manner. Most often the creator or owner of the object sets the permissions for the object.

Because all rights are not associated with a specific object and are applied at the domain (domain controllers) or local (workstation or member server) level, they can sometimes override permissions set on an object. For example, a user logged on to a domain account that is a member of the Backup Operators group has the right to perform backup tasks for all servers of the domain. Doing so requires the ability to read all files on those servers, even files on which their owners have set permissions that explicitly deny access to all users, including members of the Backup Operators group. A right—in this case, the right to perform a backup—takes precedence over all file and directory permissions. The following diagram shows the range of user rights within a domain (all domain controllers have the same user rights) and on workstations (every workstation and member server has it's own set of user rights.


User rights on this member server
PDC
User rights on Domain A controllers
BDC
BDC
Domain A
User rights on this workstation
User rights on this workstation
PDC
User rights on Domain B controllers
BDC
Domain B
User rights on this workstation

Setting User Rights

Members of the Administrators local group in a domain or on a local computer (member server or workstation) have the built-in ability to grant rights to users for the domain or the computer, respectively. The easiest way to provide rights to a user is to add a user's account to a built-in group that has the desired rights. (Each built-in group conveys certain rights and abilities to its members.) However, when you create new local groups, or if a special situation occurs, it is possible to grant a right to, or remove it from, a user or a group account.

The following table describes the user rights that can be managed with the **User Rights** command on the **Policy** menu.

Note When you administer the User Rights policy for a domain, the computers referred to in the following table are the primary and backup domain controllers of the domain; when you administer the User Rights policy on a workstation or member server, the computer referred to is the workstation or member server.

User right	Allows a user to
Access this computer from network	Connect over the network to a computer.
Add workstations to domain	Add a workstation to the domain, allowing the workstation to recognize the domain's user and global group accounts and those of trusted domains.
Back up files and directories	Back up files and directories, allowing the user to read all files. This right supersedes file and directory permissions, and also applies to the registry.
Change the system time	Set the time for the internal clock of a computer.
Force shutdown from a remote system	This right is not currently implemented. It is reserved for future use.
Load and unload device drivers	Install and remove device drivers.
Log on locally	Log on at the computer itself, from the computer's keyboard.
Manage auditing and security log	Specify what types of resource access (such as file access) are to be audited. View and clear the security log. This right does not allow a user to set system auditing using the **Audit** command in the **Policy** menu of User Manager for Domains. This ability is always held only by the Administrators group.
Restore files and directories	Restore files and directories, allowing the user to write to all files. This right supersedes file and directory permissions, and also applies to the registry.
Shut down the system	Shut down Windows NT Server.
Take ownership of files or other objects	Take ownership of files, directories, and other objects on a computer.

If **Show Advanced User Rights** is selected, some additional rights (shown in the following table) can be managed with the User Rights policy. Many of these advanced rights are useful only to programmers writing applications to run on Windows NT Server or Windows NT Workstation, and are not typically granted to a group or user. The first two advanced user rights, **Bypass traverse checking** and **Log on as a service**, are of special interest to administrators.

Advanced user right	**Allows**
Bypass traverse checking	A user to change directories and travel through a directory tree, even if the user has no permissions for those directories.
Log on as a service	A process to register with the system as a service, used to administer the Directory Replicator service. For information about directory replication, see Chapter 4, "Managing Shared Resources and Resource Security."
Act as part of the operations system	A user to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.
Create a page file	A user to create a paging file.
Create a token object	A user or program to create access tokens. Only the Local Security Authority can do this.
Create permanent shared objects	A user to create special permanent objects, such as \Device, which are used within the Windows NT platform.
Debug programs	A user to debug various low-level objects such as threads.
Generate security audits	A user or program to generate security audit log entries.
Increase quotas	A user to increase object quotas (not available in this version of Windows NT Server).
Increase scheduling priority	A user to boost the priority of a process.
Lock pages in memory	A user to lock pages in memory so they cannot be paged out to a backing store such as PAGEFILE.SYS.
Log on as a batch job	A user to log on using a batch queue facility for delayed logons.
Modify firmware environment variables	A user to modify system environment variables. (Users can always modify their own user environment variables).
Profile single process	The use of Windows NT platform profiling (performance sampling) capabilities on a process.
Profile system performance	The use of Windows NT platform profiling capabilities on the system. (This can slow the system down.)
Replace a process-level token	A user to modify a process's security access token. This is a powerful privilege used only by the system.

For more information about programming rights, see the Windows NT programming documentation.

For information about how to set user rights, see "Managing the User Rights Policy" in User Manager for Domains Help.

For information about adding users to groups, see "Using Groups to Assign User Abilities" later in this chapter.

For information about granting rights to new groups, see "Granting Rights to New Local Groups" later in this chapter.

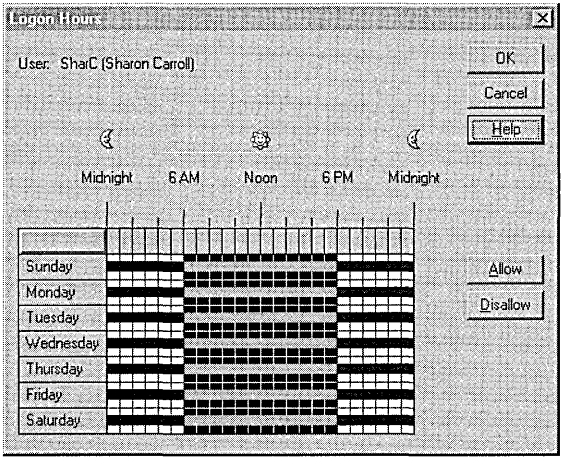
For information about the capabilities of built-in groups, see "Built-in Local Groups—Controlling What Users Can Do" later in this chapter.

Managing Logon Hours

By default, users can connect to a server 24 hours a day, 7 days a week. To restrict this access, use the **User Properties** dialog box.

When you select a user account in User Manager for Domains and view user properties, you can select **Logon Hours** in the **User Properties** dialog box to change the settings for that user. The **Logon Hours** dialog box displays a one-week calendar, with logon hours displayed in one-hour increments across seven days. A box represents each hour. For example, the first box in each row represents the hour from midnight through 12:59 A.M., and the last box in each row represents the hour from 11:00 P.M. through 11:59 P.M.

Note The logon hours are in the time zone of the primary domain controller, not of the workstation or server that the user is logging on to or connecting to.


User: SharC (Sharon Carroll)

The filled boxes indicate when the user is allowed to connect to domain servers; the empty boxes indicate when a user is prohibited from connecting.

When a user is connected to a server and the logon hours are exceeded, the user will either be disconnected from all server connections or will be allowed to remain connected but denied any new connections, depending on the status of an option in the **Account Policy** dialog box.

For information about how to set logon hours, see "Managing Logon Hours" in User Manager for Domains Help.

Managing Account Information

You can define an account expiration date and specify the account type for the selected user accounts.

When an account has an expiration date, the account is disabled at the end of that day. (Expired accounts are not deleted, only disabled.) When an account expires, a logged on user remains logged on but can establish no new network connections and cannot log on again after logging off.

By default, a new user account is a *global* user account.

Adding Local User Accounts

A *local account* is a user account provided in a domain for a user whose regular account is not in a trusted domain. Local accounts provide access to resources in a single domain, and resources can be used only by connecting to a domain controller over the network. (You can log on interactively to a local account *only* if the right to log on locally has been granted to the account.)

The local account user must first log on to the network using a workgroup computer account or a global domain account and then connect to a domain controller in the domain where the local account resides. When the user connects to the domain controller, the user's credentials (domain name, user name, and password) are passed to the domain controller. This controller first checks the domain name and, because the domain is not trusted, checks further to see if the user has a local or global user account by the same name and if the password specified in the user's credentials matches the password for the local account. If the account is found but the passwords do not match, the user is prompted for the local account password.

Creating a User Account as Local

A user account can be created as a local account to give domain access to a user who:

- Is not a member of any domain.
- Is a member of a domain that does *not* have an established trust relationship with the domain where the user's global account is located.

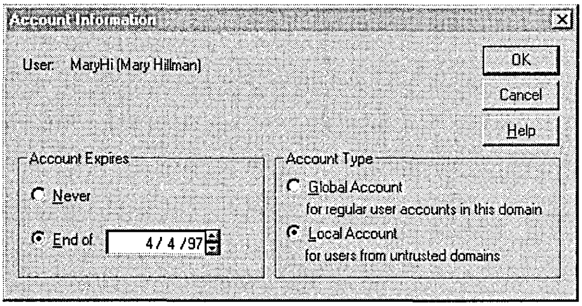
For example, a local account would be required for a user who is a member of a workgroup or whose domain account is located on servers of other systems such as LAN Manager 2.*x*, Novell NetWare, or IBM LAN Server (which do not recognize trust relationships).

If necessary, you can easily return the account type to global. For example, you would do so if you created an account for a user whose workstation is a member of a workgroup, and the workstation later joined the domain.

Tip By default, local accounts are added to the Domain Users global group. In a multiple-domain setting, the Domain Users global group in a trusted domain can be added to local groups in trusting domains to gain access to resources there. To limit local account access to resources in the domain where you want the account to be used (the trusted domain), remove the local account from the Domain Users group in that domain, or do not grant permissions on any resources in the trusting domain or domains to the Domain Users group from the trusted domain.

In User Manager or User Manager for Domains, you see the icon at the left that represents local user accounts instead of the standard global user account icon.

The default setting for a new user account is **Global Account**. When you add a new local user account, you can change the default setting in the **Account Information** dialog box.



User: MaryHi (Mary Hillman)

Account Expires
○ Never
● End of 4/ 4 /97

Account Type
○ Global Account
for regular user accounts in this domain
● Local Account
for users from untrusted domains

For information about how to manage user accounts, see “Creating a New User Account” and “Managing Account Information” in User Manager for Domains Help.

Renaming a User Account

Any user account—including built-in user accounts—can be renamed. Because it retains its security identifier (SID), a renamed user account retains all its other properties, such as its description, password, group memberships, user environment profile, logon hours, logon workstations, account information, and any assigned permissions and rights.

For information about how to rename a user account, see "Renaming User Accounts" in User Manager for Domains Help.

Deleting and Disabling User Accounts

To prevent a user from logging on, you disable or delete the user account:

- A *disabled* user account still exists, but the user is not permitted to log on; a *deleted* user account is completely removed.
- A *disabled* account still appears in the user account list of the User Manager for Domains window; a *deleted* account is removed from the user account list of the User Manager for Domains window, and it cannot be restored.
- A *disabled* account can be reenabled at any time.

To prevent accidental deletions, it is a good idea to first disable a user account, and then periodically delete the disabled accounts.

Note Internal processes in Windows NT Server refer to a user account's SID rather than its user name. So if you delete a user account that had read access to a certain shared directory and then create another user account with the same user name, the new account will *not* have access to the directory: You will have to reapply permissions to the shared directory.

For information about how to disable and delete user accounts, see "Disabling and Enabling User Accounts" and "Deleting User Accounts" in User Manager for Domains Help.

Migrating User Accounts from Novell NetWare

You can migrate user accounts from Novell NetWare servers to Windows NT Server computers.

Use the Migration Tool for NetWare in Windows NT Server to transfer user and group accounts and files and directories from Netware 2.*x* and 3.*x* servers to Windows NT Server.

For information about upgrading from NetWare to Windows NT Server, see the *Windows NT Server Networking Supplement.*

Managing Workstation and Member Server User and Group Accounts

From a computer running Windows NT Server (domain controller or member server), you can remotely manage local member server or workstation user accounts with User Manager for Domains. You can manage user accounts locally from a computer running Windows NT Workstation with User Manager.

Membership in the Built-in Administrators Group

When Windows NT Workstation is installed on a computer, or Windows NT Server is installed as a member (stand-alone) server, the built-in Administrator account is created automatically. The Administrator account is the account used by the person who manages the computer's overall configuration.

If a computer participates in a domain, the Domain Admins global group is by default a member of the computer's Administrators local group, and members of the Administrators group can administer the computer. However, a member of Administrators can remove the Domain Admins global group from the computer's Administrators group.

Administrators group members do not have automatic access to every file on the computer. If a file's permissions do not grant access, the administrator cannot use the file. Every file on an NTFS volume has an owner who can set permissions on the file. If needed, an administrator can take ownership of a file and thus have access to it. But if the administrator does so and auditing of files is selected, this event is recorded in the security log and the administrator cannot give ownership back to the original owner.

To manage workstation or member server accounts instead of domain accounts, in User Manager for Domains, type the computer name as \\computername instead of selecting or typing a domain name. With the workstation or member server selected as the domain, you can perform all the functions from a Windows NT Server computer that can be performed at the computer itself.

For information about how to select a computer instead of a domain, see "Selecting a Domain" in User Manager for Domains Help.

For information about using the NTFS file system, see Chapter 4, "Managing Shared Resources and Resource Security," and *Windows NT Server Start Here.*

For information about file auditing, see Chapter 9, "Monitoring Events."

Managing Group Accounts

Group accounts are collections of user accounts. Giving a user account membership in a group gives that user all the rights and permissions granted to the group. Group membership provides an easy way to grant common capabilities to sets of users.

Using Groups to Assign User Abilities

Because maintaining permissions for a group is easier than maintaining permissions for many user accounts, you generally want to use groups to manage access to resources (such as directories, files, or printers):

- Assign resource permissions to a group, and then add user accounts to that group as desired.
- Change the permissions provided to a set of users or add or remove the permissions assigned to the group but do not change each account.

Note When assigning user abilities, remember to take advantage of the built-in groups provided with Windows NT, which have been granted useful collections of rights and abilities. (For example, members of the Administrators group have administrative abilities in the domain and over the servers of the domain.)

Two types of groups can be maintained in a Windows NT Server domain: local groups and global groups.

Global Groups

A *global group* contains a number of user accounts from one domain that are grouped together under one group account name. A global group can contain only user accounts from the domain where the global group is created. Once a global group is created, it can be granted permissions and rights in its own domain, on workstations or member servers, or in trusting domains. However, it is best to grant rights and permissions to local groups and use the global group as the method of adding users to local groups.

Global groups can be *added* to local groups in the same domain, in domains that trust that domain, or to member servers or computers running Windows NT Workstation in the same or a trusting domain. Global groups contain domain user accounts only. You cannot create a global group on a computer running Windows NT Workstation or on a computer running Windows NT Server as a member server.

The "global" in "global groups" indicates that the group is available to receive rights and permissions in multiple (global) domains.

A global group can contain only user accounts; it cannot contain local groups or other global groups.

Local Groups

A *local group* contains user accounts and global group accounts from one or more domains, grouped together under one group account name. Users and global groups from outside the local domain can be added to the local group only if they belong to a trusting domain. Local groups make it possible to quickly assign rights and permissions for the resources on one domain (that is, the local domain) to users and groups from that domain and other domains that trust it.

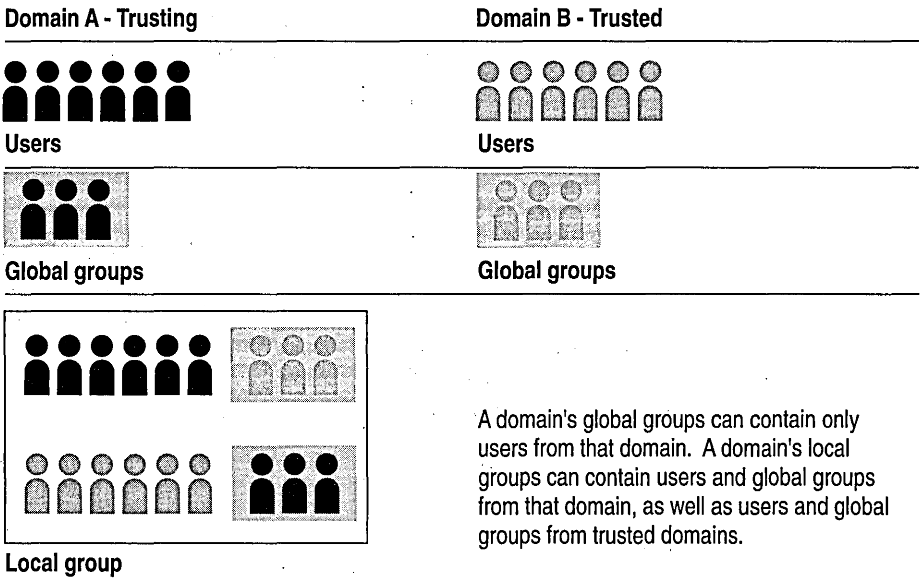
Local groups also exist on member servers and computers running Windows NT Workstation, and can contain user accounts and global groups.

The "local" in "local groups" indicates that the group is available to receive permissions and rights in only a single (local) domain.

A local group cannot contain other local groups.

The following table summarizes how the two types of groups are used.

If	Need to be used in	You can put them in
User accounts from this domain	The domain controllers, member servers, and workstations of this domain, or of other domains	A global group
User accounts from this domain or other domains	The domain controllers of this domain	A local group
Global groups from this domain or other domains	The domain controllers of this domain	A local group



A domain's global groups can contain only users from that domain. A domain's local groups can contain users and global groups from that domain, as well as users and global groups from trusted domains.

Strategies for Using Groups

A local group is a single security entity that can be granted access to many objects in a single location (a domain, or a workstation or member server) rather than having to edit the permissions on all those objects separately.

With global groups you can group user accounts which might be granted permissions to use objects on multiple domains and workstations.

For example, in a multiple-domain setting, you can think of global groups as a means of adding users to the local groups of trusting domains. To extend users' rights and permissions to resources on other domains, add their accounts to a global group in your domain and then add the global group to a local group in a trusting domain.

Even for a single domain, if you keep in mind that additional domains might be added in the future, you can use global groups added to local groups for granting all rights and permissions. Later, if another domain is created, the rights and permissions assigned to your local groups can be extended to a new domain's users by creating a trust relationship and adding global groups from the new domain to your local groups. Likewise, if the new domain trusts your domain, your global groups can be added to the new domain local groups.

Domain global groups can also be used for administrative purpose on computers running Windows NT Workstation or on member servers running Windows NT Servers. For example, the Domain Admins global group is added by default to the Administrators built-in local group on each workstation or member server that joins the existing domain. Membership in the workstation or member server local Administrators group enables the network administrator to manage the computer remotely by creating program groups, installing software, and troubleshooting computer problems.

The following table provides some guidelines for using global and local groups:

Purpose of group	Use	Comments
Group users of this domain into a single unit for use in other domains or user workstations	Global	The global group can be put into local groups or given permissions and rights directly in other domains.
Need permissions and rights only in one domain	Local	The local group can contain users and global groups from this and other domains.
Need permissions on computers running Windows NT Workstation or on member servers	Global	A domain's global groups can be given permissions on these computers, but a domain's local groups cannot.
Contain other groups	Local	The local group can contain only global groups (and users); however, no group can contain other local groups.
Include users from multiple domains	Local	The local group can be used in only the domain in which it is created. If you need to be able to grant this local group permissions in multiple domains, you will have to manually create the local group in every domain in which you need it.

For information about trust relationships, see Chapter 1, "Managing Windows NT Server Domains."

Built-in Local Groups—Controlling What Users Can Do

Being a member of one of the built-in local groups of a domain gives a user rights and abilities to perform various tasks on the domain controllers in the domain. Similarly, being a member of a built-in local group on a member server or workstation gives the user rights and abilities on that computer.

You can add a user to more than one built-in group. For example, a user in both the Print Operators and Backup Operators groups has all the rights granted to print operators and all the rights granted to backup operators.

However, not all built-in local groups exist on both Windows NT Server domain controllers and on individual Windows NT computers (Windows NT Workstation computers and member servers running Windows NT Server). The following table shows which built-in local groups exist on domain controllers and on individual computers.

Windows NT Server domain controllers	Windows NT workstations and member servers
Administrators	Administrators
Backup Operators	Backup Operators
Server Operators	Power Users
Account Operators	Users
Print Operators	Guests
Users	Replicator
Guests	
Replicator	

By default, every new domain user (global or local) is a member of the Domain Users global group, which is a member of the Users built-in local group. Each new workstation or member server user is a member of the Users built-in local group on the computer.

In general, you will want to add administrator users for a domain to the Domain Admins global group rather than adding them directly to the Administrators local group. By adding users to Domain Admins, they are also administrators on workstations and member servers.

The following tables show which rights and built-in abilities are held by each built-in local group on both Windows NT Server domains and on member servers and workstations.

Windows NT Server domain controllers

- ● Local group has right or ability
- ○ Local group does not have right or ability

	Administrators	Server Operators	Account Operators	Print Operators	Backup Operators	Everyone	Users	Guests
Rights:								
Log on locally	●	●	●	●	●	○	○	○
Access this computer from network	●	○	○	○	○	●	○	○
Take ownership of files	●	○	○	○	○	○	○	○
Manage auditing and security log	●	○	○	○	○	○	○	○
Change the system time	●	●	○	○	○	○	○	○
Shut down the system	●	●	●	●	●	○	○	○
Force shutdown from a remote system	●	●	○	○	○	○	○	○
Back up files and directories	●	●	○	○	●	○	○	○
Restore files and directories	●	●	○	○	●	○	○	○
Load and unload device drivers	●	○	○	○	○	○	○	○
Add workstations to domain[1]	○	○	○	○	○	○	○	○
Built-in abilities:								
Add workstation to domain	●[1]	○	●[1]	○	○	○	○	○
Create and manage user accounts	●	○	●[2]	○	○	○	○	○
Create and manage global groups	●	○	●[2]	○	○	○	○	○
Create and manage local groups	●	○	●[2]	○	○	○	●[3]	○
Assign user rights	●	○	○	○	○	○	○	○
Manage auditing of system events	●	○	○	○	○	○	○	○
Lock the server	●	●	○	○	○	●[4]	○	○
Override the lock of the server	●	○	○	○	○	○	○	○
Format server's hard disk	●	○	○	○	○	○	○	○
Create common groups	●	●	○	○	○	○	○	○
Share and stop sharing directories	●	●	○	○	○	○	○	○
Share and stop sharing printers	●	●	○	●	○	○	○	○

[1] Add workstations to domain is a built-in ability for Administrators and Account Operators, and cannot be removed from these groups. It is also a right that is granted to no one automatically but can be granted to other users by members of Administrators or Account Operators.

[2] Account operators cannot modify the accounts of Administrators, nor can they modify the Domain Admins global group or the Administrators, Server Operators, Account Operators, Print Operators, or Backup Operators local groups, or any global groups that are members of these local groups.

[3] Even though members of the Users group have the right to create local groups on a server, they will not be able to unless they are allowed to log on locally at the server, or have access to the User Manager for Domains tool.

[4] Even though Everyone has the right to lock the server, only those users also able to log on locally at the server will actually be able to lock it.

Workstations and member servers

● Local group has right or ability
○ Local group does not have right or ability

	Administrators	Power Users	Users	Guests	Everyone	Backup Operators
Rights:						
Log on locally	●	●	●	●	●	●
Access this computer from network	●	●	○	○	●	○
Take ownership of files	●	○	○	○	○	○
Manage auditing and security log	●	○	○	○	○	○
Change the system time	●	●	○	○	○	○
Shut down the system	●	●	●	○[1]	●	●
Force shutdown from a remote system	●	●	○	○	○	○
Back up files and directories	●	○	○	○	○	●
Restore files and directories	●	○	○	○	○	●
Load and unload device drivers	●	○	○	○	○	○
Built-in abilities:						
Create and manage user accounts	●	●[2]	○	○	○	○
Create and manage local groups	●	●[3]	●[4]	○	○	○
Assign user rights	●	○	○	○	○	○
Manage auditing of system events	●	○	○	○	○	○
Lock the computer	●	●	○	○	●	○
Override the lock of the computer	●	○	○	○	○	○
Format computer's hard disk	●	○	○	○	○	○
Create common groups	●	●	○	○	○	○
Share and stop sharing directories	●	●	○	○	○	○
Share and stop sharing printers	●	●	○	○	○	○

[1] By default, even though the Guests group does not have the shutdown right, guests can still shut down the system because Everyone has this right.

[2] A power user can create user accounts, but can modify and delete only those accounts he or she creates.

[3] A power user can create local groups. A power user can also add and remove users from local groups he or she has created, as well as the Power Users, Users, and Guests local groups, but cannot modify the Administrators or Backup Operators local groups.

[4] A member of the Users group can create local groups, but can modify only the local groups that he or she created.

The following table presents the built-in rights with comments about the specific actions the rights allow, as well as what local groups have the rights by default on both domain controllers and on workstations and member servers.

		Granted to	
User rights	Comments	Domain controllers	Workstations and member servers
Manage auditing and security log	Specify what types of file and object access are to be audited. View and clear the security log.	Administrators	Administrators
Back up files and directories		Administrators, Server Operators, Backup Operators	Administrators, Backup Operators
Restore files and directories	This right supersedes file permissions; a user with the Restore right can overwrite files for which he or she has no permissions, when performing a restore.	Administrators, Server Operators, Backup Operators	Administrators, Backup Operators
Change system time		Administrators, Server Operators	Administrators, Power Users
Access this computer from network	Access the computer from another workstation on the network.	Administrators, Everyone	Administrators, Power Users, Everyone
Log on locally	Ability to log on at the computer itself on the computer's keyboard.	Administrators, Server Operators, Account Operators, Print Operators, Backup Operators	Administrators, Backup Operators, Power Users, Users, Guests
Shut down the system		Administrators, Server Operators, Account Operators, Print Operators, Backup Operators	Administrators, Backup Operators, Power Users, Users, Guests
Add workstations and member servers to domain	Allows a user who is not a member of the domain's Administrators group to add computers running Windows NT Workstation or computers running Windows NT Server as member servers to the domain.	None[1]	N/A
Take ownership of files and other objects	Take ownership of files and directories on the computer.	Administrators	Administrators
Load and unload device drivers		Administrators	Administrators
Force shutdown from a remote system	This right gives a user no abilities in this version of Windows NT but will be supported in future upgrades of the operating system.	Administrators, Server Operators	Administrators, Power Users

[1] Members of the domain's Administrators and Account Operators groups can always add workstations to a domain, whether or not they have this right assigned to them. This right is needed only to enable users who are not members of these groups to add workstations to the domain. With this right, Windows NT Server does not have to check that the user is a member of the Administrators or Account Operators group.

The following sections describe the purpose and abilities of each built-in local group:

Administrators

The Administrators local group in a domain, on a computer running Windows NT Workstation, or on a member server has full control over its computer. The Administrators local group is the only group that is automatically granted every built-in right and ability. Administrators manage the overall configuration of the domain and the domain's controllers.

By default, the Domain Admins global group is also a member of the Administrators local group, but it can be removed.

Users

Users logged on as members of the Users local group cannot log on locally at servers running Windows NT Server. However, they do possess certain rights at their local workstations and can perform most necessary tasks.

By default the Domain Users global group is a member of the Users local group, but it can be removed.

Guests

The Guests local group allows occasional or one-time users to log on to a workstation's built-in Guest account interactively (local guest logon) or to a domain's built-in Guest account remotely (network guest logon), and be granted limited abilities. Users logged on as members of the Guests local group have no rights at domain servers. However, they do have certain rights at their individual workstations. By default, the domain Guests global group is a member of the Guests local group, but it can be removed.

For information about the Guest account, see "Built-in Guest Account" earlier in this chapter.

Account Operators

Members of the Account Operators local group can use User Manager for Domains to create user accounts and groups for the domain and to modify or delete most user accounts and groups of the domain. Account Operators can also log on to domain servers, can shut down domain servers, and can use Server Manager to add computers to a domain.

However, an account operator cannot modify or delete the Domain Admins global group, nor the Administrators, Account Operators, Backup Operators, Print Operators, or Server Operators local groups or any global groups belonging to these local groups. Account operators cannot modify the accounts of members of any of these groups and cannot administer security policies.

Backup Operators

Members of the Backup Operators local group can back up and restore files on the domain's primary and backup domain controllers. They can also log on to these servers and shut them down.

Print Operators

Members of the Print Operators local group can create, delete, and manage printer shares on the domain's primary and backup domain controllers. They can also log on at these servers, and shut them down.

Server Operators

Members of the Server Operators local group can manage the domain's primary and backup domain controllers. For example, server operators can create, delete, and manage printer shares at these servers; create, delete and manage network shares; back up and restore files; lock and unlock these servers; format a server's hard disk; and change the system time. They can also log on from servers and shut down servers.

Replicator

The Replicator local group supports directory replication functions. The only member of the domain's Replicator local group should be a domain user account used to log on the Replicator services of the primary domain controller and the backup domain controllers in the domain. Do not add the user accounts of actual users to this group.

For information about directory replication, see Chapter 4, "Managing Shared Resources and Resource Security."

Special Groups

In addition to the built-in groups mentioned, their groups are created by the system and are used for special purposes. Because the memberships of these groups cannot be altered, the groups are not listed in User Manager for Domains.

However, when you administer a computer and Windows NT presents lists of groups, these special groups sometimes appear in the list. For example, they can appear when assigning permissions to directories, files, shared network directories, or printers.

Group	Refers to
Everyone	Anyone using the computer. This includes all local and remote users (that is, the Interactive and Network groups combined). In a domain, members of Everyone can by default access the network, connect to a server's shared network directories, and print to a server's printers.
Interactive	Anyone using the computer locally.
Network	All users connected over the network to the computer.
System	The operating system.
Creator Owner	Transfer of permissions to creators of subdirectories, files, and print jobs. For a directory, if permissions are granted to the Creator Owner group, the creator of a subdirectory or file will be granted those permissions for that subdirectory or file. For a printer, if permissions are granted to the Creator Owner group, the creator of a print job will be granted those permissions for that print job.

Using Administrators and Operators—An Example

Suppose a medium-sized group is deciding how to assign its technical staff to the various administrator and operator groups. (It is recommended that at least one member of either the Administrators or Server Operators group is present during all hours that people are using the network.)

- At least one person must have an administrator account. Members of the Administrators group are ultimately responsible for planning and maintaining network security for the department. If desired, members of the domain's Administrators group can administer users' Windows NT Workstation computers.
- People responsible for hiring new or temporary employees, or for helping newly hired people get started would be good candidates for the Account Operators group. They can create domain accounts for the new employees and put these accounts in the appropriate groups.
- If the domain's Administrators group has few members, assign at least one additional person to the Server Operators group. This group keeps the domain servers running. Accordingly, members of this group can shut down servers, set the system time on servers, lock and override the lock of servers, share directories and printers on the server, and format its hard disks.
- If printing documents quickly is important, add several capable people to the Print Operators group to ensure that printer problems can always be addressed quickly.

Built-in Global Groups—Providing Automatic Memberships in Local Groups

On a domain's primary and backup domain controllers, three global groups are built in: Domain Admins, Domain Users, and Domain Guests. None of these groups can be deleted.

Domain Admins

The Domain Admins global group is initially a member of the Administrators local group for the domain and of the Administrators local group for every computer in the domain running Windows NT Workstation or Windows NT Server.

The built-in Administrator user account is a member of the Domain Admins global group. It is also a member of the Administrators local group and cannot be removed.

Because of these memberships, a user logged on as an administrator can administer the domain, the primary and backup domain controllers, and all other computers running Windows NT Workstation and Windows NT Server in the domain. (However, to prevent Domain Admins from administering a particular workstation or a server that is not a domain controller, remove the Domain Admins global group from that computer's Administrators group.)

To provide administrative-level abilities to a new account, add the account to the Domain Admins global group. Members of this group can administer the domain, the servers and workstations of the domain, and a trusted domain that has added the Domain Admins global group from this domain to the Administrators local group in the trusted domain.

For information about using global groups, see "Strategies for Using Groups" earlier in this chapter.

Domain Users

The Domain Users global group initially contains the domain's built-in Administrator account. By default, all new accounts created thereafter in the domain are added to the Domain Users group, unless you specifically remove them.

The Domain Users global group is, by default, a member of the Users local group for the domain and of the Users local group for every computer in the domain running Windows NT Workstation or member servers running Windows NT Server. Domain Users is the default primary group for each user. (A primary group is a feature for Macintosh clients and users running POSIX compliant applications. For information about using primary groups with services for Macintosh, see the Windows NT Server Networking Supplement.)

Because of these memberships, users of the domain have normal user access to and abilities for the domain and the computers in the domain running Windows NT Workstation and Windows NT Server as member servers. (However, you can prevent Domain Users from being granted this access on a particular workstation or on a server that is not a domain controller by removing the Domain Users global group from that computer's Users group.)

Domain Guests

The Domain Guests global group initially contains the domain's built-in Guest user account. If you add user accounts that are intended to have more limited rights and permissions than typical domain user accounts, you might want to add those accounts to the Domain Guests group and remove them from the Domain Users group.

The Domain Guests global group is a member of the domain's Guests local group.

Global group	**Initial contents**	**Who can modify**[1]
Domain Admins	Administrator	Administrators
Domain Users	Administrator	Administrators, Account Operators
Domain Guests	Guest	Administrators, Account Operators

[1] None of these groups can be deleted.

Creating New Groups

To create and define additional groups, use User Manager for Domains:

- Create new *local* groups for granting permissions to resources.
- Create new *global* groups to organize users based on the type of work they do.

For example, suppose you have a color printer in your domain, and you want to restrict access to it:

1. Create a local group that has permission to print on the color printer.
2. Create a global group consisting of users who are allowed to use the color printer.
3. Add the global group to the local group.
4. Add or remove people who can use the printer by changing the membership of the global group.

If you want members of this group to be able to use a printer connected to a particular workstation or member server, add the global group to the local group that governs printing on *that* computer. Likewise, if a color printer is available on a trusting domain, you can place your global group into a local group in that domain.

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

When adding a group you will be asked to provide a *group name*. It must be unique to the domain or to the computer being administered. A global group name can contain up to 20 characters. It can also contain any uppercase or lowercase characters except the following:

" / \ [ ] : ; | = , + * ? < >

A local group name can contain up to 256 characters. It can also contain any uppercase or lowercase characters except the backslash character (\).

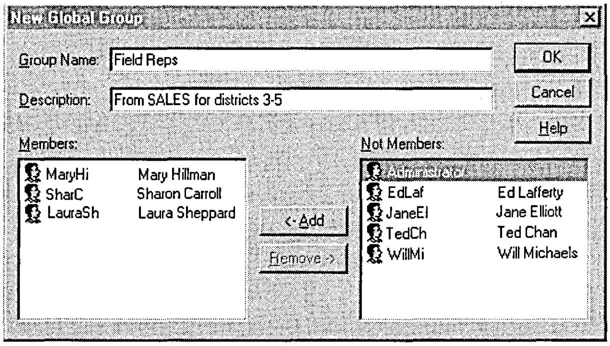
A global group name cannot consist solely of periods (.) and spaces.

Note When a group name is displayed and when the distinction is necessary, Windows NT Server identifies the domain or workstation the group is from by presenting the name in the form DOMAINNAME\groupname or COMPUTERNAME\groupname. For example, a group named Managers from a domain named Engineering would be displayed as ENGINEERING\Managers.

To create a new group, you either copy an existing group or create a completely new one. By copying, you ensure that the new group has the same members as the original group. However, the permissions and rights of the original group are not copied to the new group.

Creating a New Global Group

To create a new global group, you give the group a name and then add members (user accounts in the local domain) to it.



Group Name: Field Reps

Description: From SALES for districts 3-5

Members:

MaryHi	Mary Hillman
SharC	Sharon Carroll
LauraSh	Laura Sheppard

Not Members:

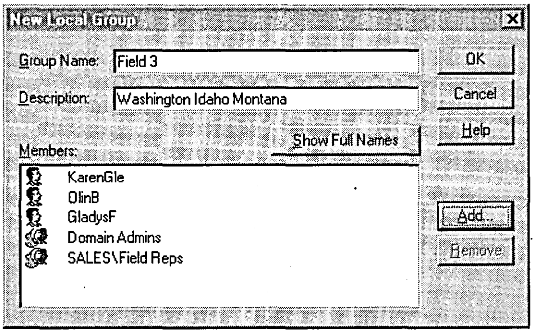
Administrator	
EdLaf	Ed Lafferty
JaneEl	Jane Elliott
TedCh	Ted Chan
WillMi	Will Michaels

Note When **Low Speed Connection** is chosen on the **Options** menu in User Manager for Domains, global groups cannot be created, modified, or copied.

For information about how to manage global groups, see "Creating a New Global Group", "Copying a Global Group", and "Managing Global Group Properties" in User Manager for Domains Help.

Creating a New Local Group

To create a new local group, give the group a name and then add members (user accounts and global groups from the local domain or a trusting domain) to it.


New Local Group

Group Name: Field 3

Description: Washington Idaho Montana

Members:

- KarenGle
- OlinB
- GladysF
- Domain Admins
- SALES\Field Reps

For information about how to manage local groups, see "Creating a New Local Group", "Copying a Local Group", and "Managing Local Group Properties" in User Manager for Domains Help.

Changing a Group's Membership or Description

You can add new members or remove members or change the description of a local group or a global group by selecting a group in User Manager for Domains and clicking **Properties** on the **User** menu.

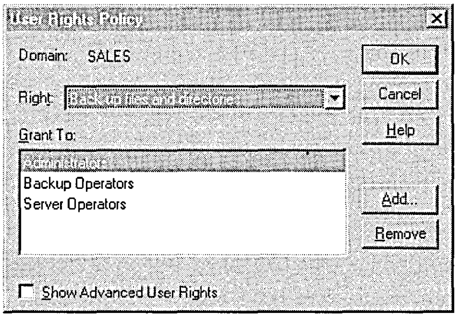
For information about how to add, remove, or change group members, see "Managing Global Group Properties" and "Managing Local Group Properties" in User Manager for Domains Help.

Granting Rights to a Local Group

You can grant or revoke rights to and from users and groups. You cannot control other abilities directly. They are granted to some built-in local groups when Windows NT Workstation or Windows NT Server is installed. The only way for you to grant a user one of these built-in abilities is to make that user a member of the appropriate local group. For example, the only way to allow a person to create user accounts on a domain is to add that person's account to either the Administrators or Account Operators local group on the domain. The built-in abilities of local groups for workstations and member servers, as well as for domain controllers, are listed in "Built-in Local Groups — Controlling What Users Can Do" earlier in this chapter. On Windows NT Server domains, rights are granted and restricted on the domain level; if a group has a right in a domain, its members have that right on all primary and backup domain controllers in the domain. On each Windows NT Workstation computer and on each Windows NT Server computer that is not a domain controller, rights granted apply only to that single computer.

- When you create new local groups in a domain, User Manager for Domains is used to grant rights to the group.
- When you create new local groups on a workstation or member server, User Manager (or User Manager for Domains remotely) is used to grant rights to the group.

The **User Rights** command on the **Policy** menu lets you grant user rights to local groups. The **User Rights Policy** dialog box lists each right selected and the groups that have them. You can add or remove groups from the **Grant To** list.



User Rights Policy

Domain: SALES

Right: Back up files and directories

Grant To:

Administrators
Backup Operators
Server Operators

For information about how to grant user rights, see "Managing the User Rights Policy" in User Manager for Domains Help.

Deleting a Group

Groups created with User Manager for Domains can be deleted, but the built-in groups provided with Windows NT Server and Windows NT Workstation cannot. Deleting a group removes only that group; it does not delete the user accounts or global groups that are members of the deleted group

A deleted group cannot be recovered, so be sure you want to delete a group before you do so. When you delete a group, the SID for the group account is deleted, and SIDs are used only once. For this reason, resource permissions associated with the group cannot be reestablished by creating a new group using the same account name.

For information about how to delete groups, see “Deleting a Local Group” and “Deleting a Global Group” in User Manager for Domains Help.

CHAPTER 3

Managing User Work Environments

User work environments include the desktop items and settings, such as screen colors, mouse settings, window size and position, and network and printer connections.

You can use the following tools to manage user work environments on a Windows NT Server network:

- User profiles

  The user profile contains all user-definable settings for the work environment of a computer running Windows NT, including display settings and network connections. All user-specific settings are automatically saved into the Profiles folder within the system root folder (typically C:\winnt\profiles).

- System Policy Editor

  System policy enables you to control the user-definable settings in Windows NT and Windows 95 user profiles, as well as system configuration settings. You can use the System Policy Editor to change desktop settings and restrict what users can do from their desktops.

- Logon scripts

  A logon script is a batch file (.bat) or executable (.exe) file that runs whenever a user logs on at any type of workstation on the network. The script can contain operating system commands, such as commands to make network connections or start applications.

- Environment variables

  Environment variables specify the computer's search path, directory for temporary files, and other similar information.

User Profiles

On computers running Windows NT Workstation or Windows NT Server, *user profiles* automatically create and maintain the desktop settings for each user's work environment on the local computer. A user profile is created for each user when the user logs on to a computer for the first time.

User profiles provide several advantages to users:

- When users log on to their workstations, they receive the desktop settings as they existed when they logged off.
- Several users can use the same computer, and each receives a customized desktop when they log on.
- User profiles can be stored on a server so that user profiles can follow users to any computer running the Windows NT version 4.0 platform on the network. These are called *roaming* user profiles.

As an administrative tool, user profiles provide these options:

- You can create customized user profiles and assign them to users to provide consistent work environments that are appropriate to their tasks.
- You can specify common group settings for all users.
- You can assign mandatory user profiles to prevent users from changing any desktop settings.

User profiles can be used on computers running Windows 95, but they must be enabled before they are available. User profiles have no effect on computers running MS-DOS, UNIX, or OS/2.

For more information on using user profiles with computers running Windows 95, see "Using Windows 95 User Profiles on Windows NT Server Networks" later in this chapter.

Settings Saved in a User Profile

A user profile contains configuration preferences and options for each user: a snapshot of a user's desktop environment.

The following table describes the settings in a user profile.

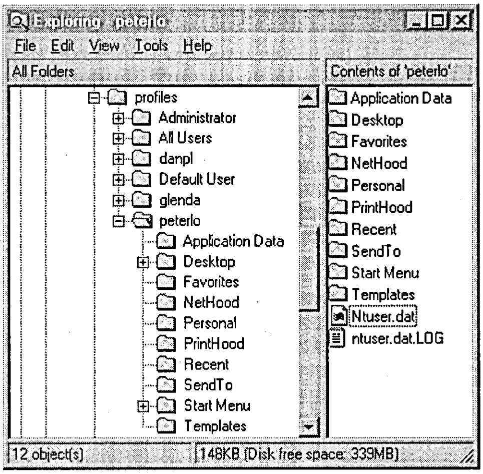
Source	Parameters saved
Windows NT Explorer	All user-definable settings for Windows NT Explorer.
Taskbar	All personal program groups and their properties, all program items and their properties, and all Taskbar settings.
Printers Settings	Network printer connections.
Control Panel	All user-defined settings made in Control Panel.
Accessories	All user-specific application settings affecting the user's Windows NT environment, including Calculator, Clock, Notepad, Paint, and HyperTerminal, among others.
Windows NT-based applications	Any application written specifically for Windows can be designed so that it tracks application settings on a per-user basis. If this information exists, it is saved in the user profile.
Online Help bookmarks	Any bookmarks placed in the Windows NT Help system.

Structure of a User Profile

Every user profile begins as a copy of *Default User*, a default user profile stored on each computer running Windows NT Workstation or Windows NT Server. The NTuser.dat file within Default User displays configuration settings from the Windows NT Registry. Every user profile also uses the *common program groups*, contained in the All Users folder.

User Profile Folders

Every user profile begins as a copy of *Default User*, a default user profile stored on each computer running Windows NT Workstation or Windows NT Server. The Default User profile folder, user profile folders for each user, and All User profile folders are located in the Profiles folder in the system root (usually C:\Winnt). The Default User folder and individual user profile folders contain an NTuser.dat file plus a directory of links to desktop items.



12 object(s) 148KB (Disk free space: 339MB)

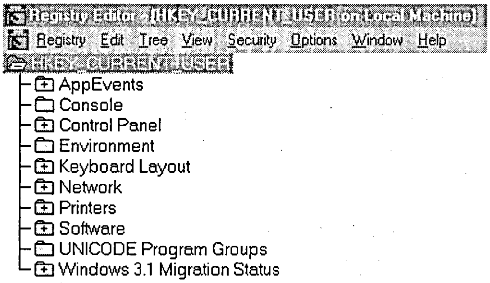
The user profiles folders contain links to various desktop items.

User profile folder	Contents
Application Data	Application-specific data. For example, a customer dictionary. Application vendors decide what data to store in the User Profile folder.
Desktop	Desktop items, including files and shortcuts.
Favorites	Shortcuts to program items and favorite locations.
NetHood	Shortcuts to Network Neighborhood items.
Personal	Shortcuts to program items.
PrintHood	Shortcuts to printer folder items
Recent	Shortcuts to the most recently used items.
SendTo	Shortcuts to document items.
Start Menu	Shortcuts to program items.
Templates	Shortcuts to template items.

Note The NetHood, PrintHood, Recent, and Templates folders are hidden and, by default, do not appear in Windows NT Explorer. To view these folders and their contents in Windows Explorer, click **Options** on the **View** menu, and then click **Show all files**.

NTuser.dat File

The *NTuser.dat* file is the registry portion of the user profile. NTuser.dat is a cached copy of the Windows NT Registry HKEY_CURRENT_USER subtree on the local computer. The registry is a database repository for information about the computer's configuration, including the hardware, installed software, environment settings, and other information. In the registry, the settings that determine the work environment for the user who is currently logged on to the computer are stored in HKEY_CURRENT_USER.


Registry Editor - [HKEY_CURRENT_USER on Local Machine]
Registry Edit Tree View Security Options Window Help
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Environment
Keyboard Layout
Network
Printers
Software
UNICODE Program Groups
Windows 3.1 Migration Status

All Users Folder

Although they are not copied to user profile folders, the settings in the All Users folder are used with user profile folders to create the user profile.

The Windows NT platform supports two program group types:

- *Common program groups* are always available on a computer, no matter who is logged on. Only administrators can add, delete, and modify them.
- *Personal program groups* are private to the user who creates them.

Common program groups are stored in the All Users folder under the Profiles folder. The All Users folder also contains settings for the Desktop and **Start** menu.

On computers running Windows NT Workstation or Windows NT Server, only members of the Administrators group can create common program groups.

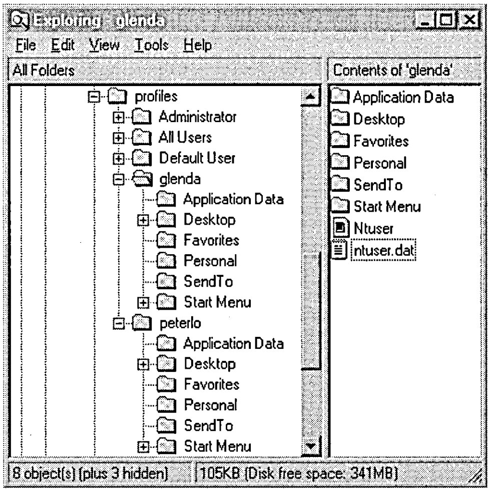
For information on adding new program groups, see "To add a new submenu to the Programs menu" in Windows NT Help.

How Local User Profiles Are Created

The local user profile is the user profile stored on the computer under the user name in the Profiles folder. When no preconfigured server-based (roaming) user profile exists for a user, the first time a user logs on to a computer, a user profile folder is created for the user name. The contents of Default User are then copied to the new user profile folder. The user profile, along with the common program group settings in the All Users folder, create the user's desktop. When the user logs off, any changes made to the default settings during the session are saved to the new user profile folder. The user profile in Default User remains unchanged.

If the user has a user account on the local workstation in addition to a domain user account or more than one domain user account, the local user profile is different for each account because different user profiles are generated for each user that logs on. When the user logs off, changed settings are saved to only one user profile, depending on which account the user logged on to.

When a user has a local user profile on a computer, the user profile folder contains the NTuser.dat file and a transaction log file named NTuser.dat.LOG. The log file is used to provide fault tolerance, allowing Windows NT to recover if a problem occurs while the NTuser.dat file is being updated.



Using Roaming User Profiles

Roaming user profiles can be implemented in three ways:

- Add a user profile path to each user account to automatically create an empty user profile folder named for the user in the server location and to allow users to create their own user profiles.

- Add a user profile path to each user account and copy a preconfigured user profile to the user profile path specified in each user account.
- Add a user profile path to each user account, copy a preconfigured user profile to the user profile path specified in each user account, and then rename the NTuser.dat file to NTuser.man in the user profile path specified in each user account. This creates a mandatory user profile.

In User Manager For Domains, you can assign a server location for user profiles. If you enter a user profile path into a user's domain account, a copy of the user's local user profile is saved both locally and in the user profile path location when the user logs off. The next time that user logs on, the user profile in the user profile path location is compared to the copy in the local user profile folder and the most recent copy of the user profile is opened. The local user profile becomes a roaming user profile by virtue of the centralized domain location. It is available wherever the user logs on, providing the server is available.

If the server is not available, the local cached copy of the roaming user profile is used. If the user has not logged on to the computer before, a new local user profile is created. In either case, if the centrally stored user profile is not available at logon, it is not updated when the user logs off. If the user profile is not downloaded due to server problems, it is not uploaded when the user logs off. The next time the user logs on, they must specify which user profile to use — the newer locally cached copy of the user profile or the older centrally stored copy.

To create a preconfigured roaming user profile, use User Manager for Domains to assign a server location for a user profile and then use the **User Profile** tab of the System option in Control Panel to copy a preconfigured user profile to the server. The first time the user logs on, instead of getting a copy of the Default Profile, the user gets a copy of the preconfigured user profile from the server. Thereafter, the user profile functions just like a standard roaming user profile. Each time the user logs off, the user profile is saved locally and is also copied to the server.

Note To copy a user profile, you must use the **User Profile** tab of the System option in Control Panel. You cannot use Windows NT Explorer or any other file management tool.

A mandatory user profile is just a preconfigured roaming user profile that the user cannot update. The user can still modify the desktop, but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile is downloaded again. User profiles become mandatory when you rename the NTuser.dat file on the server to NTuser.man. This extension makes the user profile read-only.

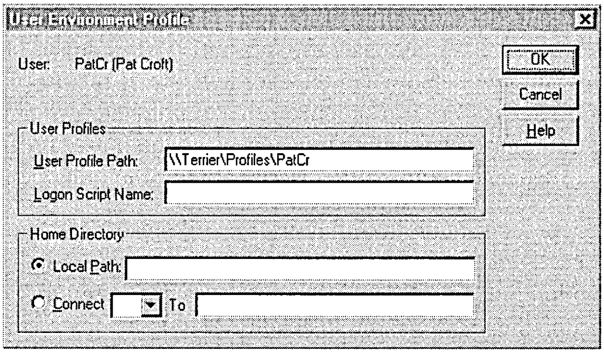
The same mandatory user profile can be used by as many users as needed.

Tip When control over user choices and work styles is desirable for either security or to compensate for user computer skills, system policy offers more choices for control. You can select a subset of settings to control, and you can control both user and computer settings. For more information, see "System Policy" later in this chapter.

For information on modifying user accounts, see User Manager for Domains Help.

Adding the User Profile Path to User Accounts

In User Manager for Domains, you can use the **User Environment Profile** dialog box to add the user profile path location. Open the **User Properties** dialog box for a user account, and click the **Profiles** button to add the user profile path.



User Environment Profile

User: PatCr (Pat Croft)

User Profiles

User Profile Path: \\Terrier\Profiles\PatCr

Logon Script Name:

Home Directory

● Local Path:

○ Connect To

Use a full path in each user account:

*server**share*\*profilename*

For *share*, create a Profiles folder if it does not already exist and share the folder with Everyone.

For *profilename*, use the user name for the user account.

The user profile path location can be on any server; it does not have to be a domain controller. When the user logs on, Windows NT Server checks the user's account to see if there is a user profile path. If the path exists, the user profile is located by the system.

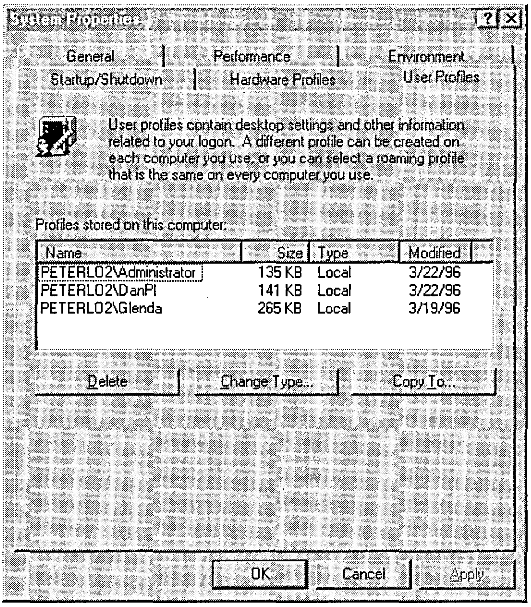
For information on modifying user accounts, see User Manager for Domains Help.

Copying the User Profile to the Server Location

To provide a specific user profile for some users, copy the user profile to the proper location by running Control Panel, choosing System, and then selecting the **User Profiles** tab. This location must match the **User Profile Path** entry for the user's account in User Manager For Domains.

In the **User Profiles** tab in the **System Properties** dialog box, all user profiles that have been created on the computer are listed in the **Profiles Stored On This Computer** box.

To copy a specific user profile, click **Copy To**, and then either type the name of the destination folder or browse the network for it.



User profiles contain desktop settings and other information related to your logon. A different profile can be created on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

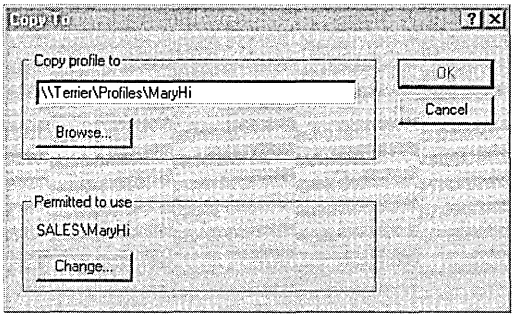
Name	Size	Type	Modified
PETERLO2\Administrator	135 KB	Local	3/22/96
PETERLO2\DanPl	141 KB	Local	3/22/96
PETERLO2\Glenda	265 KB	Local	3/19/96

For more information on creating preconfigured user profiles, see "Preparing Preconfigured Roaming and Mandatory User Profiles" later in this chapter.

For information on copying user profiles, see Control Panel Help.

Adding Users and Groups to the Permissions List for a Roaming User Profile

The System option in Control Panel also copies appropriate permissions along with the user profile so that users have access to the user profile. However, when you copy a user profile to a location for use by another user or group, you must add the user or group to the permissions list. The **Permitted to use** box shows the user who has permissions to use the user profile. Click **Change** to add the user or group to the permissions list for the user profile.



Copy To

Copy profile to: \\Terrier\Profiles\MaryHi

Permitted to use: SALES\MaryHi

Note If you assign a roaming user profile path to a group, each time a group member logs off, his or her user profile is written over the centrally stored user profile. For this reason, it is best to make group user profiles mandatory, or use system policy to specify different settings for different groups.

For information about system policy, see "System Policy" later in this chapter.

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

For information on adding users and groups to a permissions or auditing lists, see User Manager for Domains Help.

For information on modifying user accounts, see "To configure the user environment profile" in User Manager for Domains Help.

Changing the User Profile Type for Slow Connections

Users who log on to the network over slow links, such as when using a Remote Access Service (RAS) connection, can use their local user profile instead of slowing their logon for the process of downloading the roaming user profile from the server. When a user logs on under these conditions, a dialog box appears allowing the user to specify which user profile to load.

When already logged on, you can use the System option in Control Panel to change your user profile type from roaming to local and vice versa. The setting remains in effect until you change it. When you change the type from roaming to local, the cached copy of your roaming user profile is opened every time you log on, and changes are saved to that local user profile only.

For information on changing your profile type, see "To switch between a roaming and local user profile" in System Policy Editor Help.

Preparing Preconfigured Roaming and Mandatory User Profiles

Although you can use any account to create a preconfigured roaming or mandatory user profile, it is often more convenient and efficient to use a test account. For example, if you plan to create and maintain three different preconfigured roaming or mandatory user profiles for your sales, payroll, and production departments, create three different test accounts called Sales Profile, Payroll Profile, and Prod Profile. Then, log on with each account to create the appropriate user profile for the user group. After you log back on as Administrator, use User Manager for Domains to modify the user's individual accounts or the appropriate group account, and then use the **User Profile** tab of the System option in Control Panel to copy the user profiles to the appropriate server.

Allowing for Different Hardware Configurations

Because user profiles can be used on various types of workstations, you should keep in mind that these workstations can have different hardware configurations, particularly different video cards and display monitors.

Because a user profile determines screen placement and size of windows, the type of display hardware a workstation has affects how well the user profile works. For example, the window setup in a user profile created for a computer with a super-VGA screen may not look correct when loaded on a computer with a regular VGA monitor.

To prevent problems:

- When creating or editing a user profile for a single user, use a computer with the same type of video hardware as the computer the user typically uses.
- When creating a mandatory user profile for several users, create a single user profile for the whole group of users only if they all use computers with the same type of video hardware.

Deleting a User Profile

If you no longer want to use a roaming or mandatory user profile that is assigned to users delete the user profile path from the user accounts in User Manager for Domains.

To delete a user profile from the centrally stored location, use the **User Profile** tab of the System option in Control Panel.

For information on modifying user accounts, see User Manager for Domains Help.

Customizing the Default User Profile for All Computers on a Domain

If you want to create a customized domain-wide default user profile for all computers running Windows NT Workstation or Windows NT Server, you can create a customized user profile and copy it to the domain PDC using the **User Profile** tab of the System option in Control Panel.

Log on to any computer running Windows NT Workstation or Windows NT Server, create a custom user profile, and then log off. Log back on to the computer using the Administrator account, and use the **User Profile** tab of the System option in Control Panel to copy your customized version to the Netlogon folder in the system root folder on the PDC.

For example, if the domain controller is named Central, copy the user profile to \\Central\Netlogon\Default User. The Default User directory is created, and the links and NTuser.dat file are copied.

When you copy the user profile, in the **Copy To** dialog box you permit Everyone to use the user profile. This user profile is downloaded to the Default User (Network) folder on every computer at startup.

For information on customizing the Default User profile for all computers in a domain, see “To change the local default user profile” in System Policy Editor Help.

For information about synchronization, see Chapter 1, “Managing Windows NT Server Domains.”

Customizing the Local Default User Profile for One Computer

You can customize a particular computer's default user profile when special circumstances require that a computer perform in a consistent way that is different from other computers. For example, if you want to have one computer with certain applications and settings preset for a specialized or dedicated task, you can create a custom user profile and copy it to the Default User folder.

System Default Profile

When Windows NT is running on a computer that no user is logged on to, a dialog box appears, prompting you to press CTRL+ALT+DEL to log on. This dialog box and other aspects of the Windows NT environment at this point, such as the screen's background color and its use of wallpaper and screen savers, are controlled by the system default profile. The settings for this profile are stored in System32\config\default. The system default profile can be changed by using Windows NT Registry Editor to edit the .Default key in HKEY_USERS.

For information about using Windows NT Registry Editor, see Appendix A, "Windows NT Registry."

Using Windows 95 User Profiles on Windows NT Server Networks

Unlike user profiles in Windows NT Workstation and Windows NT Server, which are automatic and always available, user profiles in Windows 95 must be enabled on the local computer using the Passwords option in Control Panel. Once enabled, user profiles are used as follows:

- Windows 95 local user profiles operate the same way as user profiles operate in Windows NT Workstation and Windows NT Server.
- Roaming user profiles can be used on a Windows NT Server network if Client for Microsoft Networks is selected as the primary network logon client, or on a NetWare network if Client for NetWare Networks is selected as the primary network logon client.
- Mandatory user profiles can be used but must be created for each user.

Windows 95 and Windows NT User Profile Differences

Because of the differences between Windows 95 user profiles and Windows NT user profiles, you cannot create user profiles for Windows 95 clients on a computer running Windows NT Workstation or Windows NT Server.

Registry File Differences

Different files are used for the registry portion of user profiles in Windows 95 than are used in user profiles in Windows NT.

Windows NT Server	Windows 95
NTuser.dat	User.dat
NTuser.dat.LOG	User.da0
NTuser.man	User.man

Note The Windows 95 User.da0 and Windows NT Server files provides slightly different functionality. While Windows 95 writes a copy of User.dat to User.da0 each time the user logs off, Windows NT uses NTuser.dat.LOG as a transaction log file to provide fault tolerance. This allows Windows NT to recover the user profile if a problem occurs while Windows NT is updating NTuser.dat.

File Structure Differences

The same folder structure is used for both Windows NT and Windows 95 with one exception: Windows 95 does not support the Application Data folder.

Functional Differences

Windows NT and Windows 95 profiles have the following functional differences:

- Windows 95 does not support common groups
- Windows 95 user profiles do not copy all desktop items–only shortcut (.lnk) and program information (.pif) files.
- Windows 95 user profiles don't support a centrally stored Default User profile.
- Windows 95 clients don't use the Windows NT Server profile path to obtain roaming user profiles. They can be retrieved only from the user's home directory.
- To use mandatory user profiles on computers running Windows 95 on a Windows NT Server network, an administrator must create a custom user profile for each user and copy the user profile files to each user's home directory.

For more information on common groups, see "All Users Folder" earlier in this chapter.

For more information on using a centrally stored Default User profile, see "Customizing the Default User Profile for All Computers on a Domain" earlier in this chapter.

For more information on Windows 95 user profiles, see the *Windows 95 Resource Kit.*

How User Profiles are Updated for Windows NT 4.0

When upgrading from Windows NT Server 3.5*x* to Windows NT Server 4.0, user profiles undergo format changes that consist of changing the user profile from a single file (version 3.5*x*) to a folder (version 4.0) containing the user profile plus a directory of links to various desktop items.

When roaming user profiles exist in Windows NT 3.5*x*, upgrading to version 4.0 has the following effects:

- The original roaming user profile is retained in the same server location.
- A new user profile is created in Windows NT 4.0 that consists of the original user profile updated to the Windows NT 4.0 format.
- Both versions remain available to users, so they can continue to use computers running Windows NT 3.5*x* and receive their roaming user profiles. However, if a user uses both operating systems, the two user profile versions are stored and updated separately.

Note Although roaming user profiles from both Windows NT version 3.5*x* and 4.0 are available to users, local user profiles are converted to Windows NT version 4.0 user profile format.

File name extensions of user profiles in Windows NT 3.5*x* change to the 4.0 version of the user profile type, and the NTuser file is added to each user profile folder with the appropriate extension for a roaming or mandatory user profile.

Windows NT 3.5*x* type and file name	Windows NT 4.0 type, folder name, and NTuser file name and extension
Roaming/personal = username.usr	Roaming = username.pds
	file name = NTuser.dat
Mandatory = username.man	Mandatory = username.pdm
	file name = NTuser.man

Note The .pds and .pdm extensions for username files stand for profile directory structure and profile directory mandatory, respectively.

Logging on For the First Time After an Upgrade

The first time a user that has been using a Windows NT 3.5*x* roaming user profile logs on to a computer running Windows NT 4.0, a Windows NT version 4.0 user profile folder is created on the server. The user profile folder is named for the user name from the Windows NT 3.5*x* user profile, with the addition of a .pds extension. For example, if your Windows NT 3.5*x* user profiles is Joe.usr, a Joe.pds folder is created the first time Joe logs on to a computer running Windows NT 4.0. The Joe.pds folder is then propagated with the appropriate folders and files to create Joe's Windows NT 4.0 user profile.

You do not have to change the user profile path in User Manager for Domains. Each time Windows NT version 4.0 sees that your user account specifies a Windows NT 3.5*x* user profile (identifiable by a .usr extension), Windows NT automatically looks for the same user profile, but with a .pds extension. For example, if you log on to a computer running Windows NT Workstation version 4.0, and your user account specifies \*server**share**username*.usr, Window NT looks for \*server**share**username*.pds.

Mandatory User Profile Upgrade

Upgrading of mandatory user profiles from Windows NT Server version 3.5*x* to 4.0 is not automatic. The following steps explain how to set up a mandatory user profile in Windows NT Server 4.0 and have it coexist with a mandatory user profile created in Windows NT Server 3.*x*.

- Log on to a computer and create a user profile with the settings you want for the mandatory user profile.
- Log off the computer and log back on as Administrator.
- Use the **User Profile** tab in the System option in Control Panel to copy the new user profile to the user profile path location. Give the new user profile folder the same name as the 3.5*x* user profile name, but add the .pdm extension (to keep the new user profile from overwriting the 3.5*x* user profile).

  \\server\share\profilename.pdm
- In the new user profile folder, rename NTuser.dat to NTuser.man.

The first time a user logs on to a computer running Windows NT Workstation or Windows NT Server 4.0, the mandatory user profile is downloaded to the local computer.

The 3.5*x* user profile still exists as *profilename.man* in the same user profile path location. When the user logs on to a computer running Windows NT Workstation or Windows NT Server version 3.5*x*, the 3.5*x* version of the mandatory user profile is downloaded from the server.

Note An alternative to creating a new registry file (NTuser.man) for the mandatory user is to follow the preceding steps, and then copy the 3.5*x* mandatory user profile into the user profile path folder as NTuser.man (replacing the existing file). However, because 3.5*x* mandatory user profiles undergo an upgrade the first time they are downloaded to a computer running Windows NT Workstation or Windows NT Server 4.0 and because the server copy of the user profile is never overwritten by the local user profile, the upgrade process must take place each time the user logs on. To avoid this inconvenience, it is best to create a new mandatory user profile when upgrading.

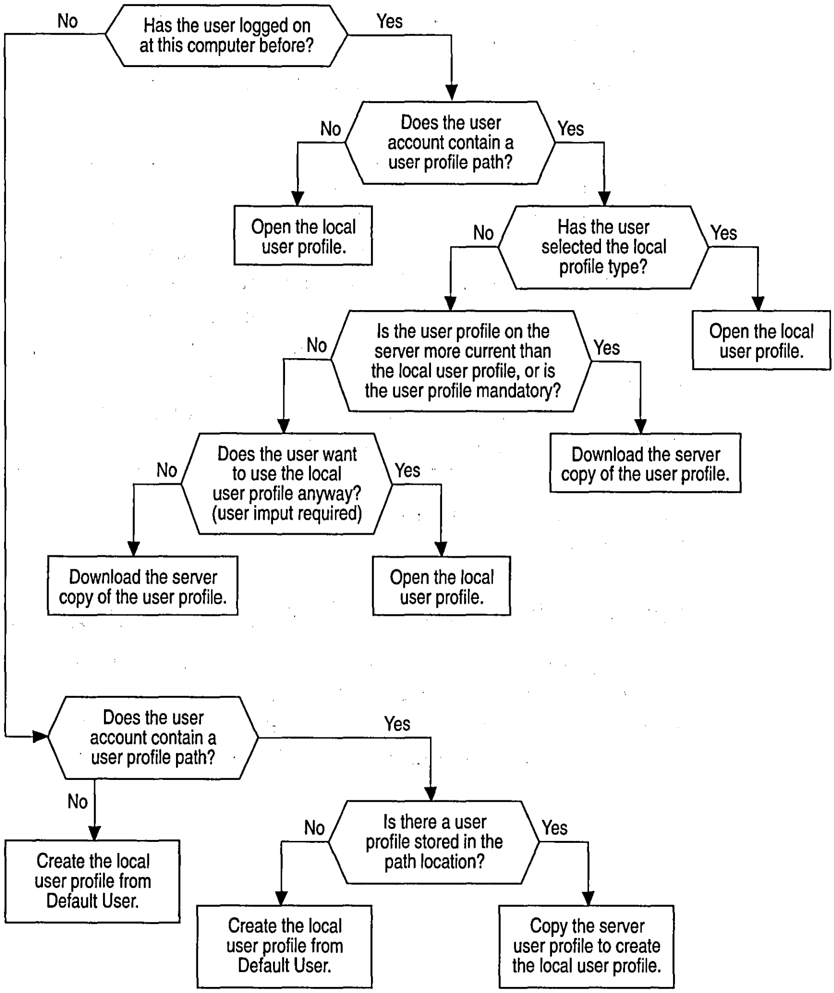
For information on modifying multiple user accounts, see User Manager for Domains Help.

System Policy as an Alternative to Mandatory User Profiles

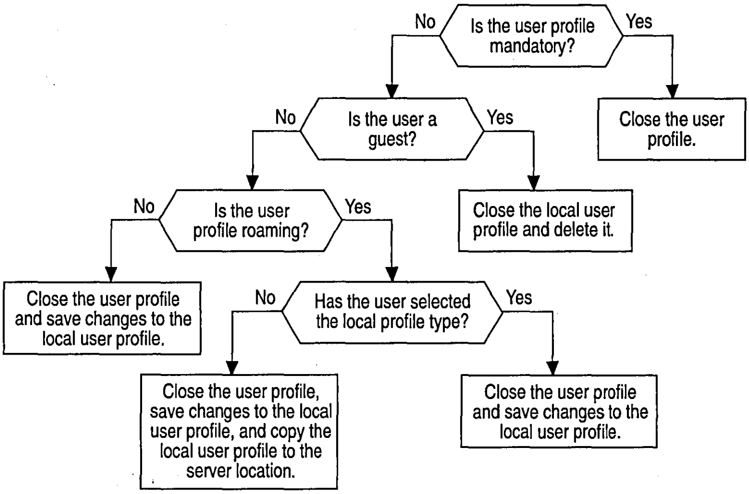
When upgrading to Windows NT Server 4.0, you might consider the added control of system policy as a replacement for old mandatory user profiles. With system policy, you can mandate all the user profile settings of a mandatory user profile, plus control computer-specific settings as well.

How User Profiles are Opened and Saved

The sequence for opening user profiles at logon is shown in the following chart.


No
Has the user logged on at this computer before?
Yes
No
Does the user account contain a user profile path?
Yes
Open the local user profile.
No
Has the user selected the local profile type?
Yes
Open the local user profile.
No
Is the user profile on the server more current than the local user profile, or is the user profile mandatory?
Yes
Download the server copy of the user profile.
No
Does the user want to use the local user profile anyway? (user imput required)
Yes
Download the server copy of the user profile.
Open the local user profile.
Does the user account contain a user profile path?
Yes
No
Create the local user profile from Default User.
No
Is there a user profile stored in the path location?
Yes
Create the local user profile from Default User.
Copy the server user profile to create the local user profile.

The following chart shows the sequence for saving user profiles at logoff.


Is the user profile mandatory?
No
Yes
Close the user profile.
Is the user a guest?
No
Yes
Close the local user profile and delete it.
Is the user profile roaming?
No
Yes
Close the user profile and save changes to the local user profile.
Has the user selected the local profile type?
No
Yes
Close the user profile, save changes to the local user profile, and copy the local user profile to the server location.
Close the user profile and save changes to the local user profile.

System Policy

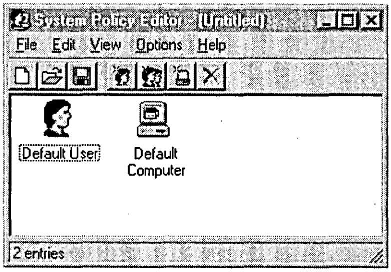
On computers running Windows NT Workstation or Windows NT Server, the contents of the user profile are taken from the user portion of the Windows NT Registry. Another portion of the registry, the local computer portion, contains configuration settings that can be managed, along with user profiles, using System Policy Editor. With this tool, you create a *system policy* to control user work environments and actions, and to enforce system configuration for all computers running Windows NT Workstation and Windows NT Server.

With system policy, you can control some aspects of user work environments without enforcing the restrictions of a mandatory user profile. You can restrict what users can do from the desktop; such as restrict certain options in Control Panel, customize parts of the desktop, or configure network settings.

How System Policy Works

The desktop settings in user profiles, as well as logon and network access settings, are stored in the computer's registry database. *System policy for users* overwrites settings in the current user area of the registry, and *system policy for computers* overwrites the current local machine area of the registry. This allows you to control user actions (user profiles) as well as computer actions for users and groups. In System Policy Editor, you manage the user desktop by changing the **Default User** settings, and you manage the logon and network settings by changing the **Default Computer** settings.

Using System Policy Editor, you create a file called NTConfig.pol that contains settings for users (user profiles) and computers (logons and network access settings). To enable a uniform policy for all network computers running Windows NT Server, Windows NT Workstation, you save this file to the Netlogon folder in the system root folder of the primary domain controller: \\PDCservername\Netlogon.


System Policy Editor - (Untitled)
File Edit View Options Help
Default User
Default Computer
2 entries

When a user logs on to any network computer running Windows NT, the operating system looks in the Netlogon folder in the logon server's system root folder to see if there is an NTConfig.pol file present. If the file is found, the contents of the file are copied to the local computer's registry, and is used to overwrite the current user and local machine portions of the registry.

System Policy Editor entries change local computer registry settings in the following ways:

- Desktop settings for Default User in System Policy Editor modify the HKEY_CURRENT_USER key in the registry, which defines the contents of the user profile that is in effect for the computer.
- Logon and network access settings for Default Computer in System Policy Editor modify the HKEY_LOCAL_MACHINE key in the registry.

When a user logs on to the domain, the contents of the NTConfig.pol file on the server are merged with the NTuser.dat file found in the user profile location for the user logging on. Settings in NTuser.dat that do not match NTConfig.pol settings are overwritten, and thus system policy controls the user profile settings for the entire domain. Settings for Default Computer that are not contained in the user profile are added to the local machine portion of the registry.

Customizing System Policy for Users, Groups, and Computers

If you have special users, groups, or computers that need settings that are different from the default settings, you can change the default settings to accommodate special needs and add users, groups, and computers as appropriate. Users, groups, or computers you add receive separate entries in the NTConfig.pol file that contain the settings that are different from the default system policy settings. When a user or group member who has special policy settings in NTConfig.pol logs on, the system finds NTConfig.pol and also the special settings that apply specifically to the user or group member. Similarly, if a computer is added and special settings entered in System Policy Editor, anyone logging on to that computer receives those computer settings.

Note Computer policy is applied when the user logs on. Policy is taken from the user's logon domain, not the computer's domain. This can cause problems when users log on in different domain, and not all domains use system policy. For example, Sue has a user account in the South domain, and travels to the North site. When she logs on to a computer in the North domain, she is validated by a logon server in the South domain. If Joe, who has a user account in the North domain, logs on after Sue logs off, and the North domain doesn't use system policy, the South domain computer profile is not overwritten and remains in effect. You can correct this problem by implementing system policy on all domains, or using the Manual update mode to load a specify policy on affected computers.

Profile Evaluation for Users and Computers

When multiple profiles apply to one user, a user profile for a specific user takes precedence over a user profile for a group that the user is a member of. Similarly, if no specific user profile has been defined for the user, a group profile for a group that includes the user is used, if available, before the Default User profile is used.

If no computer profile is defined for a specific computer, the Default Computer profile is used. If multiple group profiles apply to a user, they are applied in the order specified in the **Group Priority** dialog box.

For information on specifying system policy for groups, see "To specify system policy priority for groups" in System Policy Editor Help.

Using Manual Update Mode

Manual update mode ensures that system policy is always copied from a specific server, regardless of who logs on. When you can change the remote system policy file update mode from automatic to manual, you specify a path other than the Netlogon folder on the PDC. To use this feature, you must use System Policy Editor on individual computers to change the update path.

For more information on changing the update mode, see "To change the system policy file path for manual update" in System Policy Editor Help.

System Policy Templates

System policy templates allow you to set system policy for networks using computers running Windows NT Workstation and Windows NT Server, Windows 95, or a combination (user profiles must be enabled on each computer running Windows 95). The templates provide the necessary framework for overwriting the Registry keys on the different systems.

When you install System Policy Editor, the following template files are installed automatically:

- WINNT.adm. Provides System Policy Editor settings specific to the Windows NT operating system and registry structure
- WINDOWS.adm. Provides System Policy Editor settings specific to the Windows 95 operating system and registry structure
- COMMON.adm. Provides the System Policy Editor settings that are common to both the Windows NT and Windows 95 registry structures, and that are not contained in either WINNT.adm or WINDOWS.adm.

System policy files created on computers running Windows NT Server cannot be used on computers running Windows 95, and vice versa.

For information about enabling and using user profiles and system policy on Windows 95 computers, see the *Windows 95 Resource Kit.*

For information on loading additional policy templates, see "To add a policy template" in System Policy Editor Help.

Using System Policy Editor to Create System Policy

System Policy Editor can be used to create system policy as follows:

- Create default settings for the computer and user policy for the domain.
- Create custom settings that apply to individual users, groups of users, or individual computers.
- Specify the manner and location from which to download policy for all or some users.

Note The user options described in this section are for computers running Windows NT. For information about Windows 95 system policy settings, see the *Windows 95 Resource Kit.*

Default System Policy Settings: Default Computer and Default User

When you create a new system policy file, System Policy Editor displays two icons representing the computer and user portions of the registry. When you click either **Default Computer** or **Default User**, a graphic representation of categories in the associated portion of the registry appears. Within each major category, subcategories and settings provide options for changing the way computers and users operate. For some settings, selecting a check box opens a set of choices or text boxes; for others, specific information must be provided.

Some settings available in System Profile Editor use the terms *disabled*, *removed*, or *hidden*. These terms explain how the item appears to the user.

- A disabled command appears dimmed on the menu.
- A removed command or item does not appear on the menu.
- A hidden item cannot be seen by the user.

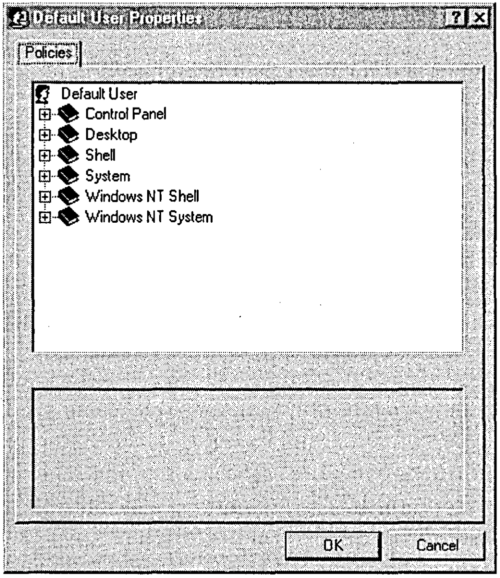
For example, if you select **Hide Screen Saver Tab**, the Screen Saver tab in the **Control Panel Display** option does not appear.

Check-Box Selection Levels

In addition to the usual on/off nature of check boxes, System Policy Editor check boxes have a third setting, which is dimmed. The purpose of the this setting is to indicate that there is no change to the previous setting in the registry.

User Policy: Setting Restrictions on User Profiles

The **Default User** option allows you to control the user profile settings. Each selection in the **Default User Properties** dialog box contains settings that control what the user can do from the desktop to shape the user work environment.



Control Panel

Use this category to restrict the user activity in the Display option in Control Panel or to deny any access to the Display option.

Desktop

You can specify the background wallpaper and color scheme for the desktop.

Shell

In the Shell category, you can customize desktop folders and restrict what appears on the desktop and restrict the use of the **Run**, **Find**, and **Shut Down** commands. You can create custom folders by entering paths to program items, desktop icons, startup items, Network Neighborhood items, and **Start** menu items that you want to come from a location other than user profile folders. You can provide locations for custom desktop icons, applications you want in the Startup folder, or even replace the entire **Start** menu.

System

You can disable Windows NT Registry Editor (Regedt32.exe) and Windows 95 Registry Editor (Regedit.exe) so that users cannot edit the registry files. You can also provide a list of Windows-based applications users can use. Any application not in the list is unavailable.

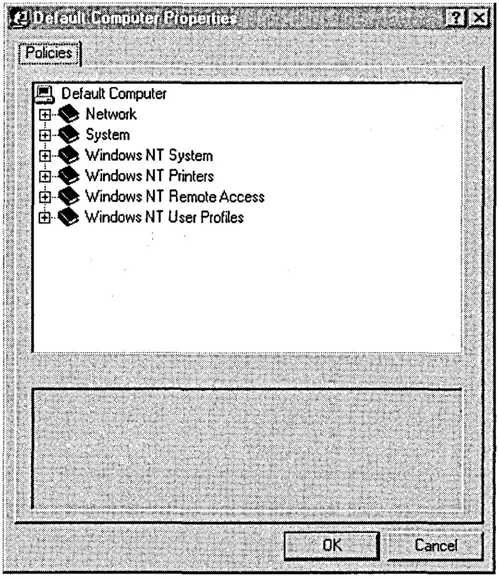
Windows NT System

When you select **Parse Autoexec.bat**, Windows NT reads the environment variables from this file and merges them with the user's environment variables.

For information on managing system policy, see "To manage system policy" in System Policy Editor Help.

Computer Policy: Determining Logon and Network Access

The **Default Computer** option allows you to control logon and network access settings for computers. Each selection in the **Default Computer Properties** dialog box contains settings that prevent users from modifying the hardware and environment settings for the operating system.



Network

You can provide remote update of system policies instead of updating from Ntconfig.pol on domain controllers. By typing a path to a different policy file, you can enable manual update of the policy file in a location other than the server location.

Load Balancing enables computers running Windows 95 to take policies from multiple logon servers. Enabling Load Balancing prevents bottlenecks on large networks when many users try to access the same policy file.

In addition, you can specify to have error messages displayed when a policy cannot be applied.

For information on managing system policy, see "To manage system policy" in System Policy Editor Help.

System

You can specify the contents of the **Run** and **Run once** entries that are used to specify which applications should run at startup.

You can also change default SNMP (Simple Network Management Protocol) configuration by adding or removing communities, managers, and public community traps. The default for these settings are established when the SNMP service is configured on the host. System provides three options for changing default SNMP configuration

Windows NT System

System security. For Windows NT System, you can set logon policy for user accounts, including creating a logon banner and enabling or disabling automatic logon. Automatic logon allows the user to bypass the CTRL+ALT+DELETE key combination when the system is started.

Logon security. Enable or disable the **Shut Down** button in the **Welcome** dialog box. Disabling the button on servers ensures that an unauthorized user cannot shut down the system.

FTP logon policies. For computers running the File Transfer Protocol (FTP) Server Service, you can set policy for allowing and logging anonymous logons, setting a timeout limit for unsuccessful (idle) connections, and specifying the home directory for new users.

Windows NT Printers

For print servers, you can disable the print spooler browse process that periodically sends information to other print servers about which printers the server shares. This browsing consumes some CPU and network capacity, which might not be necessary for some print operations.

You can change the priority of print job assignments to ports and also set the print spooler to beep every 10 seconds if an error condition occurs for a remote print job.

Windows NT Remote Access

When using a remote access server, you can set a maximum number for unsuccessful authentication retries and a maximum time limit for authentication. You can also set the time interval between call-back attempts and a time limit for automatic disconnection from the server.

For information on managing system policy, see "To manage system policy" in System Policy Editor Help.

Using System Policy Editor to Edit the Registry

You can use the **Open Registry** command on the System Policy Editor **File** menu to make changes to the Windows NT Registry settings on the local computer. Using **Open Registry**, the changes you set in System Policy Editor are made immediately in the registry when you use **Save** on the **File** menu.

You can use the **Connect** command on the System Policy Editor **File** menu to make changes to the Windows NT Registry settings on a remote computer. This feature allows remote adjustment to computer registries. For example, a help desk technician can connect to a computer and correct settings that a user mistakenly changed.

Note System policy is designed to manage registry settings for the entire domain; direct changes to registry settings are not recommended unless a specific instance of user or computer incompatibility occurs.

Using Logon Scripts to Configure User Work Environments

A logon script runs automatically whenever a user logs on to a computer running either Windows NT Server or Windows NT Workstation. Although a logon script is typically a batch file (.bat extension), any executable program (.exe extension) can also be used.

Logon scripts are optional. They can be used to configure user working environments by creating network connections and starting applications. Logon scripts are useful when you want to affect the user work environment without managing all aspects of it.

Note User profiles can restore network connections at logon that were established prior to logging off, but they cannot be used to create new network connections at logon.

Creating Logon Scripts

You can create logon scripts using a text editor and then use User Manager for Domains to assign different logon scripts to different users or assign the same logon script to multiple users.

There are several special parameters you can use when creating logon scripts:

Parameter	Description
%HOMEDRIVE%	The user's local workstation drive letter connected to the user's home directory
%HOMEPATH%	The full path of the user's home directory
%HOMESHARE%	The share name containing the user's home directory
%OS%	The operating system of the user's workstation
%PROCESSOR_ARCHITECTURE%	The processor type (such as 80386) of the user's workstation
%PROCESSOR_LEVEL%	The processor level of the user's workstation
%USERDOMAIN%	The domain containing the user's account
%USERNAME%	The user name

Assigning Logon Scripts to User or Group Accounts

You assign a logon script in a user account or group account by entering a path to the logon script file in User Manager For Domains. When a user logs on and a path to a logon script is present in the user account, the file is located and run at logon.

In the **User Environment Profile** dialog box, you can assign logon scripts to user accounts by typing the filename (for example, Clerks.bat) in the **Logon Script Name** box. At logon, the server authenticating the logon locates the logon script (if one is assigned) by looking for the specified file following that server's local logon script path (usually C:\WINNT\System32\Repl\Import\Scripts). If a relative path is provided before the filename (for example, Admins\CristalW.bat), the server looks for the logon script in that subdirectory of the logon script path.

The entry in the **Logon Script Name** box specifies only the filename (and optionally the relative path) and does not create the actual logon script. You create a logon script of the specified name and place it in the appropriate directory on the appropriate replication export server.

You can place a logon script in a local directory of a user's computer, but you usually use this location when you are administering user accounts that exist on a single computer rather than in a domain. In this case, you must place the logon script following the computer's logon script path or in a subdirectory of that logon script path. The logon script path for a Windows NT computer is *systemroot*\System32\Repl\Import\Scripts.

For information on configuring a user environment profile, see User Manager for Domains Help.

Setting Up Replication of Logon Scripts

A logon script is always downloaded from the server that validates a user's logon request. For users with accounts on Windows NT Server domains that have one or more backup domain controllers, any one of the domain controllers can authorize a user's logon attempt. To ensure that logon scripts always work for users, you should be sure that logon scripts for all user accounts in a domain exist on every primary and backup domain controller in the domain.

The best way to ensure that logon scripts are always available is to use the Replicator service. This service maintains identical copies of a directory tree on multiple computers. When you make a change to a file in the master copy of the tree (located on the *export server*), the Replicator service automatically copies the change to the other computers (the *import computers*).

When you use the Replicator service with logon scripts, you set up one domain controller as the export server and all the other domain controllers in the domain as import servers.

The logon script path can be configured for each server of a domain using either Server Manager (administering servers either locally or remotely) or the Server option in each server's Control Panel. Use the **Directory Replication** dialog box to set up replication export and replication import and to specify a local path to user logon scripts.

Usually, a master collection of logon scripts is maintained by an administrator in an export directory (usually C:\WINNT\System32\Repl\Export\Scripts and its subdirectories) of one replication export server in the domain, and this master collection is replicated to all the servers in the domain so that each server has its own local copy of all logon scripts.

For information on Directory Replication, see "Managing Export Replication" and "Managing Import Replication" in Server Manager Help.

For information about directory replication, see Chapter 4, "Managing Shared Resources and Resource Security."

Using Environment Variables to Manage Workstations

When managing multiple user and group accounts, you often need to make the same change to many accounts. You can use environment variables to replace specific names or labels with a general one that is replaced by the appropriate specific data when copied.

Changing the System Environment Variables

Windows NT requires certain information to find programs, to allocate memory space for some programs to run, and to control various programs. This information—called the system and user environment variables—can be viewed using the System option in Control Panel in the **Environment Variables** tab. These environment variables are similar to those that can be set in the MS-DOS operating system, such as PATH and TEMP.

The *system environment variables* are defined by Windows NT Workstation and Windows NT Server and are the same no matter who is logged on at the computer. If you are logged on as a member of the Administrators group, you can add new variables or change the values.

The *user environment variables* can be different for each user of a particular computer. They include any environment variables you want to define or variables defined by your applications, such as the path where application files are located.

After you change any environment variables in **Environment Variables** tab in the **System Properties** dialog box and click **OK**, Windows NT saves the new values in the registry so they are available automatically the next time you start your computer.

If any conflict exists between environment variables, Windows NT Workstation and Windows NT Server resolve the conflict in this way:

- System environment variables are set first.
- Variables defined in Autoexec.bat (except for Path variables) are set next and override system variables.
- User environment variables defined in the System dialog box are set next and override both the system and Autoexec.bat variables.
- Path variables defined in Autoexec.bat are set last.

Note Path settings, unlike other environmental variables, are cumulative. The full path (what you see when you type **path** at the command prompt) is created by appending the path contained in Autoexec.bat to the paths defined in the System option in Control Panel.

Using System Environment Variables in User Profile Paths, Home Directory Paths, and Logon Scripts

Any system environment variable on a client computer running Windows NT Workstation can be used in a user account's user profile path, logon script path, home directory path, and within a logon script itself. To use the system environment variable in this way, enclose it in percent signs (%); for example, to use a client's *servername* environment variable in a user profile path, type **\\%servername%\scripts** in the **User Profile Path** box.

One use of this feature is to ensure that logon scripts and user profiles are run most efficiently on domains that span WAN (wide area network) links, especially if you have users that sometimes work at both sites. Suppose you have two physical sites, Paris and London. On every computer running Windows NT Workstation and Windows NT Server at the London site, set the *servername* system environment variable to the computer name of a backup domain controller in London. On Paris computers set *servername* in a similar way, but use the computer name of a Paris backup domain controller. Then, in every user account in the domain, use *%servername%* in the logon script paths. When a user logs on, the logon script is always loaded from a server at the local site.

CHAPTER 4

Managing Shared Resources and Resource Security

Security on a network running Microsoft Windows NT Server begins with passwords for user accounts and is extended by the rights and permissions granted to users to interact with network resources. The following topics are discussed in this chapter:

- Sharing network resources such as directories, files (including program files), printers, and the ClipBook Viewer
- Securing shared network resources
- *Directory replication*, in which directories shared with multiple users are stored on several computers to speed file access
- Resource monitoring and protection features, including precautions that protect resources from virus and Trojan horse programs

Sharing Network Resources

Windows NT Server enables you to designate resources you want to share with others. For example, when a directory is shared, authorized users can make connections to the directory (and access its files) from their own workstations. And when a printer is shared, many users can print from it over the network.

Once a resource is shared, you can restrict its availability over the network to certain users. These restrictions, called *share permissions*, can vary from user to user. With Windows NT Server, you create the appropriate level of network resource security with a combination of resource sharing and resource permissions.

Differences Between NTFS and FAT Volume Security

Windows NT Server provides superior performance, reliability, and security for file sharing—especially if you use the Windows NT file system (NTFS). With NTFS, you can use permissions to protect individual files, and you can apply this protection for access locally (at the workstation or server where the file is stored) as well as for access over the network.

NTFS File and Directory Permissions

On NTFS volumes, you can set *file permissions* on files and *directory permissions* on directories that specify which groups and users have access and what level of access is permitted. NTFS file and directory permissions apply both to users working at the computer where the file is stored and to users accessing the file over the network when the file is in a shared directory.

Share permissions for NTFS volumes work in combination with file and directory permissions. When a directory is shared, these permissions, set through the shared directory, allow users to connect to the share. Using the default permissions (Full Control) for NTFS shared directories, you can manage the security of the files using directory and file permissions.

Note Using Full Control permission for Everyone for all NTFS shared directories is the easiest way to manage NTFS file security. You can apply directory and file permissions, and allow share access to Everyone through share permissions.

FAT Share Permissions

With volumes that have the file allocation table (FAT) file system, you can protect files only at the directory level, only over the network, and only if the directory is shared. Once a directory is shared, you can protect it by specifying one set of share permissions that applies to the share point, and thus to users who connect to the shared directory over the network. Share permissions are significantly less versatile than the file and directory permissions used for NTFS volumes. File-level protection is not available for FAT volumes.

For information about setting share permissions see "Setting Permissions on Shared Directories," later in this chapter.

File and Directory Compression on NTFS Partitions

Files on NTFS volumes (but not FAT volumes) can be compressed and uncompressed using Windows NT Explorer or the command-line utility **compact**. In the Explorer, right-click any directory or file and click Properties to compress or uncompress:

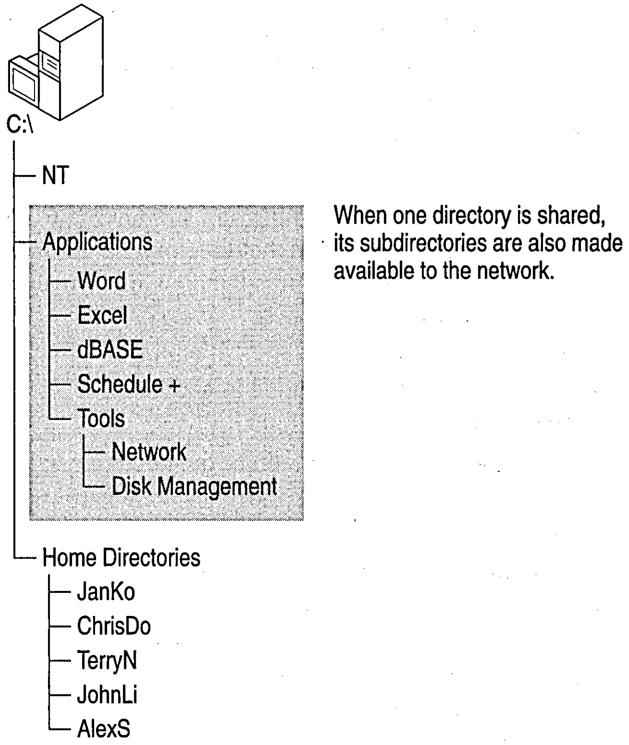
- You can compress one file or all files in a directory. Compressing a directory ensures that new files created in the directory are automatically compressed. Uncompressing a directory ensures that new files created in the directory are created uncompressed.
- When you copy or move a file into a directory or subdirectory within an NTFS volume (or from one NTFS volume to another), the file inherits the compression state of the destination directory.
- When you move a file into a directory or subdirectory within an NTFS volume, the file retains its compression state, regardless of the compression setting of the destination directory.
- When you move a file from one NTFS volume to another, the file inherits the compression state of the destination directory.
- When you compress or uncompress a directory, the Explorer prompts you to indicate whether to compress or uncompress existing subdirectories in the selected directory. Existing subdirectories in compressed or uncompressed directories retain their compression state unless you change it.
- You can choose to highlight compressed files and directories in an alternate color by clicking **Options** on the **View** menu.
- Other file operations can be performed during compression and uncompression.

For information about how to compress and uncompressed files, folders, and volumes, see “To compress a file on an NTFS volume”, and “Compressing an NTFS volume” in Windows NT Help.

Sharing Resources With Network Users

The only way to make a file accessible over the network is to share its directory.

When you share a directory on the server, users can theoretically gain access to that directory, the files in it, all subdirectories of that directory and their contents, and all subdirectories of those subdirectories and their contents, and so on. Every point on the directory tree below the shared directory can be available to network users.



When one directory is shared, its subdirectories are also made available to the network.

However, if the shared directory is in an NTFS volume, you can use directory permissions to effectively block access to some directories in a shared directory tree. A shared directory is often referred to simply as a share. For example, in the preceding figure, you could share the Applications directory but set permissions that restrict access to the dBASE® directory.

When you share a directory, you give it a *share name*, by which network users refer to it. (A share name can be the same as the actual directory name, but it does not have to be.)

Note Windows NT Server, Windows NT Workstation, and Windows 95 users can see share names by double-clicking the names of computers on the network in Network Neighborhood. MS-DOS users can use the **net view** command to see share names. Windows for Workgroups users see share names in File Manager when they connect to a network drive.

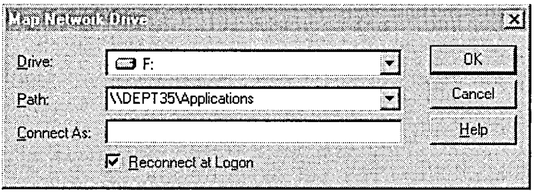
You can share multiple directories on a directory tree, thereby making them accessible to users in two ways: as a directory that is actually shared and as a subdirectory of another shared directory.

Connecting to Shared Directories

There are several ways to connect to shared directories. In Windows NT Server, Windows NT Workstation, and Windows 95, you can use the **Find** command on the **Start** menu to connect to any computer or shared directory on the network, or double-click a computer in Network Neighborhood.

To assign a drive letter in My Computer for a particular share, use the **Map Network Drive** command on the **Tools** menu in the Explorer. Type the server name and share name into the **Path** box using the form \\servername\sharename. For **Drive** you can use the next letter available, or select a letter from the drop-down list.

For example, to connect to the shared directory Applications on the server named Dept35, type the location in the **Path** box as shown below:



Drive: F:

Path: \\DEPT35\Applications

Connect As:

☑ Reconnect at Logon

In the Explorer and My Computer, the mapped drive appears in the window as

Applications on 'Dept35' (F:)

The share appears as a drive on your computer, and the contents of the shared directory can be viewed as if they were on your computer. You can have the connection re-established each time you log on, or clear the **Reconnect at Logon** check box to automatically disconnect when you log off.

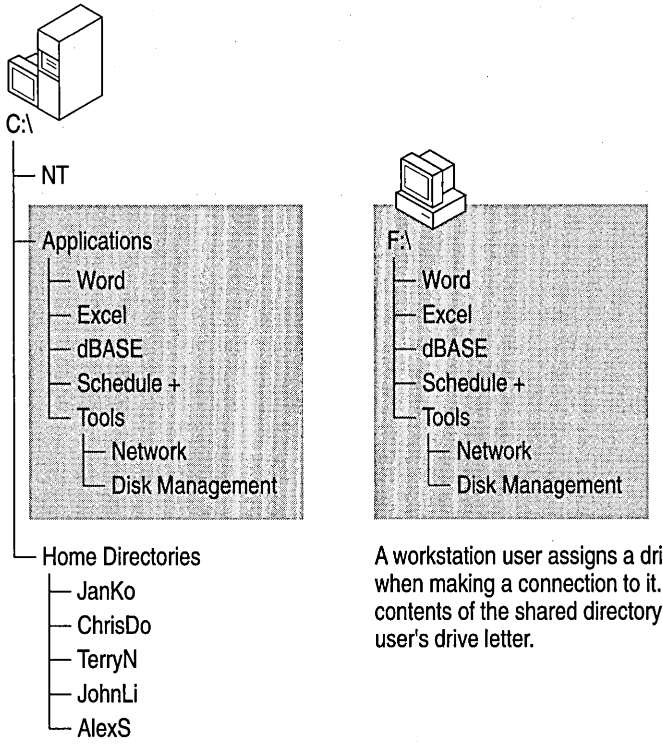
Note In addition to uniform naming convention (UNC) names such as the names of network servers, domain name system (DNS) names can be used in the **Map Network Drive** dialog box. DNS names use periods to separate each part of the name; for example, \\accounting.trey.com.\public. For more information about DNS names, see TCP/IP online Help.

If you want to connect to a shared directory using a different user account, use the **Connect As** box to type the user name for that account. If the account is in a different domain, type the domain name followed by a backslash and then the user name; for example, **projects\patc**.

For MS-DOS computers with LAN Manager client software (but without Windows), use the **net use** command to make network connections:

```
net use f: \\dept35\applications
```

In the following diagram, the server on the left represents the Dept35, and the Applications directory is the share.



A workstation user assigns a drive letter to a directory when making a connection to it. Then, to the user, the contents of the shared directory are the contents of the user's drive letter.

For information about how to map a connection to a network drive, see "To assign (map) a drive letter to a shared network resource" in Windows NT Help.

Considerations for MS-DOS Users

- If a share will be accessed by users of MS-DOS (including users of Windows for Workgroups), follow the MS-DOS 8.3 naming convention for the share name. (The name can have up to eight characters, optionally followed by a period and up to three more characters.) MS-DOS computer users will be unable to access shares with share names that do not follow this convention.
- If a share will be accessed only by Windows NT Workstation or Windows NT Server users, the share name can include up to 80 characters.

- On NTFS and FAT volumes, files and directories can have share names of up to 255 characters. And to ensure access by MS-DOS users, Windows NT Server and Windows NT Workstation provide *name mapping*: Each file or directory with a name that does not conform to the MS-DOS 8.3 standard is automatically given a second name that does. MS-DOS users connecting to the file or directory over the network see the name in the 8.3 format; Windows NT Workstation and Windows NT Server users see the long name. However, Windows NT Workstation and Windows NT Server do not generate short names for share names that do not conform to MS-DOS naming standards, only for files and directories with long names. When naming a share, use the 8.3 standard.
- Windows NT Server name mapping also allows applications that do not support long file names to access files with such names. These applications refer to files that have long names by their shorter names.

Note If an application that does not support long file names opens a file with a long name and then saves the file, the long name is lost, and only the short name remains.

Windows NT Server uses the following rules to convert a long name into a short name:

- Spaces are removed.
- Characters not allowed in MS-DOSnames are changed to underscores (_).
- The name is truncated to its first six remaining characters (or all the characters before the first period in the long name, if the first period is in the first six characters). A tilde and a digit are then added to these six characters. The digit for the first short name created for a set of six characters is 1. If more names using these six characters are created, the next short name uses a 2 instead of a 1, and so on up to ~4. If a fifth name is created, then the last 4 characters are replaced by a set of random characters, and ~1. The random characters change to create any successive names.
- If the long name has any periods followed by another character, the last of those periods and the first three characters following that period are used as the file name extension of the short name. For example, VERY.IMPORTANT.MEMOS is shortened to VERYIM~1.MEM.

If you are using Windows NT Server in an environment where long file names are not always supported, you might want to continue using MS-DOS conventions for the first six characters of names and use periods only to separate the name from the extension. For example, you could name a file AUGSAL~August 1996 Sales Report.XLS. Then the short name would be AUGSAL~1.XLS.

Although a range of characters can appear in file names, the command prompt is limited to the characters available in the OEM code page you installed when you set up Windows NT Server or Windows NT Workstation. If you plan to work with files at the command prompt, use alphanumeric characters in file names and avoid using characters that do not map to the OEM code pages (such as the bullet character).

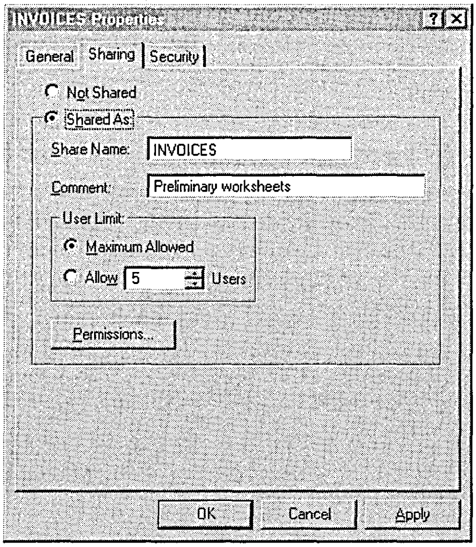
Caution Disk tools, such as Scan Disk, and file maintenance tools that are not designed to use long file names should **not** be used on volumes containing Windows NT Workstation or Windows NT Server versions 3.51 or 4.0 files. The tools can corrupt long file names, which can lead to data loss. Do not modify long file names (or any Windows NT system files) when using another operation system.

Sharing Directories

Where and how you share directories depends on how you are logged on:

- If you are logged on as a member of the Administrators or Power Users local group to a computer running Windows NT Server as a member server or a computer running Windows NT Workstation, you can share directories on the local computer.
- If you are logged on to a domain controller as a member of the Administrators or Server Operators local group, you can share directories on the domain.
- If you are logged on to a domain account as a member of the domain Administrators or Server Operators local group, you can share directories remotely using Server Manager.

If you are sharing a directory on your local computer, you can select the folder for the directory in Windows Explorer and click **Properties** on the **File** menu. Use the **Sharing** tab in the folder's **Properties** dialog box to share the directory and set permissions.



○ Not Shared
● Shared As:
Share Name: INVOICES
Comment: Preliminary worksheets
User Limit:
● Maximum Allowed
○ Allow 5 Users

For information about how to share a directory, see "To share a directory with other people" in Windows NT Help.

You can also use Server Manager to view a computer's shares, add new shares, and stop sharing directories. Server Manager also allows you to monitor and control the use of shared files.

For information about how to share directories using Server Manager, see "Sharing a Directory", "Viewing Shared Resources", and "Stopping Directory Sharing" in Server Manager Help.

Windows NT Server automatically creates special shares for administrative and system use. Depending on the configuration of the computer being administered, some or all of the following special shares can appear in this list. Usually, you should not remove or modify these special shares.

Share name	Represents
driveletter$	The root directory of a storage device on the computer. For example, C$ is a share name by which the root directory of drive C can be accessed over the network. Only members of the Administrators, Backup Operators, and Server Operators groups can connect to these shares.
ADMIN$	A resource used by the system during remote administration of a computer. The path of this resource is always the Windows NT system root (the directory in which Windows NT was installed, for example, C:\WINNT). Only members of the Administrators, Backup Operators, and Server Operators groups can connect to this share.
IPC$	A resource sharing the named pipes that are essential for communication between programs. Used during remote administration of a computer and when viewing a computer's shared resources.
NETLOGON	A resource used by the Net Logon service on domain controllers for processing domain logon requests. This resource is provided only for Windows NT Server, not for Windows NT Workstation.
PRINT$	A resource that supports shared printers.
REPL$	A resource created by the system when a Windows NT Server computer is configured as a replication export server. Required for export replication.

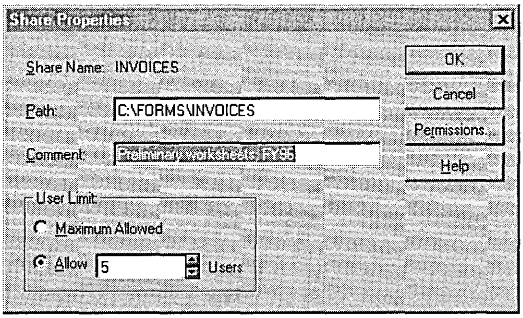
For information about how to view shared resources, see "Viewing Shared Resources" in Server Manager Help.

Changing Share Properties

To change properties on a share, you must be logged on as a member of the Administrators or Server Operators group for domain controllers, or Administrators or Power Users for workstations and member servers. Members of the Administrators group can change share properties on administrative shares as well (for example, ADMIN$).

In Server Manager you can select a shared directory and make changes to its properties. Use the **Share Properties** dialog box to change the directory path, add a comment, or change the number of users allowed to connect to the share at one time. Click **Permissions** to see the users and groups who have permission to use the share and to change permissions.

Tip For NTFS volumes, use directory and file permissions for controlling security both locally and over the network, and allow Full Control access to Everyone on the share.



Share Name: INVOICES

Path: C:\FORMS\INVOICES

Comment: Preliminary worksheets, FY96

User Limit:

○ Maximum Allowed

● Allow 5 Users

For information about how to manage share permissions, see "To set, view, change, or remove permissions through a shared directory" in Windows NT Help.

Stopping Directory Sharing

When you stop sharing a directory, it is no longer available over the network. To stop sharing a directory, you must be logged on as a member of the Administrators or Server Operators group.

The **Shared Directory** dialog box displays shared directories you have created, as well as shared directories created by the system. In general, you should not stop sharing directories created by the system (those shares that display "$," such as C$ or PRINT$). Administrative shares that are deleted are re-created automatically the next time the Server service is started.

Caution If you decide to stop sharing a directory while users are connected, users can lose data.

Use Server Manager or the Explorer to stop sharing a directory.

Sharing ClipBook Pages

ClipBook Viewer enables you to share information among different applications and users and to dynamically link and embed that information into other files and documents on the same computer or on other Windows NT computers. For more information about ClipBook Viewer and object linking and embedding (OLE), see the *Windows NT Server Resource Kit.*

When a piece of information is transferred to ClipBook Viewer, it takes the format of a *page*. ClipBook Viewer can hold up to 127 pages, which can be shared with other users. The user who creates a page can set permissions specifying whether other users can use the page.

To create, share, stop sharing, and delete a ClipBook Viewer page, a user must be in one of the following groups:

- Administrators
- Server Operators
- Power Users
- Users

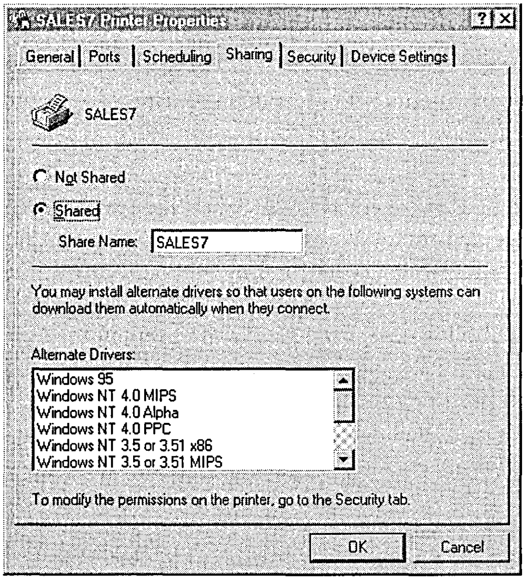
In addition, the special group Everyone can use ClipBook Viewer to see a list of pages shared on the computer.

Sharing Printers

Printers can be shared by the following users:

- Users logged on to a computer running Windows NT Workstation or a member server running Windows NT Workstation as a member of the Administrators or Power Users local group.
- Users logged on to a domain controller as a member of the Administrators, Server Operators, or Print Operators local group.
- Users logged on to a domain account as a member of the domain Administrators local group.

After a printer has been added, it can be shared using the **Sharing** tab in the **Printer Properties** dialog box. Click **Printers** in the Settings group on the **Start** menu to add printers, share printers, install printer drivers, configure printer ports, set printer properties, and set permissions.



○ Not Shared

● Shared

Share Name: SALES7

You may install alternate drivers so that users on the following systems can download them automatically when they connect.

Alternate Drivers:

Windows 95
Windows NT 4.0 MIPS
Windows NT 4.0 Alpha
Windows NT 4.0 PPC
Windows NT 3.5 or 3.51 x86
Windows NT 3.5 or 3.51 MIPS

To modify the permissions on the printer, go to the Security tab.

For information about setting up and sharing printers, and about printer permissions, see Chapter 5, "Setting Up Print Servers."

For information about how to manage printer sharing, see "To set up a new printer", "To share your printer with other people", "To use a shared network printer", and "To stop sharing your printer" in Windows NT Help.

Sharing Windows NT Server Resources With Other Network Computers

Computers running different operating systems that interact with other networks or with workgroups can share files and printers with Windows NT Server network computers:

- Domain computers running Windows for Workgroups can use and share directories and printers on a Windows NT Server network.
- LAN Manager 2.*x* servers and clients can use and share directories and printers on a Windows NT Server network.
- Windows 95 computers running Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks can use and share directories and printers on a Windows NT Server network.

- Apple Macintosh clients running Services for Macintosh can use files and printers on Windows NT Server and Windows NT Workstation computers.
- Novell NetWare clients running File and Print Services for NetWare enables a Windows NT Server computer to function as a NetWare 3.12-compatible file and print server.
- With the Client Service for NetWare in Windows NT Workstation and the Gateway Service for NetWare in Windows NT Server, users can access file and print resources on servers running NetWare 2.*x* through 4.*x*.

For information about integrating other computers with Windows NT Server, see Chapter 1, "Managing Windows NT Server Domains," and the Windows NT Server Networking Supplement.

Securing Resources

For NTFS volumes, you can use Windows NT Explorer to set permissions on directories and files on computers running Windows NT Server. Permissions set on the directories and files themselves apply both to users working at the computer itself and, if the directory is shared, to users accessing these files over the network.

You can set file permissions to a fine degree of granularity. For example, you can set different permissions for each file in a directory. You can set many types of permissions, as well. You can let one user read the contents of a file and change it, let another user only read the file, and prevent all other users from any access to the file.

Note This type of access restriction is not available for files on FAT volumes, which are always readable and changeable by users working at the computer itself. However, you can protect shared directories on FAT volumes by specifying one set of permissions that apply to users for all files and subdirectories of the shared directory. These permissions are called *share permissions*.

Similar types of permissions can be set on shared printers managed by Windows NT Server computers. For information about setting printer permissions, see "Setting Permissions on Network Printers" later in this chapter.

How NTFS Permissions Work

Before sharing a directory on an NTFS volume, set individual permissions on the directory and its files and subdirectories. Each permission specifies the access that a group or user can have to the directory or file.

Windows NT Server offers a set of *standard permissions* for NTFS directories and files. The standard permissions are combinations of specific types of access, which are called *individual permissions*. The individual permissions and their abbreviations are:

Read (R)	Write (W)	Execute (X)
Delete (D)	Change Permissions (P)	Take Ownership (O)

Standard permissions and their meanings for directories and files are shown in the following tables, along with the individual permissions they represent. In the first column of the first table (for directory permissions), the first set of parentheses following the standard permission indicates the individual permissions for the directory itself. The second set of parentheses indicates the individual permissions that apply for new files subsequently created in the directory.

Standard Permissions for NTFS Directories and Files

Permissions	Meaning
Directory:	
No Access (None) (None)	User cannot access the directory in any way, even if the user is a member of a group that has been granted access to the directory.
List (RX) (Not Specified)	User can list only the files and subdirectories in this directory and change to a subdirectory of this directory. User cannot access new files created in this directory.
Read (RX) (RX)	User can read the contents of files in this directory and run applications in the directory.
Add (WX) (Not Specified)	User can add files to the directory but cannot view the contents of the directory.
Add & Read (RWX) (RX)	User can add files to the directory and read current files but cannot change files.
Change (RWXD) (RWXD)	User can read and add files and change the contents of current files.
Full Control (All) (All)	User can read and change files, add new ones, change permissions for the directory and its files, and take ownership of the directory and its files.

(continued)

Standard Permissions for NTFS Directories and Files

Permissions	Meaning
File:	
No Access	User cannot access the file in any way, even if the user is a member of a group that has been granted access to the file.
Read (RX)	User can read the contents of the file and run it if it is an application.
Change (RWXD)	User can read, modify, and delete the file.
Full Control (All)	User can read, modify, delete, set permissions for, and take ownership of the file.

When you set a standard permission, the abbreviations for the individual permissions appear beside the standard permission. For example, when you set the standard permission Read on a file, the abbreviation *RX* appears beside it.

In addition to setting standard permissions, you can set special access permissions. Special access permissions allow you to define a custom set of individual permissions for directories and files. For information about special access permissions, see "Setting Customized 'Special Access' Permissions," later in this chapter.

To work with NTFS security effectively:

- Users can use a directory or file only if they have been granted permission to do so or if they belong to a group that has permission to do so.
- Permissions are cumulative, but the No Access permission overrides all others. For example, if the coworkers group has Change permission for a file, and the finance group has only Read permission and John is a member of both groups, John will be granted Change permission. However, if the finance group's permission for the file is changed to No Access, John will be unable to use the file, despite his membership in the coworkers group.
- When you create files and subdirectories in a directory, they inherit permissions from the directory. For example, if you add a file to a directory that allows the coworkers group Change permission and the finance group Read permission, those same permissions apply to the file.
- The user who creates a file or directory is the owner of that file or directory. The owner can always control access to the file or directory by changing the permissions set on it. Users who are members of the Administrators group can always take ownership of a file or directory.

- File permissions always override directory permissions.
- The easiest way to administer security is by setting permissions for groups rather than individual users. Typically, a user needs access to many files. If the user is a member of a group that has access to the files, you can end the user's access by removing the user from the group rather than changing the permissions on each of the files. Setting permissions for an individual user does not override the access granted to the user through groups to which the user belongs.

Taking Ownership of NTFS Files and Directories

Every file and directory on an NTFS volume has an *owner*. The owner controls how permissions are set on the file or directory and can grant permissions to others.

When a file or directory is created, the person creating the file or directory automatically becomes its owner. It is expected that administrators will create most files on network servers, such as when they install applications on the server. Therefore, most files on a server will be owned by administrators, except for data files created by users and files in users' home directories.

Ownership can be transferred in the following two ways:

- The current owner can grant the Take Ownership permission to other users, allowing those users to take ownership at any time.
- An administrator can take ownership of any file on the computer. For example, if an employee leaves the company suddenly, the administrator can take control of the employee's files.

Note Although an administrator can take ownership, the administrator cannot transfer ownership to others. This restriction keeps the administrator accountable.

For more information, see "To take ownership of files or directories" in Windows NT Help.

Setting Permissions on NTFS Volumes

When you set permissions on directories and files on a server running Windows NT Server, you control directory and file access by:

- Local groups, global groups, and individual users in the domain containing the server
- Global groups and individual users in domains that this domain trusts
- The special identities Everyone, System, Network, Interactive, and Creator Owner

You can grant permissions to the built-in local groups (such as Administrators and Domain Users) and to any groups you create in the domain.

Special Identities

Everyone represents all current and future users of the network, including guests and users from other domains. You can assign Everyone permissions for both directories and files.

System represents the operating system of the local computer. System is initially granted permissions for several system directories when Windows NT is installed, and you should not revoke these permissions. You usually do not have to grant permissions to System for any file or directories you create, unless a system service needs to access them.

Network represents all current and future users accessing this file or directory over the network. Interactive is the opposite—it represents any user who accesses the file or directory while working at the server itself. For example, while CristalW accesses a file over the network (while working at her own workstation), she has any permissions assigned to Network, but not those assigned to Interactive. If CristalW moves to the server and accesses the file from there, she then has permissions assigned to Interactive but not those assigned to Network.

You can set Creator Owner permissions only on directories. Creator Owner represents users who subsequently create files and directories in the current directory. If you set Creator Owner permissions on a directory, anyone who creates a file or subdirectory there is automatically granted the permissions you gave to Creator Owner for that file or subdirectory.

Default Directory Permissions

When a new subdirectory or file is created on an NTFS volume, you can set permissions on it. If you do not set permissions, the new subdirectory or file inherits the permissions of the directory containing it. The following tables list the permissions set by default on directories on both Windows NT Server and Windows NT Workstation.

Default Directory Permissions on Windows NT Server

● Permission allows use
○ Permission does not allow use

	Full Control	Change	RWXD	Read	RWX	List	No Access
\ (Root directories of all NTFS volumes)							
Administrators	●	○	○	○	○	○	○
Server Operators	○	●	○	○	○	○	○
Everyone	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32							
Administrators	●	○	○	○	○	○	○
Server Operators	○	●	○	○	○	○	○
Everyone	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\CONFIG							
Administrators	●	○	○	○	○	○	○
Everyone	○	○	○	○	○	●	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\DRIVERS							
Administrators	●	○	○	○	○	○	○
Server Operators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\SPOOL							
Administrators	●	○	○	○	○	○	○
Server Operators	●	○	○	○	○	○	○
Print Operators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\REPL							
Administrators	●	○	○	○	○	○	○
Server Operators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○

Default Directory Permissions on Windows NT Server *(continued)*

● Permission allows use
○ Permission does not allow use

	Full Control	Change	RWXD	Read	RWX	List	No Access
\SYSTEM32\REPL\IMPORT							
Administrators	●	○	○	○	○	○	○
Server Operators	○	●	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Replicator	○	●	○	○	○	○	○
NETWORK	○	○	○	○	○	○	●[1]
\SYSTEM32\REPL\EXPORT							
Administrators	●	○	○	○	○	○	○
Server Operators	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Replicator	○	○	○	●	○	○	○
\USERS							
Administrators	○	○	●	○	○	○	○
Account Operators	○	○	●	○	○	○	○
Everyone	○	○	○	○	○	●	○
\USERS\DEFAULT							
Everyone	○	○	○	○	●	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\WIN32APP							
Administrators	●	○	○	○	○	○	○
Server Operators	●	○	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
\TEMP							
Administrators	●	○	○	○	○	○	○
Server Operators	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Everyone	○	●	○	○	○	○	○

[1] Because of the special way the initial permissions are set up on SYSTEM32\REPL\IMPORT, the No Access permission assigned to NETWORK does not apply to the permissions initially granted to Administrators, Server Operators, and Everyone. For example, Administrators can still access this directory over the network, because in this special case that permission overrides the No Access assigned to NETWORK.

Default Directory Permissions on Windows NT Workstation

● Permission allows use
○ Permission does not allow use

	Full Control	Change	RWXD	Read	RWX	List	No Access
\ (Root directories of all NTFS volumes)							
Administrators	●	○	○	○	○	○	○
Everyone	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32							
Administrators	●	○	○	○	○	○	○
Everyone	○	●	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\CONFIG							
Administrators	●	○	○	○	○	○	○
Everyone	○	○	○	○	○	●	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\DRIVERS							
Administrators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\SPOOL							
Administrators	●	○	○	○	○	○	○
Power Users	○	●	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\SYSTEM32\REPL							
Administrators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○

Default Directory Permissions on Windows NT Workstation *(continued)*

● Permission allows use
○ Permission does not allow use

	Full Control	Change	RWXD	Read	RWX	List	No Access
\SYSTEM32\REPL\IMPORT							
Administrators	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Replicator	○	●	○	○	○	○	○
NETWORK	○	○	○	○	○	○	●[1]
\USERS							
Administrators	○	○	●	○	○	○	○
Everyone	○	○	○	○	○	●	○
\USERS\DEFAULT							
Everyone	○	○	○	○	●	○	○
CREATOR OWNER	●	○	○	○	○	○	○
\WIN32APP							
Administrators	●	○	○	○	○	○	○
CREATOR OWNER	●	○	○	○	○	○	○
Everyone	○	○	○	●	○	○	○
\TEMP							
Administrators	○	○	●	○	○	○	○
CREATOR OWNER	○	○	●	○	○	○	○
Everyone	○	○	○	●	○	○	○

[1] Because of the special way the initial permissions are set up on SYSTEM32\REPL\IMPORT, the No Access permission assigned to NETWORK does not apply to the permissions initially granted to Administrators, Server Operators, and Everyone. For example, Administrators can still access this directory over the network, because in this special case that permission overrides the No Access assigned to NETWORK.

In addition to these permissions, the special identity System (representing the operating system) has Full Control permission for all these directories.

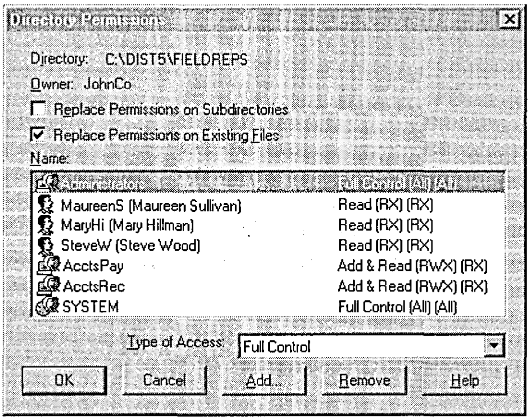
Caution Do not revoke the default permissions on these directories. If you do, parts of the operating system might not work.

Setting Permissions on NTFS Directories

When you set directory permissions, you set permissions on not only the directory but, by default, on all the files and subdirectories in the directory.

Note To change permissions on the directory, you must be the owner of the directory or have been granted permission to do so by the owner.

New files and new subdirectories inherit the permissions of the directory that contains them. The **Directory Permissions** dialog box shows these inherited permissions. The **Name** box shows the groups and users for whom permissions have been set. (If you have selected multiple directories, permissions are shown only if they are the same for all directories.) You can change permissions, add a group or user to the list, or remove a group or user from the list.



Directory: C:\DIST5\FIELDREPS

Owner: JohnCo

□ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

Administrators	Full Control (All) (All)
MaureenS (Maureen Sullivan)	Read (RX) (RX)
MaryHi (Mary Hillman)	Read (RX) (RX)
SteveW (Steve Wood)	Read (RX) (RX)
AcctsPay	Add & Read (RWX) (RX)
AcctsRec	Add & Read (RWX) (RX)
SYSTEM	Full Control (All) (All)

Type of Access: Full Control

When you set a standard permission, two sets of individual permissions are displayed next to it: the permissions set on the directory and the permissions set on files in the directory. For example, when you set Add & Read permission on a directory, you see (*RWX*), signifying Read, Write, and Execute permissions on the directory, and *(RX*), signifying Read and Execute permissions on files in the directory.

Some directory permissions set file permissions to Not Specified. When file access for a user or group is not specified, that group or user cannot use files in the directory unless access is granted by another means (for example, by permissions set on individual files).

The following table shows permissions for directories and the actions on directories available to users for each permission.

● Permission allows use ○ Permission does not allow use	No Access	List	Read	Add	Add & Read	Change	Full Control
Display directory filenames	○	●	●	○	●	●	●
Display the directory's attributes	○	●	●	●	●	●	●
Go to the directory's subdirectories	○	●	●	●	●	●	●
Change the directory's attributes	○	○	○	●	●	●	●
Create subdirectories and add files	○	○	○	●	●	●	●
Display the directory's owner and permissions	○	●	●	●	●	●	●
Delete the directory	○	○	○	○	○	●	●
Delete any file or empty subdirectory in the directory	○	○	○	○	○	○	●
Change directory permissions	○	○	○	○	○	○	●
Take ownership of the directory	○	○	○	○	○	○	●

Note Groups or users granted Full Control permission on a directory can delete files in that directory no matter what permissions protect the files.

The following table shows permissions for directories and the actions on files available to users for each permission.

● Permission allows use ○ Permission does not allow use	No Access	List	Read	Add	Add & Read	Change	Full Control
Display the file's owner and permissions	○	○	●	○	●	●	●
Display the file's data	○	○	●	○	●	●	●
Display the file's attributes	○	○	●	○	●	●	●
Run the file if it is a program	○	○	●	○	●	●	●
Change the file's attributes	○	○	○	○	○	●	●
Change data in and append data to the file	○	○	○	○	○	●	●
Delete the file	○	○	○	○	○	●	●
Change the file's permissions	○	○	○	○	○	○	●
Take ownership of the file	○	○	○	○	○	○	●

Controlling Subdirectory Permissions

When a group or user is granted permissions through the Creator Owner identity, directory permissions are not passed on to subdirectories.

When you are setting permissions on an NTFS directory, you can use the Creator Owner special group to allow users to control only the subdirectories and files that they create within the directory. Permissions set for Creator Owner are transferred to the user who creates a directory or file within the directory.

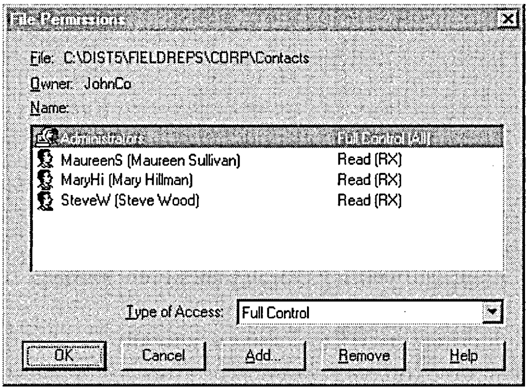
For example, if you give Add & Read permission to Everyone on the directory, and Change permission to Creator Owner, when one user adds files to the directory, the user can change and delete the files, while other users can only read them. Permissions that are not inherited by subdirectories are marked with an asterisk.

For information about how to manage directory permissions, see "To set, view, change, or remove directory permissions" in Windows NT Help.

Setting Permissions on NTFS Files

The **File Permissions** dialog box shows the permissions the file inherited. The **Name** box shows the groups and users for whom permissions have been set on the file. (If you have selected multiple files, permissions are shown only if they are the same for all files.) You can change permissions set for the listed groups and users, add a group or user to the list, or remove a group or user from the list.

Note To change permissions on the file, you must be the owner of the file or have been granted permission to do so by the owner.



File Permissions

File: C:\DIST5\FIELDREPS\CORP\Contacts

Owner: JohnCo

Name:

Administrators	Full Control (All)
MaureenS (Maureen Sullivan)	Read (RX)
MaryHi (Mary Hillman)	Read (RX)
SteveW (Steve Wood)	Read (RX)

Type of Access: Full Control

The following table shows permissions for files and the actions available to users for each permission.

● Permission allows use
○ Permission does not allow use

	No Access	Read	Change	Full Control
Display the file's data	○	●	●	●
Display the file's attributes	○	●	●	●
Run the file if it is a program	○	●	●	●
Display the file's owner and permissions	○	●	●	●
Change the file's attributes	○	○	●	●
Change data in and append data to the file	○	○	●	●
Delete the file	○	○	●	●
Change the file's owner and permissions	○	○	○	●

Strategies for Using NTFS File Permissions

- Grant permissions to groups, not individual users.
- Create local groups and assign permissions to them, rather than assigning permissions directly to global groups.

  For more information about the strategies of using groups and users, see Chapter 2, "Working With User and Group Accounts."
- When you create and share a file or directory on a server, grant Full Control to the Administrators local group. This ensures that all administrators of that domain can change permissions for and otherwise administer the file or directory in the future.

Example for Setting Up File Permissions

Suppose you need to set file permissions on a server used by a small department. The file server includes an applications directory, home directories for each of the department's users, a public directory where users can share files, and a drop directory where users can file confidential reports that only the group manager can read.

In the applications directory, make all executable programs read-only to all users, to prevent viruses and Trojan horses. You can also grant the individual Change Permissions (P) permission to members of the Administrators group, so that administrators can give themselves Write permission when it is time to update an application. Giving members of the Administrators group the Write permission initially provides less virus protection than giving them Change permission and forcing them to change permissions before updating the application.

If none of your applications need to write any files (such as initialization setting files) in their own directories, you should also make all the directories containing applications read-only.

For the home directories, give each user Full Control over his or her own directory, and do not give anyone permissions for any other directory.

For the public directory, you can give all users Change permission, which lets them read and write to the directory. Change is more appropriate than Full Control because Full Control also allows users to set permissions for the public directory and take ownership of it.

To create a drop directory, just grant Users or Everyone the Add permission for the directory, and give the Change permission to the manager who is to read the files in the directory.

Give access to WINNT directory files or subdirectories only to Administrators or Server Operators.

Setting Customized "Special Access" Permissions

In general, the standard directory and file permissions are all you need to secure your directories and files. However, if you use NTFS and need to create a custom set of permissions, you can use *special access* permissions. You can set special access permissions on directories, on all the files in selected directories, or on selected files. (Special access permissions on a directory affect the directory only.)

The following table shows special access permissions for directories and the actions available to users for each directory permission.

● Permission allows use ○ Permission does not allow use	Read	Write	Execute	Delete	Change Permissions	Take Ownership	Full Control
Display filenames in the directory	●	○	○	○	○	○	●
Display the directory's attributes	●	○	●	○	○	○	●
Add files and subdirectories	○	●	○	○	○	○	●
Change the directory's attributes	○	●	○	○	○	○	●
Go to the directory's subdirectories	○	○	●	○	○	○	●
Display directory owner and permissions	●	●	●	○	○	○	●
Delete the directory	○	○	○	●	○	○	●
Change the directory's permissions	○	○	○	○	●	○	●
Take ownership of the directory	○	○	○	○	○	●	●

The following table shows special access permissions for files and the actions available to users for each permission.

● Permission allows use ○ Permission does not allow use	Read	Write	Execute	Delete	Change Permissions	Take Ownership	Full Control
Display the file's owner and permissions	●	●	●	○	○	○	●
Display the file's data	●	○	○	○	○	○	●
Display the file's attributes	●	○	●	○	○	○	●
Change the file's attributes	○	●	○	○	○	○	●
Change data in and append data to the file	○	●	○	○	○	○	●
Run the file if it is a program	○	○	●	○	○	○	●
Delete the file	○	○	○	●	○	○	●
Change the file's permissions	○	○	○	○	●	○	●
Take ownership of the file	○	○	○	○	○	●	●

For information about setting special access permissions, see "To set special access permissions" in Windows NT Help.

Setting Permissions on Shared Directories

Permissions set on shared directories are called *share permissions*, and they determine who can use shared directories over the network, and in what manner.

On NTFS volumes, you can set permissions on directories and files, and these permissions apply to users accessing the files at the server. When the NTFS directory is shared, these same file and directory permissions apply to users accessing the shared directory over the network. Therefore, share permissions are not critical to security of NTFS directories.

Directories on FAT volumes, however, cannot be protected from access by users working at the computer itself; they can be protected by permissions only after they are shared, and the permissions affect only access over the network. For FAT volumes, share permissions provide the only way to limit access to network files. You can specify one set of share permissions on a shared directory that applies to users for all files and subdirectories of the shared directory.

The method for setting share permissions is the same for NTFS and FAT file types. Use the **Sharing** tab in the directory property sheet to set permissions on the shared directory. When you share a directory, you can grant each group and user one of four types of permissions for the share and all of its subdirectories and files: Full Control, Change, Read, or No Access.

To secure shared directories effectively, keep the following in mind:

- To work with shared directory permissions, you must be logged on as a member of the Administrators or Server Operators group.
- The default permissions set on a newly created share are Full Control for Everyone.
- Permissions set through a shared directory are effective only when the directory is reached over the network.
- Permissions set through a shared directory apply to all files and subdirectories in the shared directory.
- Permissions set through a shared directory in an NTFS volume operate in addition to NTFS permissions set on the directory itself.

The following table shows the permissions for files and directories granted through a shared directory and the actions available to users for each permission:

● Permission allows use
○ Permission does not allow use

	No Access	Read	Change	Full Control
Display subdirectory names and filenames	○	●	●	●
Display the data and attributes of files	○	●	●	●
Run program files	○	●	●	●
Go to the directory's subdirectories	○	●	●	●
Create subdirectories and add files	○	○	●	●
Change data in and append data to files	○	○	●	●
Change the file's attributes	○	○	●	●
Delete subdirectories and files	○	○	●	●
Change permissions (NTFS files and directories only)	○	○	○	●
Take ownership (NTFS files and directories only)	○	○	○	●

Use the **Access Through Share Permissions** dialog box to change permissions for the listed groups and users and to modify the permissions list.

For information about how to manage share permissions, see "To set, view, change, or remove permissions through a shared directory" in Windows NT Help.

Share Permissions for NTFS Volumes

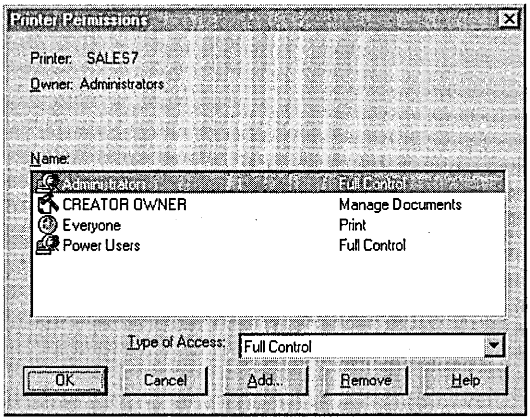
Share permissions on directories in NTFS volumes work with the permissions you set on an individual directory and its files, but they affect the permissions a user has when accessing a directory over the network.

Because NTFS volumes allow individual directory and file permissions, you can control these permissions best at these levels. If you use share permissions, you can use the default shared directory access of Full Control for Everyone, and use directory and file permissions to control access.

Setting Permissions on Network Printers

Printer permissions specify the type of access a user or group has to use the printer. The printer permissions are No Access, Print, Manage Documents, and Full Control.

Note If you are the owner of the printer or have Full Control permission, you can set and change printer permissions.



Printer: SALES7

Owner: Administrators

Name:

Administrators	Full Control
CREATOR OWNER	Manage Documents
Everyone	Print
Power Users	Full Control

Type of Access: Full Control

For information about setting print permissions, see Chapter 5, "Setting Up Print Servers."

For information about how to set printer permissions, see "To limit access to a shared printer", in Windows NT Help.

File Sharing and Permission Examples

Suppose you need to set file permissions on a server used by a small department. The file server includes an applications directory, home directories for each of the department's users, a public directory where users can share files, and a drop directory where users can file confidential reports that only the group manager can read. In the applications directory, make all executable programs read-only to all users to prevent introduction of viruses and Trojan horses. (For information about viruses and Trojan horses, see "Protecting Against Viruses and Trojan Horses" later in this chapter.) You can also grant the individual Change Permissions (P) permission to Administrators. This allows administrators to give themselves Write permission when it is time to update an application. Giving Administrators the Write permission initially provides less virus protection than giving them the Change Permissions permission and forcing them to change permissions before updating the application.

- If none of your applications needs to write any files (such as initialization setting files) in their own directories, make all the directories containing applications read-only.
- For home directories, give each user Full Control over his or her own directory, and do not give anyone permissions for any other directory.
- For the public directory, give all users Change permission, which lets them read and write to the directory. (Change is more appropriate than Full Control, which also allows users to set permissions for the public directory and take ownership of it.)
- To create a drop directory, grant Users or Everyone the Add permission for the directory, and grant the Change permission to the manager who is to read the files in the directory.
- Give only Administrators or Server Operators access to files or subdirectories under the WINNT directory.

Managing Directory Replication

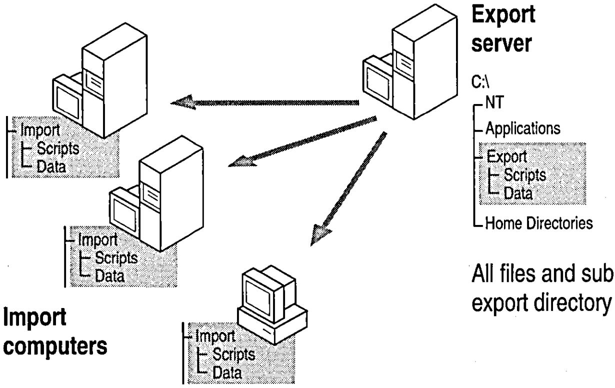
Keeping shared resources current is a helpful task performed by Windows NT Server Directory Replicator service. If you have a set of files that you want distributed to many users, you can set up and maintain identical directory trees on multiple servers and workstations, and split the load between several computers.

Configure one server to act as an export server. Place the master copies of the files here. Configure the other computers to act as import computers.

Only one copy of each file needs to be maintained, yet every computer that participates has an available, identical copy of that set of files. Each export server maintains a list of computers to which subdirectories are exported, and each import computer maintains a list of computers from which subdirectories are imported.

When you update a file in the directory tree on one server (the export server), the updated file is automatically copied to all the other computers (the import computers). Only servers running Windows NT Server can be export servers; import computers can run either Windows NT Server or Windows NT Workstation.

A file is replicated when it is first added to an exported directory and every time a change is saved to the file on the export server.



All files and subdirectories of the export directory are replicated.

Replication helps balance loads. If you have many users who need to periodically receive the same file, you can replicate the file directory to several computers to prevent any one server from becoming overburdened.

You can even replicate directories between computers in different domains. Export servers can export to domain names, and import computers can import from those domain names. This is a convenient way to set up directory replication for many computers; each export server and import computer needs to specify only a few domain names for export or import, rather than a long list of many computer names.

How Directory Replication Works

Directory replication is initiated and carried out by the *Directory Replicator service*. This service operates on each export server and import computer that participates in replication. The service on each computer logs on to the same user account, which you create for this purpose.

You set up an export server and import computers to send and receive updated files. An export directory on the export server contains all the directories and subdirectories of files to be replicated, and when changes are saved to files in these directories, the files automatically replace the existing files on all the import computers.

You can also specify whether to have the export server send changes out as soon as a file has changed or, to prevent exporting partially changed trees, to wait until one export subdirectory has been stable for two minutes before exporting.

In addition, you can lock a particular export or import directory, when needed. Changes to the locked directory are not exported or imported until you unlock the directory.

On the export server, you also designate which computers or domains are to receive replicated copies of the directories this server is exporting.

An export server has a default export path:

C:\systemroot\SYSTEM32\REPL\EXPORT

All directories to be replicated are exported as subdirectories in the export path. Subdirectories created in the export path, and files placed in those subdirectories, are automatically exported. Export servers can replicate any number of subdirectories (limited only by available memory), with each exported subdirectory having up to 32 subdirectory levels in its tree.

An import computer has a default import path:

C:\systemroot\SYSTEM32\REPL\IMPORT.

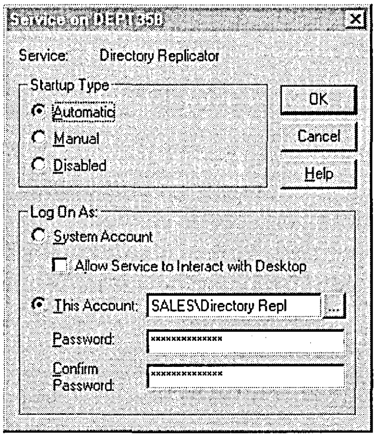
Imported subdirectories and their files are automatically placed here. You do not need to create these import subdirectories. They are created automatically when replication occurs.

A network can have multiple export servers. To ensure the integrity of replicated information, they usually do not export duplicate subdirectories. Each master export subdirectory is usually maintained on and exported by a single export server. It is possible to set up multiple servers that export the same subdirectory, but the exported files in those multiple master subdirectories might not be identical.

Replication Prerequisites

Before a computer can participate in replication, you must create a special user account. Then for each computer in a domain that will participate in replication, configure its Directory Replicator service to log on using that special account:

- In User Manager for Domains, create a domain user account for the Directory Replicator service to use to log on. Be sure the user account has the **Password Never Expires** option selected, all logon hours allowed, and membership in the domain's Backup Operators group.
- After the user account is created for each computer that will be configured as an export server or an import computer, use Server Manager to configure the Directory Replicator service to start up automatically and to log on under that user account. Be sure the password for that user account is typed correctly.



Service on DEPT35B

Service: Directory Replicator

Startup Type

● Automatic

○ Manual

○ Disabled

Log On As:

○ System Account

□ Allow Service to Interact with Desktop

● This Account: SALES\Directory Repl

Password: ***************

Confirm Password: ***************

For more information, see "To configure startup for a service" in Windows NT Help.

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

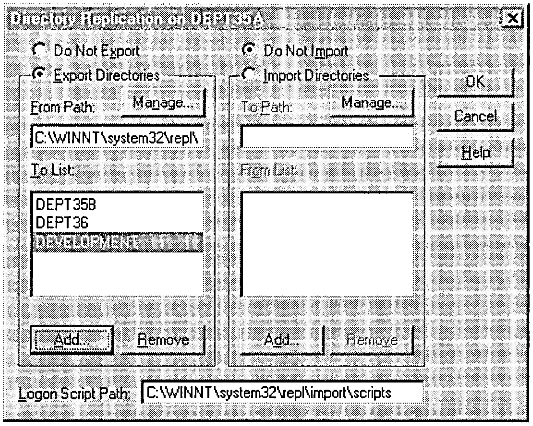
Setting Up an Export Server

Any computer running Windows NT Server can be set up as an export server. (A computer running Windows NT Workstation cannot.)

Before you set up an export server, you must perform these tasks on the export server:

- Assign a logon account to the Directory Replicator service of the export server.
- Create the directories to be exported. They must be subdirectories of the replication export path (usually C:\systemroot\ SYSTEM32\REPL\EXPORT).

Use the **Directory Replication** dialog box to set up an export server.



Directory Replication on DEPT35A

○ Do Not Export
● Export Directories
From Path: C:\WINNT\system32\repl\
To List:
DEPT35B
DEPT36
DEVELOPMENT

● Do Not Import
○ Import Directories
To Path:
From List:

Logon Script Path: C:\WINNT\system32\repl\import\scripts

For more information, see "To set up an export server" in Windows NT Help.

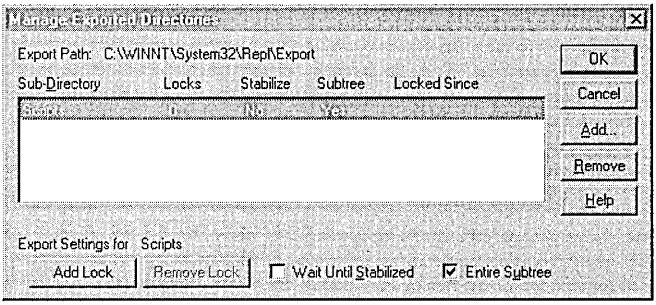
Managing Exported Subdirectories

By clicking **Manage** under **Export Directories** in the **Directory Replication** dialog box, you can manage certain features of subdirectory replication by the export server:

- You can *lock* a subdirectory to prevent it from being exported to any import computers. For example, if you know a directory will be receiving a series of changes that you do not want partially replicated, you can put one or more locks on the subdirectory in the export path. Until you remove the lock or locks, the subdirectory will not be replicated. The date and time the lock was placed is displayed so that you know how long a lock has been in force.

- When you *stabilize* a subdirectory, the export server waits two minutes after changes before exporting the subdirectory. The waiting period allows time for subsequent changes to take place so that all intended changes are recorded before being replicated.
- You specify whether the entire *subtree* (the export subdirectory and all of its subdirectories) or just the first-level subdirectory in the export directory path is exported.

To manage locks, stabilization, and subtree replication for the subdirectories exported from an export computer, click **Manage** under **Export Directories** in the **Directory Replication** dialog box.



Manage Exported Directories

Export Path: C:\WINNT\System32\Repl\Export

Sub-Directory	Locks	Stabilize	Subtree	Locked Since
Scripts	1	No	Yes	

Export Settings for Scripts

□ Wait Until Stabilized ☑ Entire Subtree

For information about how to manage export subdirectories, see "To Manage Locks, Stabilization, and Subtree Replication for Export Directories" in Server Manager Help.

Replicating Logon Scripts

Logon scripts are files that can be assigned to user accounts. Each time a user logs on, the assigned logon script is run. The logon script allows an administrator to affect the user's environment without managing all aspects of it. When a server processes a logon request, the system locates the logon script by combining a file name specified in User Manager for Domains with a path specified in Server Manager.

If you use logon scripts in a domain that has a primary domain controller and at least one backup domain controller, you should replicate logon scripts among the domain controllers. Master copies of every logon script for a domain should be stored in one replication export directory of one server. This might be the primary domain controller, but it does not need to be. Copies of these master logon scripts should be replicated to each server that participates in authenticating logons for the domain. If this is done, only one copy of each logon script will need to be maintained, yet every server that participates in authenticating domain logons will have an available, identical copy of all user logon scripts.

By default, replication is configured so that Windows NT Server computers export subdirectories and logon scripts from the directory C:\systemroot\SYSTEM32 \REPL\EXPORT\SCRIPTS, and import subdirectories and logon scripts to the directory C:\systemroot\SYSTEM32\REPL\IMPORT\SCRIPTS. For the primary domain controller and each backup domain controller, the path to imported logon scripts must be entered in the **Logon Script Path** box of the **Directory Replication** dialog box.

Note The logon script path cannot be administered for member servers running Windows NT Server or for computers running Windows NT Workstation computers. On these computers, store logon scripts in C:\systemroot\SYSTEM32\REPL\IMPORT\SCRIPTS or in subdirectories of that path.

For information about how to manage logon scripts, see "Setting the Logon Script Path" in Server Manager Help.

Setting Up an Import Computer

Both Windows NT Server and Windows NT Workstation computers can be set up as import computers. A computer running Windows NT Server that is configured as an export server can also be configured as an import computer.

Before you set up an import computer, you must assign a logon account to the Directory Replicator service of the import computer.

On the import computer you do not need to create the imported subdirectories. A subdirectory is automatically created the first time it is imported.

Use the **Directory Replication** dialog box to set up an import computer. The Windows NT Server version of the **Directory Replication** dialog box is slightly different from the Windows NT Workstation version of this dialog box. The Windows NT Workstation version contains only the items related to imported directories.

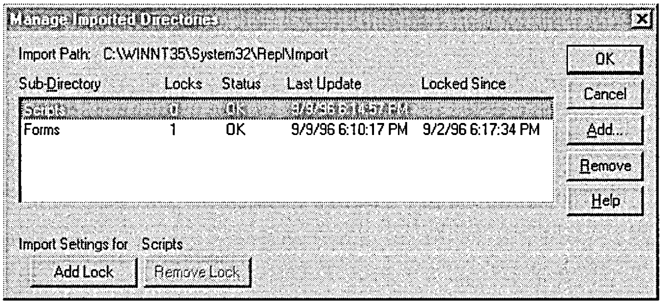
Tip You can set up a server to replicate a directory tree to itself (from its export directory to its import directory). This replication can provide a local backup of the files, or you can use the import version of these files as another source for users to access, while preserving the export version of the files as a source master.

For more information, see "Managing import Replication" in Server Manager Help.

Managing Locks and Viewing Import Subdirectory Status

You can use *locks* to prevent imports to subdirectories on an import computer. Import of a locked subdirectory to that import computer is prevented until the lock is removed. Locking a subdirectory on an import computer affects replication to only *that* computer, not to other import computers.

You can manage locks on subdirectories and also view the status of each subdirectory by clicking **Manage** under **Import Directories** in the **Directory Replication** dialog box.



Import Path: C:\WINNT35\System32\Repl\Import

Sub-Directory	Locks	Status	Last Update	Locked Since
Scripts	0	OK	9/9/96 6:14:57 PM	
Forms	1	OK	9/9/96 6:10:17 PM	9/2/96 6:17:34 PM

Import Settings for Scripts

The **Status** column can have one of four entries:

- OK indicates that the subdirectory is receiving regular updates from an export server and that the imported data is identical to that exported.
- No Master indicates that the subdirectory is not receiving updates. The export server might not be running, or a lock might be in effect on the export server.
- No Sync indicates that although the subdirectory has received updates the data is *not* up-to-date. This could be due to a communications failure, open files on the import computer or export server, the import computer not having access permissions at the export server, or an export server malfunction.
- No entry (blank) indicates that replication never occurred for that subdirectory. Replication might not be properly configured for this import computer, for the export server, or both.

The **Last Update** column shows the date and time of the latest change to the import subdirectory or to any of its subdirectories.

For more information, see "To view a list of, or manage locks for, import subdirectories" in Server Manager Help.

Replication of Multiple Directory Trees

Suppose you have a domain where you want to replicate two directory trees—one for logon scripts and one for other data. The groups of computers that need to import the two trees are different. The four domain controllers need the logon scripts. However, only two of the domain controllers and two Windows NT Workstation computers need to import the other data. The best solution is to set up different servers as the export servers of the scripts directory tree and the data directory tree.

Remember that a single export server has only one list of import computers to which it replicates. If you set up only a single export server for the two directories, it exports both directory trees to all import computers, even though not all import computers use both directory trees.

Replication Troubleshooting Tips

Directory replication problems can have a variety of causes. When the Replicator Service generates an error, you view the error in the Event Viewer. The Event Viewer displays information about the **Status** column in the **Manage Import Directories** dialog box and information about messages that appear while you are configuring directory replication servers.

The following sections describe some of the common problems encountered during directory replication.

Access Denied

If the Event Viewer shows "access denied" errors for the Directory Replicator service, be sure the service is configured to log on to a specific account and that the account used by the import computer's Directory Replicator service has permission to read the files on the export computer.

The default permissions for an export directory grant Full Control to the Replicator local group. If Full Control permission is removed from the directory, exported files are copied to the import computers but receive the wrong permissions, and an access denied error is written to the event log. If necessary, click **Permissions** in the export directory's **Sharing** tab to grant Full Control to the Replicator local group for the export directories.

Exporting to Specific Computers

Be sure to specify export servers and import computers in the **To List** and **From List**, respectively, in the **Directory Replication** dialog box. If you do not, exporting will occur to all import computers in the local domain, and importing will occur from all export servers in the local domain.

Lost Permissions on SYSTEM32\REPL\IMPORT

Do not use the Explorer or File Manager to examine permissions on the SYSTEM32\REPL\IMPORT directory. If you do, the special permissions initially set there can be lost. These initial permissions enable directory replication to work, and you do not need to change them.

Replication to a Domain Name Over a WAN Link

Directory replication to a domain name does not always succeed when some or all replication import computers are located across a wide area network (WAN) bridge from an export server. When adding names to the export **To List** on an export server, and when adding names to the import **From List** on an import computer, specify the computer names (instead of or in addition to specifying the domain name) for those computers separated by a WAN bridge.

Assessing and Managing Resource Use

In Server Manager, use the **Properties** command to display a summary of connections and resource usage for the selected computer.

The **Properties** dialog box displays a usage summary for the computer.

Item	**Description**
Sessions	The number of users remotely connected to the computer
Open Files	The number of shared resources opened on the computer
File Locks	The number of file locks on open resources of the computer
Open Named Pipes	The number of named pipes open on the computer

For each resource use summary that you can view in Server Manager, you can intervene in a user's session with the resource.

To administer a property associated with one of the five buttons at the bottom of the **Properties** dialog box, click the button.

Choose	To
Users	View a list of all the users who are connected to the computer over the network and the resources opened by a selected user. One or all of the users can be disconnected.
Shares	View a list of the computer's shared resources and the users who are connected to a selected resource over the network. One or all of the users can be disconnected.
In Use	View a list of the open shared resources on the computer. One resource or all resources can be closed.
Replication	Manage directory replication for the computer and to specify the path to user logon scripts.
Alerts	View and manage the list of users and computers that are notified when administrative alerts occur on the computer.

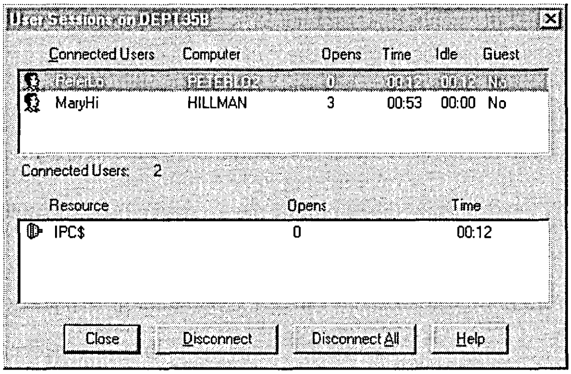
Viewing or Disconnecting User Sessions

In Server Manager, you can view information about a computer by right-clicking the computer and selecting **Properties**. In the **Computer Properties** dialog box, you can click buttons to view users, shares, current remote connections, replication import and export servers, and to send administrative alerts.

Click the **Users** button in the **Computer Properties** dialog box to view all users connected (over the network) to the computer and the resources opened by a selected user. To display the **User Sessions** dialog box, double-click a computer name in the Server Manager window and then click **Users**.

In the **User Sessions** dialog box, you can disconnect one or all users.

Caution To prevent data loss, always warn users before disconnecting them. (See "Sending a Message to Users" later in this chapter.)



User Sessions on DEPT358

Connected Users	Computer	Opens	Time	Idle	Guest
PeterLo	PETERLO2	0	00:12	00:12	No
MaryHi	HILLMAN	3	00:53	00:00	No

Connected Users: 2

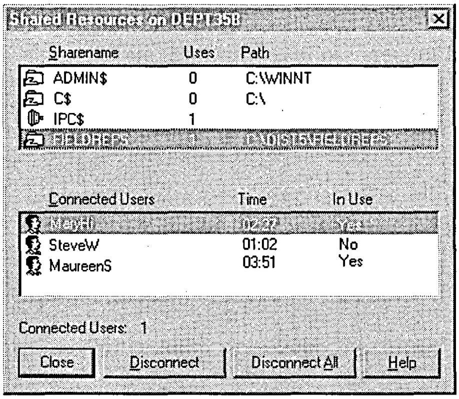
Resource	Opens	Time
IPC$	0	00:12

Note While you are remotely administering another computer, your user account is listed as a user connected to the IPC$ resource. It cannot be disconnected.

For more information, see “Managing Server Properties” and “Viewing User Sessions” in Server Manager Help.

Viewing or Disconnecting Shared Resources

Use the **Shared Resources** dialog box to view the shared resources available on the selected computer (view the properties for the computer, and click **Shares**). You can see users who are connected over the network to a selected resource, and you can disconnect one or all users.



Shared Resources on DEPT358

Sharename	Uses	Path
ADMIN$	0	C:\WINNT
C$	0	C:\
IPC$	1	
FIELDREPS	1	C:\DISKS\FIELDREPS

Connected Users	Time	In Use
MaryHi	02:27	Yes
SteveW	01:02	No
MaureenS	03:51	Yes

Connected Users: 1

Note While you are remotely administering another computer, your user account is listed as a connected user for the IPC$ share. It cannot be disconnected.

When you disconnect a selected user from shared resources or disconnect all users from shared resources, each user is disconnected from all shared resources on the computer, not just the resource shown in the **Sharename** list.

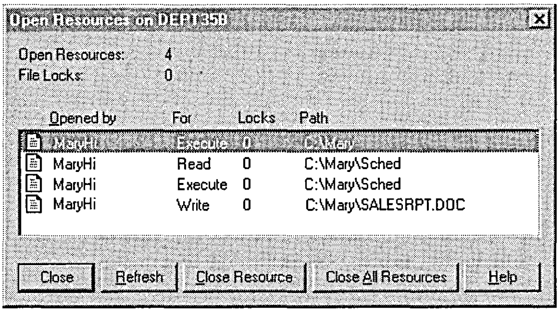
Caution To prevent data loss, always warn users before disconnecting them. (See "Sending a Message to Users" later in this chapter.)

For more information, see "Viewing Shared Resources" in Server Manager Help.

Viewing or Closing Resources In Use

You can view the list of resources that are open on a computer, and you can close a single resource or close all resources. When you close a resource, you disconnect the users who are connected.

Use the **Open Resources** dialog box to view and close resources (view the properties for the computer, and click **In Use**).



Open Resources on DEPT35B

Open Resources: 4
File Locks: 0

Opened by	For	Locks	Path
MaryHi	Execute	0	C:\Mary
MaryHi	Read	0	C:\Mary\Sched
MaryHi	Execute	0	C:\Mary\Sched
MaryHi	Write	0	C:\Mary\SALESRPT.DOC

Item	Description
Open Resources	The total number of open resources on the computer
File Locks	The total number of file locks on open resources
Icon	A graphic representation of each listed resource: A file A named pipe A print job in a print spooler A resource of an unrecognized type

(continued)

Item	Description
Opened By	The user name (or sometimes the computer name) of the user who opened the resource
For	The permission granted when the resource was opened
Locks	The number of locks on the resource
Path	The path of the open resource

In some cases, a print job is monitored as an open named pipe.

Note While you are remotely administering another computer, your connection is displayed in the **Open Resources** dialog box as an open named pipe. It cannot be closed.

For more information, see "Viewing Resources In Use" in Server Manager Help.

Sending a Message to Users

A message can be sent to all users who are connected to a computer using the **Send Message** command on the **Computer** menu in Server Manager. For example, you can do this before you disconnect one or more users or before you stop the Server service on that computer.

For a message to be sent and received, the Messenger service must be running on the computer sending the message and on the computers receiving the message.

For more information, see "Sending a Message to connected Users" in Server Manager Help.

Managing Administrative Alerts

The **Alerts** dialog box displays and manages the list of users and computers that are notified when administrative alerts occur at the selected computer.

Administrative alerts are generated by the system and relate to server and resource use. They warn about security and access problems, user session problems, server shutdown because of power loss when the UPS service is available, and printer problems. For example, an alert is generated when disk space becomes low.

For alerts to be sent, the Alerter and Messenger services must be running on the computer originating the alert. For alerts to be received, the Messenger service must be running on the destination computer.

For more information, see "Managing Administrative Alerts", "Starting and Stopping Services", and "Configuring Service Startup" in Server Manager Help.

Auditing Resource Use

Auditing files and directories on a server provides a history of their use. You can identify who took various types of actions with the files and directories and hold those users accountable for their actions. You can also audit printers.

The audit category **File and Object Access** creates a security event log entry each time a user in the audit list:

- Accesses a directory or file that is set for auditing.
- Uses a printer that is connected to the computer whose directories and files are being audited.

You can audit successful or failed actions, or both.

For information about auditing files and directories, see Chapter 9, "Monitoring Events."

For information about auditing printers, see Chapter 5, "Setting Up Print Servers."

For information about how to audit files and directories, see "To audit a file or directory", "To remove file or directory auditing for a group or user" in Windows NT Help.

Protecting Against Viruses and Trojan Horses

In today's computing world, you must prevent intentional intrusions into your network that take the form of viruses and Trojan horses:

- *Viruses* are programs that attempt to spread from computer to computer and either cause damage (by erasing or corrupting data) or annoy users (by printing messages or altering what is displayed on the screen).
- *Trojan horses* are programs that masquerade as other common programs in an attempt to receive information. An example of a Trojan horse is a program that masquerades as a system logon screen to retrieve user names and password information. The writers of the Trojan horse can use this information later to break into the system.

By taking some precautions as a matter of course, you can go a long way toward preventing intrusions by viruses and Trojan horses.

Preventing Virus Outbreaks

- Educate your network users. Few realize that they can unwittingly bring viruses into the network by loading a program from a source such as an online bulletin board.
- Have at least one commercial virus-detection program and use it to regularly to check your file servers for viruses. If possible, you should also make virus-detection software available to your users.
- Set file permissions to make all applications available on network servers and Windows NT workstations read and execute only, thereby preventing them from being replaced by viruses.
- Before putting a new application or file on the network, put it on a computer not attached to the network, and check it with your virus-detection software. You might want to also log on to this computer using an account with only guest access to the computer so that the program being tested will have only guest permissions and be unable to modify any important files.
- Regularly back up the files on your file servers (and workstations, if possible) so that damage is minimized if a virus attack does occur. For information about backups, see Chapter 6, "Backing Up and Restoring Network Files."

Preventing Trojan Horse Attacks

Windows NT Server provides an important safeguard against Trojan horse programs. Before a user can log on at a Windows NT Server or Windows NT Workstation computer, the user must type the *secure attention sequence*, CTRL+ALT+DEL. This series of keystrokes always displays the Windows NT operating system logon screen; it can never activate Trojan horse programs. Users are guaranteed to be providing their user name and password only to the operating system itself. To ensure effective security, you should educate your users to always type CTRL+ALT+DEL before logging on at a computer, even if the logon window already appears on the screen.

The secure attention sequence is also required before users can unlock locked workstations or change their passwords.

Another way to guard against Trojan horses is identical to a method for protecting against viruses. Make your applications read-and-execute-only so they cannot be replaced with programs that masquerade as the original program and steal information.

Configuring DCOM

In addition to supporting component object model (COM) for interprocess communication on a local computer, Windows NT Server now supports distributed component object model (DCOM). The DCOM Configuration tool can be used to configure 32-bit applications for DCOM communication over the network. Before you can use an application with DCOM, you must use this tool to set the application's properties.

DCOM builds on remote procedure call (RPC) technology by providing a more scaleable, easier to use mechanism for integrating distributed applications on a network. A distributed application consists of multiple processes that cooperate to accomplish a single task. Unlike other interprocess communication (IPC) mechanisms, DCOM gives you a high degree of control over security features such as permissions and domain authentication. It can also be used to launch applications on other computers or to integrate Web browser applications that run on the ActiveX platform.

DCOM allows you to efficiently distribute processes across multiple computers so the client and server components of an application can be placed in optimal locations on the network. Processing occurs transparently to the user, so the user can access and share information without needing to know where the application components are located. If the client and server components of an application are located on the same computer, DCOM can be used to transfer information between processes. DCOM is platform independent and supports any 32-bit application that is DCOM-aware.

For example, your company's payroll department might use an application with DCOM to print paychecks. When a payroll employee runs a DCOM-enabled client application on a desktop, the application starts a business rules server. The server application in turn connects to a database server in order to retrieve employee records such as salary information. The business rules server then transforms the payroll information into the final output and returns it to the client to print. Your application may support its own set of DCOM features. For more information about configuring your application to use DCOM, see your application's documentation.

Visual Basic Enterprise Edition customers who are currently using Remote Automation can easily migrate their existing applications to use DCOM. For more information, see your Visual Basic documentation or visit the Visual Basic web site at www.microsoft.com/vbasic.

For more information about DCOM, see the *Windows NT Server Resource Kit* version 4.0.

Setting Security on Applications

Once a DCOM-enabled application is installed, you can use the DCOM Configuration tool to:

- Set the location of the application.
- Set permissions on the server application by specifying which user accounts can or cannot access or start it. You can grant permissions that apply to all applications installed on the computer, or to only a particular application.
- Set the user account (or identity) that will be used to run the server application. The client application uses this account to start processes and access resources on other computers in the domain. If the server application is installed as a service, you can run the application using the built-in System account or a Windows NT Server service account that you have created.
- Control the level of security (for example, packet encryption) for connections between applications.
- Disable DCOM so that it cannot be used for the computer or the application.

The computers running the client application and the server application must both be configured for DCOM by using the DCOM Configuration tool. On the computer running the client application, you must specify the location of the server application that will be accessed or started. For the server application, you must specify the user account that will have permission to access or start the application, and the user account that will be used to run the application.

CHAPTER 5

Setting Up Print Servers

This chapter provides guidelines for setting up and sharing printers on a Windows NT network. Although printer setup itself is easy, it's worth taking time to understand the various options available for configuring printers. By carefully planning printer access, you can maximize the use of each printer and at the same time avoid long printing delays.

Overview of Windows NT Printing

Windows NT offers several advanced printing features:

- Clients can browse the network for available Windows network printers. The browsing function is available from Network Neighborhood, the Add Printer Wizard, and even more conveniently, from the **Print Setup** dialog box of Windows NT and Windows 95 applications.
- Clients can browse the network for printer servers running other operating systems. For example, you can browse the network for LAN Manager 2.*x* print servers and connect to print shares on these servers. In this case, Windows NT prompts you to install the appropriate printer driver locally if it is not already present.
- As an administrator, you can remotely administer Windows NT print servers, printers, documents, and printer drivers.
- As an administrator, you do not have to install printer driver files on a Windows NT client computer to enable it to use a Windows NT print server. If all printing clients are running Windows NT or Windows 95, it is only necessary to install printer driver files in one place—at the print server.

Using Windows NT Workstation as a Print Server

Both Windows NT Workstation and Windows NT Server can operate in either client or print server roles. However, because Windows NT Workstation is limited to 10 connections from other computers and because it does not support Services for Macintosh and Gateway Services for NetWare, it is an impractical print server except in small-network situations. Unless otherwise specified, all topics in this chapter apply equally to both Windows NT Workstation and Windows NT Server.

Windows NT Printing Terms

In Windows NT, a *print device* refers to the actual hardware device that produces printed output. A *printer* is a software interface between the operating system and the print device. The printer defines where the document will go before it reaches the print device (to a local port, to a file, or to a remote print share), when it will go, and various other aspects of the printing process. When users connect to printers, they are connecting to logical printer names that represent one or more print devices.

A *printer driver* is a program that converts graphics commands into a specific printer language, such as PostScript or PCL. Windows NT supplies drivers for most available print devices. When you *create a printer*, you install a printer driver and, optionally, make the printer available on the network by sharing it.

Print device resolution is measured in *dots per inch* (dpi). The greater the dpi, the better the resolution.

In Windows NT terminology, a *queue* is a group of documents waiting to be printed. In the NetWare and OS/2 environments, queues are the primary software interface between the application and print device: Users submit documents to a queue. However, with Windows NT, the printer is that interface, the document is sent to a printer, not to a queue.

The print *spooler* is a collection of dynamic-link libraries (DLLs) that receive, process, schedule, and distribute documents.

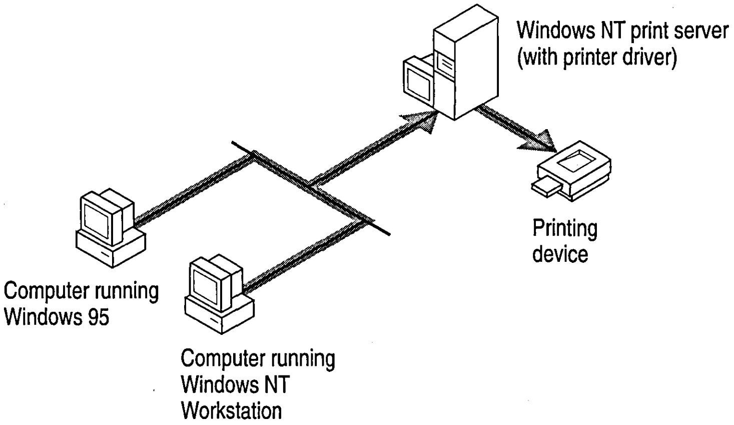
Spooling is the process of writing the contents of a document to a file on disk. This file is called a *spool file*.

A *print server* is the computer that receives documents from clients.

Network-interface print devices are print devices with their own network cards; they need not be physically connected to a print server because they are directly connected to the network.

Windows NT Remote Printing

Windows NT supports true remote printing. When Windows NT and Windows 95 clients connect to a correctly configured Windows NT print server, the printer driver is automatically installed on the client computer. If you install a newer printer driver on the server, Windows NT client computers automatically download the newer printer driver. However, if you install a newer printer driver for Windows 95 clients on a print server, users running Windows 95 must manually update the printer driver to have the newer version copied to their computers.



Non-Windows NT clients (such as MS-DOS and versions of Windows for MS-DOS) can access Windows NT printers by redirecting their output ports to the appropriate \\*server**sharename*. However, unlike computers running Windows NT and Windows 95, users at these types of client computers must install the printer driver manually and then connect to the server.

Fonts and forms available on a Windows NT print server are not accessible by non-Windows NT client computers.

Note When Windows NT clients attempt to use the Add Printer Wizard to connect to a print server managed by a computer running another network operating system, (such as LAN Manager 2.*x* or Novell NetWare), the Add Printer Wizard prompts the user to create a local printer and install a local driver. Because other network operating systems were not designed to provide the printer driver automatically, you must install the driver locally. You must be a member of the Administrators or Power Users group to connect to printer server running on another operating systems.

For information on supporting multiple hardware platforms from a Windows NT print server, see "Installing Printer Drivers for Multiple Hardware Platforms" later in this chapter.

Planning Your Printing Operations

Because every network user has occasion to print, it is worth making sure network print operations are efficient and cost-effective. Choices you need to make include:

- What print devices to use.
- What computers to use as print servers.
- How to configure shared printers for maximum use.

Choosing Printers

Today's choice of print devices includes devices specifically designed for network use. These devices offer options such as automatic port and emulation switching, dual paper bins, and double-sided printing. Before deciding on network printers, carefully evaluate your printing needs:

- Do you need a few high-volume print devices or several less expensive personal print devices?

  High-volume printers generally have more features but affect many more users if they break down.

- How many pages do you expect to print?

  You will probably experience fewer maintenance problems if you match printing volume with a printer's duty cycle (the number of pages it can print per month).

- What graphics support do you need?

  The combination of Windows NT and TrueType technology makes it possible to print sophisticated graphics and fonts on most printers, even those that normally support only bitmaps and text. TrueType is integrated with the operating environment so all Windows NT applications can use TrueType fonts without changes or upgrades. If you intend to print many graphs, charts, or halftone photographs, consider a printer that supports 600 dpi or greater.

- How important is printing speed?

  Whereas shared print devices have traditionally attached to the network through serial or parallel ports on computers, newer print devices connect directly to the network using built-in local area network (LAN) cards. Network links offer faster throughput than currently available parallel and serial buses. However, print throughput rates also depend on network traffic, the network interface card (NIC), the protocol used, and the type of print device used.

- Is the print device on the Windows NT Hardware Compatibility List (HCL)?

  The Windows NT Hardware Compatibility List lists the print devices supported by Windows NT. The latest version of the HCL can be downloaded from the Internet. For more information, see the Microsoft World Wide Web site at http://www.microsoft.com/.

Windows NT supports most traditional print devices, including dot matrix, inkjet, and laser print devices. It also supports network-interface print devices and network-aware print devices connected to the network using the AppleTalk or Transmission Control Protocol/Internet Protocol (TCP/IP) protocols.

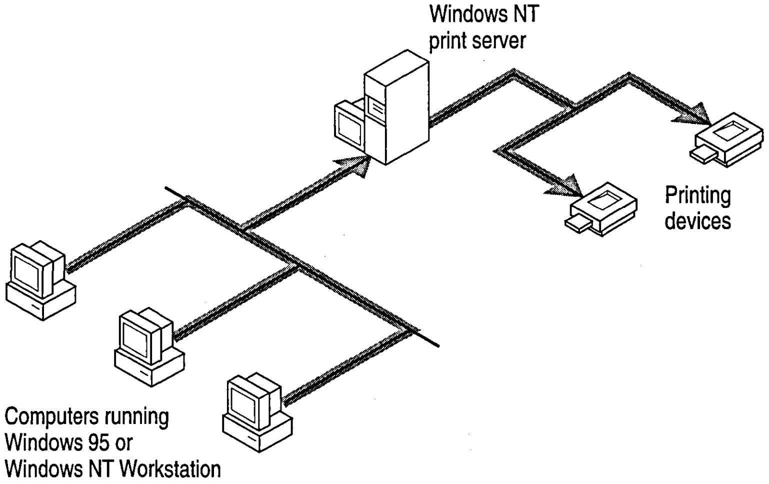
Choosing Computers to Be Print Servers

On a network of any size, you will probably concentrate printer installation at a few select servers. A computer acting as a print server might simultaneously act as a file server or database server. No special hardware requirements exist for print servers except that they have the right output ports if you're using parallel or serial print devices.

Sixteen megabytes (MB) of random access memory (RAM) is adequate for *x*86-based print servers controlling a small number of print devices. Managing a large number of printers or managing many large documents requires more memory. Disk space requirements are minimal except in cases where large or many documents are likely to accumulate.

Combining File and Print Services

When you use Windows NT for both file and print sharing, file operations have first priority. Printing transactions never slow access to files. Moreover, file operations have negligible impact on printers attached directly to the server; parallel and serial ports are always the greater bottleneck. A dedicated print server may be necessary only if the server is to manage many heavily used printers.

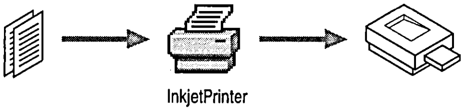


The decision to combine print and file servers may depend on security concerns. While printers should always be available to those persons using them, you may want to secure a file server by restricting it from physical access (for example, by keeping it in a secured room).

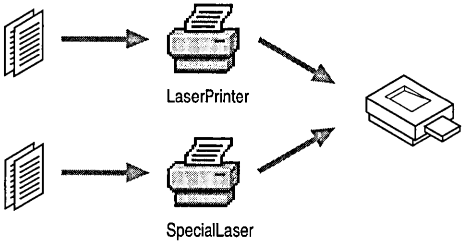
Planning How Users Access Printers

Before installing printers on a server, you need to be aware of configuration options that can improve the flexibility and efficiency of network printing. After studying these options, you will be ready to use the Printers folder to install and configure printers.

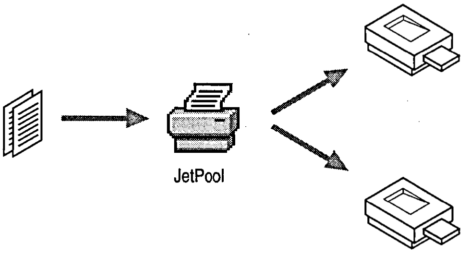
Under Windows NT, it is not necessary to have a one-to-one relationship between printers (the software) and print devices (the physical printer). By associating printers and print devices in different ways, you can offer users flexibility in their printing operations. Several configurations are possible, as shown in the following diagrams.



Single Printer to Single Print Device



Multiple Printers to Single Print Device



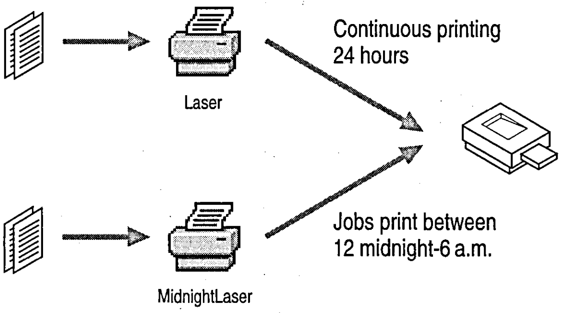
Single Printer to Multiple Identical Print Devices

The capability to assign more than one printer to a print device gives users flexibility in printing documents. For example, two printers associated with a single print device can offer different print properties: one may print separator pages and the other may not. Or one printer can hold documents and print them at night, while the other processes documents 24 hours a day.

Postponing Documents

One way to maximize use of print devices is to stagger printing times. For example, if printer traffic is heavy during the day, you can postpone printing of less important documents by routing them through a printer that prints only during off-hours.

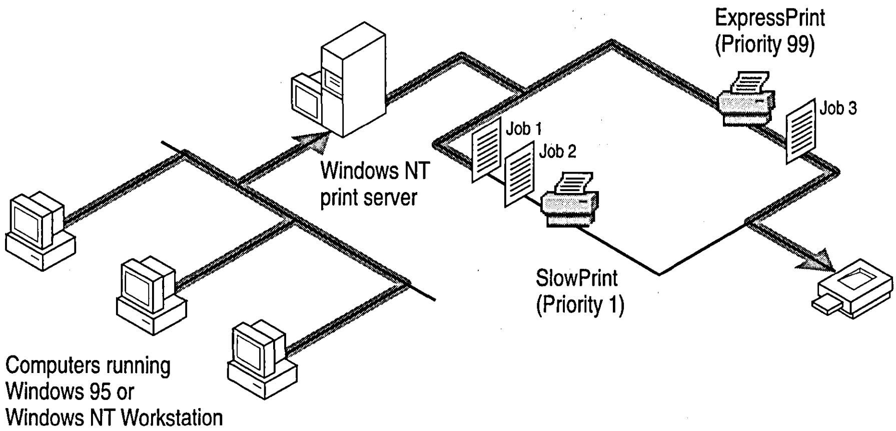
To do this, use the **Scheduling** tab of the printer's Properties sheet to define the time during which a printer can print documents. When you specify printing times, the print spooler accepts documents at any time, but it does not print to the destination print device until the designated start time. At the stop printing time, the spooler stops sending documents to the print device and saves any documents remaining until it is scheduled to start printing again.



For information on changing printer properties, see "Setting Printer Properties" later in this chapter.

Giving Printers Different Priority Levels

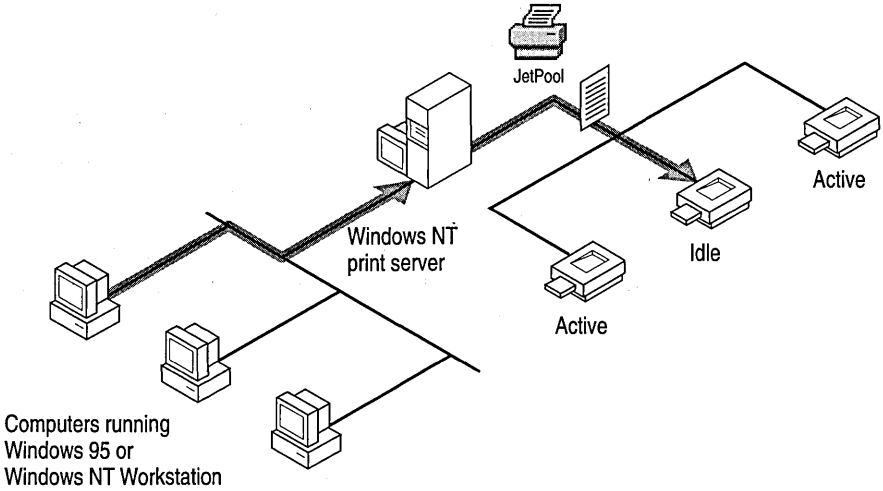
There may be times when you need to print a document immediately and want to bypass the documents waiting for a print device. You can do this by creating printers with different priority levels. (Print priority is set in the **Scheduling** tab of a printer's properties sheet.) If two printers are associated with a single print device, documents routed to the printer with the highest priority level (highest number) print first.



To take advantage of this print priority system, create multiple printers that lead to one print device. Assign each printer a priority level, and then create a group of users that correspond to each printer. For example, users in Group1 might have access rights to a priority 1 printer, users in Group2 might have access rights to a printer with priority 2, and so on. In this way, you can prioritize documents according to the users submitting their documents.

Using a Printing Pool

A *printing pool* consists of two or more identical print devices associated with one printer. To set up a pool, you create a printer using the Add Printer Wizard and assign it as many output ports as you have identical print devices. (Windows NT places no limit on the number of printers in a pool.) Whichever print device is idle receives the next document. This configuration maximizes use of print devices while minimizing the amount of time users must wait for documents.

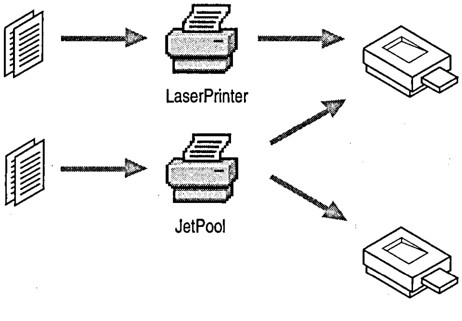


Printer pools have the following characteristics:

- All devices in the pool are the same hardware model and act as a single unit. All print property settings apply to the whole pool.
- Printer ports can be of the same type or mixed (parallel, serial, and network).
- When a documents arrives for the printer pool, the spooler checks printer output destinations to see which device is idle.
- If one device within a pool stops printing—when it runs out of paper, for example—it will hold a single document at that device. Other documents continue to print to the other devices in the pool, while the delayed document waits until the nonfunctioning device is fixed or the document is restarted.

It is impossible to predict which printer in a pool will receive a particular documents. However, if the Windows NT Messenger Service is active, a workstation will receive messages indicating when documents are complete and identifying the printer by output port. Unless you want users to rely on these messages, it is a good idea to place pooled print devices in a single location.

A particularly flexible printer configuration is one in which a print device is accessible both in and outside of a printing pool, as shown in the following figure. This configuration provides both the fast throughput of a printing pool and the flexibility of more than one printer.



Attaching Printers to Your Network

After deciding how users should share network printers, you're ready to attach print devices to the network. Shared printers can connect to the parallel or serial ports on the print server computer or directly to the network if they have a built-in network adapter card.

Configuring Parallel and Serial Printers

Print devices attach to computers through parallel or serial port connections. Parallel cables must be less than 20 feet long; serial cables can be up to 100 feet long. Standard Intel 486 and Pentium-based computers support three parallel ports and two serial ports. RISC-based computers generally come with one parallel and two serial ports built in and support as many additional ports as there is space for.

Note Although standard Intel 486 and Pentium-based computers support three parallel ports, they usually have only one installed. For easier installation, configuration, and support, or for non-network-interface print devices, use only the first parallel port (LPT1) or a serial port.

When configuring parallel ports, you might have to set hardware jumpers or switches. Serial communication requires flow control (also called *handshaking*), which defines a method for the print device to tell Windows NT that its buffer is full. Serial ports can be configured for no flow control, XON/XOFF (software flow control), or hardware flow control by choosing the Ports icon in the Windows NT Control Panel folder. Your print device documentation should tell you what communications settings to use. The setting is typically 9600 baud, No parity, 8 bits, 1 stop bit, and Hardware Handshaking.

If you are using a serial print device, use the cable that originated with the device. Wiring schemes often vary from cable to cable.

Setting Hardware Interrupt Levels

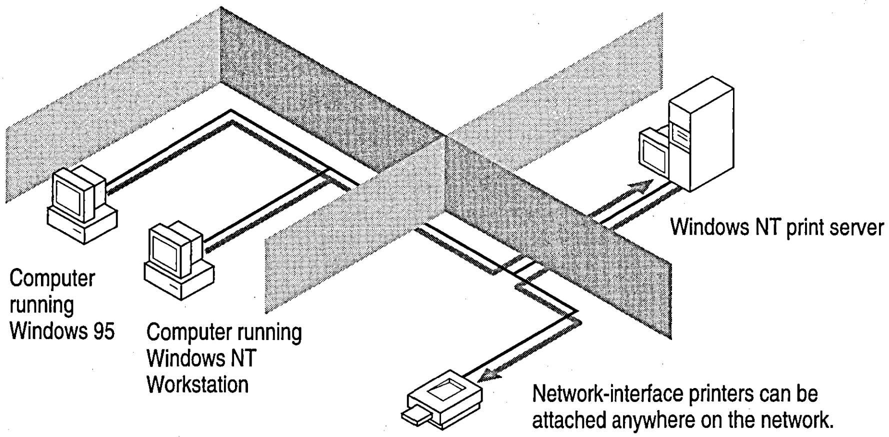
Although Windows NT supports an unlimited number of serial (COM) and parallel ports, the number of devices you can attach to a computer depends on the number of interface card slots and addresses available. If you attach print devices to COM ports on x86-based computers, you are also limited by the number interrupt request (IRQ) lines available. Because x86-based computers have a limited number of IRQs, finding an available IRQ level for COM ports can be difficult.

On RISC-based systems COM1, and COM2 are built in and do not conflict with IRQ levels on the Extended Industry Standard Architecture (EISA) bus. This frees IRQs 3, and 4 for other devices.

Some interface cards support the sharing of interrupts. This means two device addresses can use the same IRQ level. However, some devices require exclusive use of certain interrupts. To avoid conflicts, check hardware manuals for these devices before configuring your ports. To see current IRQ settings on your computer, run the Microsoft Diagnostics program (*systemroot*\SYSTEM32\WINMSD.EXE).

Configuring Network-Interface Printers

Unlike parallel and serial devices, print devices with built-in network adapter cards do not have to be physically connected to the print server. Where you locate these types of print devices has no effect on printing performance, assuming users and print devices are not on opposite sides of a network bridge or gateway. A Windows NT print server can control dozens of network-interface printers, depending on the server's processing capability, the amount of installed memory, and the size and number of documents typically sent to the print server. To maintain high server throughput levels, increase memory as you add print devices.


Windows NT print server
Computer running Windows 95
Computer running Windows NT Workstation
Network-interface printers can be attached anywhere on the network.

Network-interface print devices are attached to the network through a built-in adapter card or add-on attachment. To use a network-interface printer, install the data link control (DLC) protocol or the Microsoft TCP/IP Printing service, depending on what printing methods your print device supports. AppleTalk printers require the AppleTalk protocol. TCP/IP LPR printers require the TCP/IP protocol and Microsoft TCP/IP Printing service. Use the Network icon in the Control Panel folder to install these protocols and services during Setup or later.

In most cases, you must determine the network-print device's address before you set up your Windows NT print server. If you are printing over TCP/IP, you usually need the print device's TCP/IP address. If you are printing to a Hewlett-Packard network-interface print device, run a self-test to obtain the network card address. If you are printing to an AppleTalk print device, you need to know in which zone the print device is located.

Configuring TCP/IP and UNIX Printers

Users on any client computer can print to network-attached TCP/IP print devices or to print devices that are physically attached to most UNIX computers. To enable this on your network, at least one Windows NT computer must have the TCP/IP protocol and the Microsoft TCP/IP Printing service installed.

To take advantage of the printing capabilities of the Microsoft TCP/IP Printing service, only the single Windows NT computer that defines a TCP/IP printer needs to have TCP/IP installed. Clients can print to the Windows NT print server using any protocol that both the client and server have installed. The print server then sends the document to the TCP/IP print device.

Use the **Protocols** tab of the Network option in Control Panel to install the TCP/IP Protocol or the DLC Protocol. Use the **Services** tab of the Network option in Control Panel to install the Microsoft TCP/IP Printing service.

For more information on TCP/IP, see the *Windows NT Server Resource Kit* version 4.0 *Networking Guide.*

The Windows NT TCP/IP Printing Service (LPD)

A line printer daemon (LPD) service on the print server receives documents from line printer remote (LPR) utilities running on client systems. LPR clients and LPD servers are often UNIX systems, but LPR and LPD software exists for most operating systems, including Windows NT. Also, many network-attached print devices can be used as LPD print servers.

TCP/IP Printing Compatibility

In previous versions of Windows NT, TCP/IP printing adhered to Request For Comment (RFC) 1179. However, this RFC "describes an existing print server protocol widely used on the Internet for communicating between line printer demons" and does not specify an Internet standard. Consequently, different TCP/IP printing implementations support different options.

Several enhancements were added for TCP/IP printing in Windows NT 4.0. It now supports multiple data files per control file. When used as an intermediate spooler, it correctly passes the hostname parameter through the Windows printing subsystem. Also, Windows NT TCP/IP printing now uses TCP ports 512 through 1023 for LPR jobs instead of TCP ports 721 through 731.

You can install the LPD service under Windows NT by installing the Microsoft TCP/IP Printing Service from the Network option in the Control Panel folder. By default, the LPD service is set to start manually. To have it start automatically, use the Services icon in Control Panel, and change the startup options for the TCP/IP Print Server service.

Sending Documents using LPR in Windows NT

LPR lets a client application on one computer send a document to a print spooler service on another computer. The client application is usually named LPR and the service (or daemon) is usually named LPD. Windows NT supplies a command-line application, the LPR.EXE utility, and the LPR Port monitor. Both act as clients sending documents to an LPD service running on another computer.

You can use the Add Printer Wizard to create a TCP/IP printer in the same way that you create any printer to be used on a Windows NT network. You need the following information to create a TCP/IP printer:

- The IP identifier of the LPD print server where the printer is connected.

  The LPD print server is often a computer, but it can be a network-attached print device. In either case, the identifier can be the Domain Name Service (DNS) name or the IP address.
- The printer name as it is identified on the LPD print server.

  This is the name defined on the LPD computer or the name defined by the manufacturer for the LPD compliant network-attached print device.

For more information on running the Add Printer Wizard, see "Creating Printers on a Server" later in this chapter.

Receiving Documents Printed over LPR

Because Windows NT also supplies an LPD service (the Microsoft TCP/IP Printing service), it can receive documents sent by LPR clients, including UNIX computers and other Windows NT computers.

The LPD service is independent of the Lprmon port monitor. Lprmon runs automatically to allow a Windows NT computer (and all clients who can access this computer) to print to a printer connected to a UNIX system, as described in the preceding section.

LPR client software needs to know the name of the printer on the LPD host. If the LPD host is a computer running Windows NT, that name is the printer name, not the printer share name. In other words, use the name of the printer as identified in the Printers folder and in the printer's Properties sheet. Do not use the printer's share name, which is specified in the **Scheduling** tab of the printer's Properties sheet.

If documents sent by UNIX LPR clients do not print correctly on Windows NT print servers, the problem can often be corrected by reconfiguring the UNIX LPR software to use the lowercase (l) control command.

Note Windows NT, and most Berkeley UNIX (BSD) operating systems, comply with RFC 1179. However, most System V UNIX operating systems do not comply with this standard. Consequently, in most cases, Windows NT cannot send documents to System V computers or receive documents from them. System V computers that are configured to accept BSD documents are the exceptions. These computers can accept Windows NT documents.

For more information on TCP/IP printing and LPD, the *Windows NT Server Resource Kit* version 4.0 *Resource Guide.*

Using Printers on Novell NetWare Networks

- To enable Windows NT clients to print directly to NetWare printers, install Windows NT Client Services for NetWare (CSNW) on each client.
- To set up a print server that allows Microsoft network clients to print to a print device shared by Novell NetWare, install Windows NT Gateway Services for NetWare (GSNW) on the print server.
- To allow NetWare clients to print to Windows NT network printers and to allow Microsoft Network clients to print to NetWare servers, use Microsoft File and Print Services for NetWare (FPNW). Microsoft FPNW is not included in Windows NT but can be obtained from your software vendor.

For more information on Client Services for NetWare and Gateway Services for NetWare, see the *Windows NT Server Networking Supplement.*

Using Print Devices on AppleTalk Networks

Both Windows NT Workstation and Windows NT Server computers can print to AppleTalk print devices and AppleShare print servers. However, only Windows NT Server includes Services for Macintosh, which enables Macintosh clients to print to Windows NT print servers.

For more information on installing and configuring printers and clients for use with Services for Macintosh, see the *Windows NT Server Networking Supplement.*

Creating Printers on a Server

After physically connecting print devices, you must create a printer. To do this, run the Add Printer Wizard from the Printers folder.

Permission Required to Create a Printer

To create a printer on a server, you must be logged on as a member of the Administrators, Server Operators, or Print Operators group. (If the server is not a primary or backup domain controller, you must be logged on as a member of the Administrators or Power Users group.)

When you create a printer, you:

- Select the printer port. (If you are using a printer pool, select multiple ports.)
- Select the printer manufacturer and model.
- Set the printer name.
- Set the printer share name so it is available to network users. If Windows 3.*x* clients and MS-DOS clients will be connecting to the printer, use a short file name.
- Choose which hardware platforms and operating systems to support (Windows NT clients on Alpha, MIPS, Power PC, or *x*86 computers and Windows 95 clients).

After you define the general characteristics of your printer, you are prompted to assign the printer certain device-specific *properties* (fonts, printer memory, color, and so forth). How you set properties depends on how you want users to access print devices. (See "Planning How Users Access Printers" earlier in this chapter). If you do not change a specific property, Windows NT prints using default settings.

After you create and share the printer, it appears in the network-wide printer browse list. Windows NT and Windows 95 clients can connect to Windows NT printers from this list in the Add Printer Wizard.

For more information about sharing printers, see "Sharing Printers" later in this chapter.

For more information on specifying which hardware platforms and operating systems to support, see "Installing Printer Drivers for Multiple Hardware Platforms" later in this chapter.

For more information on setting device-specific properties, see "Setting Device-Specific Properties" later in this chapter.

For more information on installing a print driver for an unsupported printer, see "Installing a Printer Driver for an Unsupported Printer" later in this chapter.

Choosing a Port

The process of selecting a port and the subsequent options displayed by the Add Printer Wizard depend on how your printer is connected to the server or network and what software (including protocols) you have installed.

If the print device is attached to the local port, select the appropriate local port or select FILE. LPT1 through LPT3 represent parallel ports. COM1 through COM4 represent serial ports. If your Windows NT print server has a multiport serial adapter, you can set up more serial ports using the Ports option in the Control Panel. When a client prints to a print server that is configured to print to a file, the client is prompted for the file name, and the output file is stored on the clients computer.

If the print device is attached directly to the network, select the Add Port button when the Add Printer Wizard prompts you to select a port, and then select the appropriate port type. The following table lists the port options available when you click **Add Port** and explains under what conditions the port is available.

Additional port	Enables clients to print	Available
AppleTalk Printing Devices	To AppleTalk print devices	When the AppleTalk protocol is installed.
Digital Network Port	To DEC print devices.	When the Microsoft TCP/IP or DEC DECNet protocol is installed.
Hewlett-Packard Network Port	To print devices that use an HP JetDirect adapter.	When the DLC network protocol is installed.
Local Port	To a print device connected to a parallel port, serial port, specific file name, universal naming convention (UNC) name, or to the NUL port.	By default.
LPR Port	From line printer remote (LPR) applications to a Windows NT printer.	When the Microsoft TCP/IP Printing service is installed.

To create a printer pool, configure a printer to print to more than one destination. Use the **Protocols** tab of the Network option in Control Panel to install the DLC Protocol. Use the **Services** tab of the Network option in Control Panel to install the Microsoft TCP/IP Printing service.

For information on Services for Macintosh and the AppleTalk protocol, see the *Windows NT Server Networking Supplement.*

Installing Printer Drivers for Multiple Hardware Platforms

Different hardware platforms and operating systems require different printer drivers. For example, to use a printer created on an *x*86-based Windows NT computer, a client running Windows NT on an Alpha computer requires the appropriate Alpha printer driver for that printer. The driver can be installed locally or on the *x*86-based server. Likewise, x86-based clients can use an Alpha print server only if the requisite *x*86 drivers are installed locally or on the server.

If your network contains a mixture of Windows 95, Alpha, Power PC, MIPS, and *x*86-based computers, you can install printer drivers for each one on each print server. This ensures that documents originating from Windows NT or Windows 95 clients running on any of the hardware types can use all print devices. Also, if you have clients running previous version of Windows NT, you will need to install the appropriate older printer drivers for each version/platform combination. Three separate printer drivers are required for each hardware platform to support all versions of Windows NT: one for Windows NT 3.1, one for Windows NT 3.5 and Windows NT 3.51, and one for Windows NT 4.0.

Note When you choose to install an alternate driver for Windows 95, you are prompted for the Windows 95 printer driver file(s). Because Windows NT Setup cannot extract these files from the Windows 95 .cab files, you must use the Windows 95 Extract.exe program to extract the printer driver file(s) from the Windows 95 installation media (CD or floppy disks) or from the Windows 95 .cab files on the Windows NT Server CD.

For example, if your network contains Windows 95 clients, *x*86-based clients running Windows NT 4.0 and 3.51 and Alpha clients running Windows NT 4.0 and 3.51, and you are creating a shared printer on an *x*86-based computer, you should install four printer drivers in addition to the *x*86-based Windows NT printer driver that is installed by default for the printer you have selected:

- Windows 95
- Windows NT 3.5 or 3.51 *x*86
- Windows NT 4.0 Alpha
- Windows NT 3.5 or 3.51 Alpha

Windows NT print server determines whether incoming print requests are Alpha, Power PC, MIPS, or *x*86-based and automatically sends the appropriate driver to the client.

To install multiple printer drivers, select each version/hardware platform pairing in the Add Printer Wizard after you choose to share the printer. You can also add support for other platforms later from the printer's Properties Sharing property sheet.

Downloading the Printer Driver

Windows 95 clients do not obtain printer drivers on Windows NT version 4.0 print servers in the same way that Windows NT clients use the printer drivers. Windows NT clients download the printer driver from the server if a newer version has been installed on the server. However, Windows 95 clients use a technology called Point and Print to download the printer driver and some printer settings to the client only when the client runs the Windows 95 Add Printer Wizard.

For more information on changing a printer's properties after the printer is installed, see "Setting Printer Properties" later in this chapter.

Installing a Printer Driver for an Unsupported Printer

If a particular device is not supported, try setting up the printer according to the following table.

If it is a	Set it up as a
Laser printer:	
HPPCL (LaserJet) compatible	Hewlett-Packard LaserJet Plus
PostScript compatible	
Color PostScript	QMS-ColorScript
35-font Plus font set or superset	Apple LaserWriter® Plus
Dot matrix printer:	
9-pin dot matrix	
IBM compatible	IBM Proprinter
Epson® compatible	Epson FX-80 for narrow or FX-100 for wide carriage
24-pin dot matrix	
IBM 24-pin compatible	IBM Proprinter X24
Epson LQ compatible	Epson LQ-1500

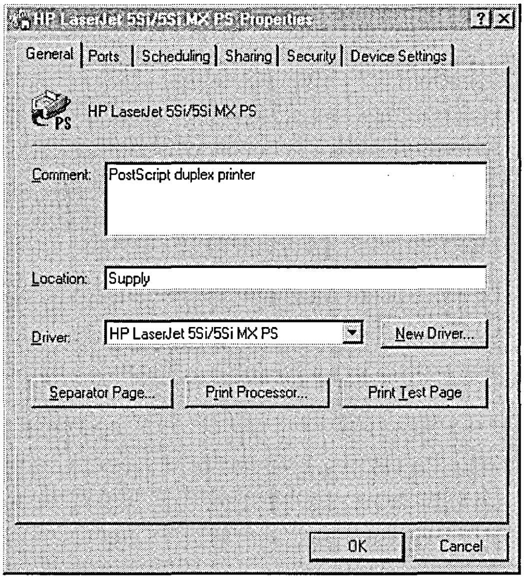
If your device is not in this list, contact the manufacturer to determine if custom drivers are available.

For information about obtaining new printer drivers for your system, obtain the latest version of the Windows NT HCL or contact your hardware manufacturer. The latest version of the HCL can be downloaded from the Internet. For more information, see the Microsoft World Wide Web site at http://www.microsoft.com/.

Setting Printer Properties

You set properties for a printer as the last step in the Add Printer Wizard and at any time by displaying the printer's Properties sheets. The printer's Properties sheet includes:

- General properties (printer driver and separator page settings)
- Port selections and port properties
- Document scheduling and spooling properties
- Printer share name and alternate printer drive settings
- Security settings
- Device-specific properties



HP LaserJet 5Si/5Si MX PS

Comment: PostScript duplex printer

Location: Supply

Driver: HP LaserJet 5Si/5Si MX PS

To view to a printer's property sheet, open the Printers folder, click the printer, and then click **Properties** on the **File** menu.

Setting General Printer Properties

Use the **General** tab of a printer's Properties sheet to:

- Set or change the printer's comment or location settings.
- Set or change the print device type (for example, HP LaserJet 4Si).
- Change the driver the printer uses.
- Select a separator page.
- Select a print processor.
- Print a test page.

The printer's comment text is useful for indicating the print device location to Windows NT clients who are browsing for a printer.

You can install an updated driver or print processor using the **New Driver** and **Print Processor** buttons, respectively.

Using Separator Pages

You can set up a printer so that one or more separator pages appear at the beginning of each document. (Separator pages typically state who submitted the document and give the date and time of printing.)

To select a separator page file, click the **Separator Page** button in the **General** tab of the printer's Properties sheet. Enter the name of the separator page file directly, or browse through the folders and select a file. Use one of three separator pages included with Windows NT or a custom separator page file you create.

The following table shows the names of separator files supplied with Windows NT, the purpose of each, and the type of printer with which each is compatible. All three separator pages can be edited. By default, separator page files are kept in the *systemroot*\SYSTEM32 folder.

File name	**Purpose**	**Compatible with**
SYSPRINT.SEP	Prints a page before each document.	PostScript
PCL.SEP	Switches printer to PCL printing and prints a page before each document.	PCL
PSCRIPT.SEP	Switches printer to PostScript printing, but does not print a separator page before each document.	PostScript

Using Custom Separator Pages

To customize a separator page, rename and modify one of the supplied separator files. The following table shows the command delimiters you can include in a separator page file. Windows NT replaces these command delimiters with appropriate data to be sent directly to the printer.

Command delimiters always start with a specific character and end with a letter or number. The first line of your custom separator page must contain only the command delimiter.

Command	Function
\	The first line of the separator file is a single character. The separator file interpreter considers this the separator file command delimiter. This table assumes that character is the backslash (\) character.
\N	Prints the user name of the person who submitted the document.
\I	Prints the document number.
\D	Prints the date the document was printed. The representation of the date is the same as the Date Format in the International section in Control Panel.
\T	Prints the time the document was printed. The representation of the time is the same as the Time Format in the International section in Control Panel.
\L*xxxx*	Prints all the characters (*xxxx*) following it until another command delimiter is encountered or until the separator page width character count is reached. (See \W*nn*.)
\Fpathname	Prints the contents of the file specified by the path, starting on an empty line. The contents of this file are copied directly to the printer without any processing.
\H*nn*	Sets a printer-specific control sequence, where *nn* is a hexadecimal ASCII code sent directly to the printer. To determine the specific numbers, see your printer manual.
\W*nn*	Sets the width, in characters, of the separator page. The default width is 80; the maximum width is 256. Any printable characters beyond this width are truncated.
\B\S	Prints text in single-width block characters until \U is encountered.
\E	Ejects a page from the printer. Use this code to start a new separator page or to end the separator page file. If you get an extra blank separator page when you print, remove this code from your separator page file.
n	Skips *n* number of lines (from 0 through 9). Skipping 0 lines simply moves printing to the next line.
\B\M	Prints text in double-width block characters until \U is encountered.
\U	Turns off block character printing.

Adding, Deleting, and Configuring Ports

Use the **Ports** tab of a printer's Properties sheet to:

- Increase or decrease the numbers of printer in a printer pool.
- Change which port a printer prints to.
- Add a new port.
- Delete a port.
- Adjust port settings.

Note When you adjust serial and parallel port settings or add and delete ports, you affect not just the selected printer, but the entire system.

Changing Scheduling and Spooling Settings

Use the **Scheduling** tab of the printer's Properties sheet to change the document scheduling and spooling settings. You can set:

- The range of time the printer is available
- Document priority
- Document spooling options
- Print-queue management options

The following table shows the specific options in the **Scheduling** tab of the printer's Properties sheet.

Option	Description
Available	Defines when the printer is available.
Priority	Sets up a varied priority print queue based on document priority.
Start printing after last page is spooled	Prevents delays when the print server prints pages faster than clients can provide them.
Start printing immediately	Prints documents as quickly as possible (the default).
Print directly to the printer	Sends documents to the print device without first writing them to the print server's hard disk drive.
Hold mismatched documents	Has the spooler hold documents if they do not match the available form. This allows other documents that do match the form to print until the correct form in loaded.

(continued)

Option	Description
Print spooled documents first	Has the spooler print documents in the order that they finish spooling, rather than in the order that they start spooling. Use this option with Start printing immediately.
Keep documents after they have printed	Allows users to resubmit a document from the print queue instead of an application.

Sharing Printers

To share a printer with network computers, select the *Sharing* tab in the printer's Properties sheet, click **Shared**, and then provide *a share name.*

Although you can create long printer names containing spaces and special characters, some clients do not recognize or handle them correctly. If you use a mixture of clients on your network, choose printer names that are 31 or fewer characters and that do not contain spaces or special characters.

Windows NT clients can connect to a printer using either the printer name or the printer share name. Clients running other operating systems connect to the printer share name. If you are sharing printers with computers running MS-DOS share names must be no more than eight characters, optionally followed by a period and one to three characters and should not contain spaces.

Note To print from MS-DOS-based applications under Windows NT to Windows NT print servers, you must first issue the **net use** command from the Windows NT command prompt. For more information on using the **net use** command, type **net use /?** at the Windows NT command prompt.

You also use the **Sharing** tab to install printer drivers form multiple platforms. For more information, see "Installing Printer Drivers for Multiple Hardware Platforms" earlier in this chapter.

Security

Using Windows NT security features you can control access to printers, track printer use and ownership, and take ownership of printers.

Controlling Printer Access

To control printer usage under Windows NT, set permissions for each printer. By default, all shared printers you create are available to all network users. To restrict access to a printer you must alter the printer's permission settings for a particular group or user. To change permissions on a printer, you must be the owner of the printer or have been granted Full Control permission. To change printer settings, click the **Security** tab in the printer's Properties sheet and then click **Permissions**.

Four types of permissions apply to network printers:

- No Access
- Print
- Manage Documents (permission to manage all documents aimed at that printer)
- Full Control

Although permissions are cumulative, the No Access permission overrides all other permissions.

To allow the following uses of a printer, grant the permission shown in the following table.

● Permission allows use
○ Permission does not allow use

	No Access	Print	Manage Documents	Full Control
Print documents	○	●	○	●
Control settings for documents	○	○	●	●
Pause, resume, restart, and delete documents	○	○	●	●
Change the printing order of documents	○	○	○	●
Pause, resume, purge printer	○	○	○	●
Change printer properties	○	○	○	●
Delete printer	○	○	○	●
Change printer permissions	○	○	○	●

By default, Administrators, Print Operators, and Server Operators have Full Control rights on a server; Administrators and Power Users have Full Control rights on workstation computers. All users can manage their own documents.

Controlling How Macintosh Clients Access Printers

Although native Macintosh networking provides support for file security, it does not provide support for print-device security. If a Macintosh client is physically able to send a document to a print device or print server, it implicitly has permission to do so. The AppleTalk protocol has no mechanism that supports client-user name or password. Macintosh print clients, therefore, cannot identify themselves on the network, and the Windows NT print server cannot impose user-level security on Macintosh clients.

You can, however, enforce one set of printer permissions on all Macintosh users as a group. The Windows NT Server MacPrint service always logs on using a user account; by default, it logs on as the System account. The System account has Print permission on all local print devices, so by default, any Macintosh client can send a document to any of the Windows NT computer's local printers. If you want Macintosh clients to have a different set of permissions, you must create a new user account, give this user account the printer permissions you want Macintosh users to have, and set the Macintosh client MacPrint service to log on using this account.

Auditing

By *auditing* a printer, you track its usage. For a particular printer, you can specify which groups or users and which actions to audit. You can audit both successful and failed actions. Windows NT stores the information generated from auditing in a file. You can view the information using Event Viewer. For more information, see Chapter 9, "Monitoring Events."

Important To audit a printer, you must set the audit policy to audit file and object access. Set the audit policy using User Manager for Domains. For more information on audit policy, see Chapter 1, "Managing Windows NT Server Domains."

To audit the following activities for a printer, select the events shown in the following table.

● Event audits action
○ Event does not audit action

	Print	Full Control	Delete	Change Permissions	Take Ownership
Printing documents	●	○	○	○	○
Changing job settings for documents	○	●	○	○	○
Pausing, restarting, moving, and deleting documents	○	●	○	○	○
Sharing a printer	○	●	○	○	○
Changing printer properties	○	●	○	○	○
Deleting a printer	○	○	●	○	○
Changing printer permissions	○	○	○	●	○
Taking ownership	○	○	○	○	●

Taking Ownership

Use the **Ownership** button to determine who owns the printer and, optionally, to take ownership of the printer. You can take ownership of a printer if you have Full Control of the printer or if you are logged on as a member of the Administrators group. Ownership allows you to set permissions for the printer.

Setting Device-Specific Properties

Device-specific printer properties describe the physical configuration of a print device, such as which paper trays are loaded, how much memory a device has, and so forth. These properties vary from device to device. When you create a printer, use the printer's Properties **Device Settings** tab to make sure device-specific properties match the settings of the print device. Although default settings work for many printing needs, some special printing options, such as those available with PostScript printer drivers, require specific settings.

Setting Printer Memory

Because page printers must store an entire page in memory, they require relatively large amounts of memory. If you are using a page printer, such as a laser printer, make sure that the amount of memory available in the device matches the value shown in the **Device Settings** tab. If the print device has substantially more or less memory than what is shown in the **Device Settings** tab, print throughput can suffer. For example, Windows NT might try to download more fonts to the printer than it can reasonably handle. (Running a printer self-test usually tells you how much RAM the device contains.)

To adjust the **Printer Memory** setting on the printer's Properties **Device Settings** tab, double-click the printer icon in the Printers folder and then click **Properties** on the **Printer** menu.

Using Print Forms

Windows NT uses form-based printing model rather than a tray-based printing model. Under a form-based model, the print server administrator configures the Windows NT print server by defining the form loaded in each paper source (tray). The form is defined in Windows NT using the following criteria:

- Size
- Printer area margins
- Form name

Using Windows-based applications running on a Windows NT-based computer, each user can select a desired print form. This frees the user from having to know which tray contains which form. The Windows NT print server spooler modules contain tray and form assignment data and send instructions to the print device to select the correct tray.

Windows-based applications can use different forms within a document. For example, you might use Envelope for the first page, Letterhead for the second page, and Letter for the third and following pages.

Note To set the default form, select the **Draw selected form only from this tray** check box in the printer's Properties **Device Settings** tab.

For information on creating custom forms, see the "Creating Custom Forms" section later in this chapter.

Choosing Font Types

Fonts are collections of characters and symbols that have a specific design and resolution. Print devices use three types of fonts:

- *Device fonts* actually reside in the hardware of your print device. They can be built into the print device itself or can be provided by a font cartridge or font card.
- *Screen fonts* are Windows NT fonts (including TrueType fonts) that can be translated for output to the print device. To install screen fonts, use the Fonts option in the Control Panel folder.
- *Downloadable soft fonts* are installed using the **Device Settings** tab of the printer's Properties sheet. Clients that use soft fonts and that print to Windows NT print servers should install soft fonts locally.

Windows NT includes three types of screen fonts that can be reproduced on printers:

- *TrueType fonts* are device-independent fonts that can be reproduced on all print devices. TrueType fonts are stored as outlines and can be scaled and rotated. To be reproduced on a print device, fonts only need to be present on the computer originating the document. The greatest benefit of TrueType in a networking environment is its portability; documents with TrueType fonts are independent of any one print device, application, or system.
- *Raster fonts* are stored as bitmaps and are device dependent. If a print device does not support raster fonts, it will not print them. Raster fonts cannot be scaled or rotated.
- *Vector fonts* are useful for devices such as pen plotters that cannot reproduce bitmaps. They can be scaled to any size or aspect ratio.

For each document, Windows NT downloads required screen and soft fonts to the print device. To improve printing times, use device fonts, which are already present at the print device.

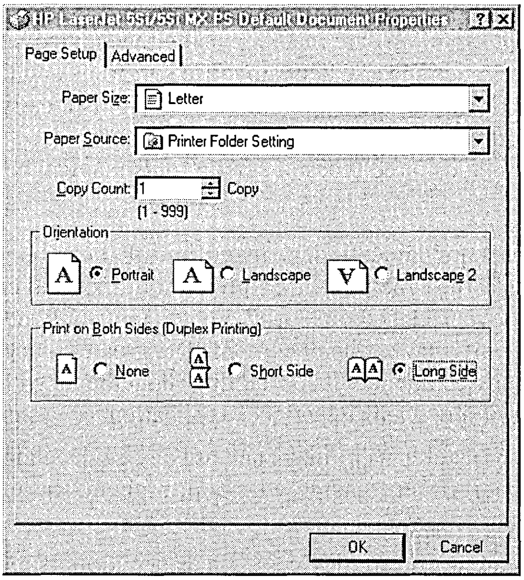
Not all devices can use all three types of printer fonts. Pen plotters, for example, cannot normally use downloadable soft fonts or print raster screen fonts.

Setting Document Defaults

It is easy to confuse printer-specific settings with document properties. Document properties do not rely on a device's physical settings. When applications create a new document, they often ask the printer for the default document settings.

The following table shows typical document and printer-specific properties.

Device-specific properties	Document properties
Color	Number of copies
Resolution	Page orientation
Memory	Two-sided printing
Font cartridge name	Collate copies
Form location	Form
Plotter pen	



Paper Size: Letter

Paper Source: Printer Folder Setting

Copy Count: 1 Copy
(1 - 999)

Orientation

● Portrait ○ Landscape ○ Landscape 2

Print on Both Sides (Duplex Printing)

○ None ○ Short Side ● Long Side

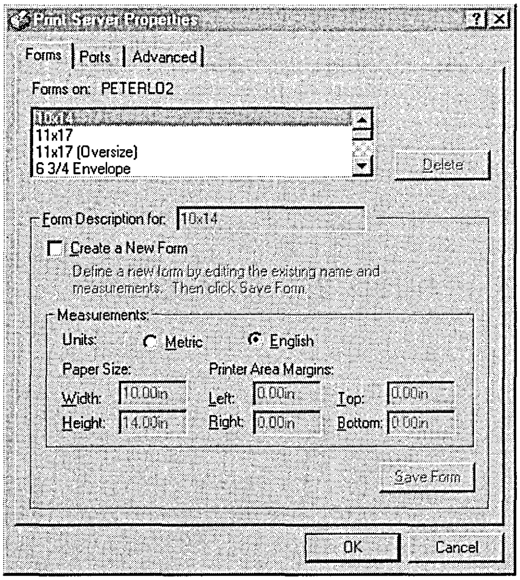
To view a printer's Document Properties, open the Printers folder, click the printer, and then click **Document Defaults** on the **File** menu.

Important Document properties set from an application always override document defaults set in the printer's property sheets. However, if an application does not set a document property (such as page orientation or paper size), the print device defaults to the document properties set in the printer's Document Properties sheets.

Setting Server Properties

You set server properties by displaying and modifying the server's Properties sheet. From these property sheets you can:

- Create custom forms that are available to all printers on the server.
- Change port settings for all ports on the server.
- Choose a new spool file location, set spooler error logging, and set notification options for all printers on the server.



Forms on: PETERLO2

10x14
11x17
11x17 (Oversize)
6 3/4 Envelope

Form Description for: 10x14

□ Create a New Form

Define a new form by editing the existing name and measurements. Then click Save Form.

Measurements:

Units: ○ Metric ● English

Paper Size: Width: 10.00in Height: 14.00in

Printer Area Margins: Left: 0.00in Right: 0.00in Top: 0.00in Bottom: 0.00in

To view a print server's Properties tab, open the Printers folder, and then click **Server Properties** on the **File** menu.

Creating Custom Forms

Any user with Full Control permission can define a new form by using the server's Properties **Forms** property sheet. For example, you could create a form called "Customer Receipt Form" that uses letter-size paper and nonstandard margins. You can also can create multiple forms with the same paper size or margins (or both), to meet specific user needs. For example, you can create forms that have unique names but the same paper size and image area (margins) to identify different departmental letterhead.

New form definitions are added to the print server's database and are stored per server, not per printer. You assign forms to a specific print device and tray using the printer's Properties **Settings** property sheet.

If an odd-sized form is needed for a single document and will not likely be used again, specify **Manual Feed** in the **Paper Tray** box.

Configuring Server Ports

The server's Properties **Ports** property sheet enables you to change some of the same settings that you can change from the printer's Properties **Ports** property sheet. From the server's **Ports** tab in the **Properties** dialog box, you add, delete, and configure ports. However, to increase or decrease the numbers of printers in a printer pool or change which port a printer is connected to, you must use the printer's Properties **Ports** property sheet.

For information on changing port settings, see "Adding, Deleting, and Configuring Ports" earlier in this chapter.

Setting Advanced Server Properties

With the server's Properties Advanced property sheet, you can:

- Set the spool folder location.
- Enable spooler event logging.
- Configure the print server to beep when remote documents encounter errors.
- Configure the print server to notify the client when a remote document has finished printing.

If you specify a spool directory located on a Windows NT file system (NTFS) formatted drive, users must have Change permission to print.

When spooler event logging is enabled, Windows NT logs errors to the system log. To view the system log, run Event Viewer.

For more information on using Event Viewer, see Chapter 9, "Monitoring Events."

Managing a Print Queue

All direct management of printers and documents takes place through the Printers folder. Some queue management options control the entire print queue; others control a single document.

When managing the queue you can:

- View a list of documents for each installed printer.
- Pause or resume printing.
- Purge documents waiting for a printer.

When managing a document you can:

- Pause or resume printing.
- Restart the document from the beginning.
- Delete a document.
- View, and optionally change, various document settings (such as the document priority and the person notified when the document is done). You can also view—but not change—the form type, paper source, page orientation, and number of copies.

For information on managing queues, see "To view documents waiting to be printed" in Windows NT Help.

Viewing and Managing Remote Printers

You can manage a local or remote print server from any Windows NT client on the network, as long as you have Full Control permission at that print server. When you select a printer from Network Neighborhood, you can remotely manage printer properties and create new printers, just as you would locally. However, to add, delete, or configure ports, you must administer the print server locally.

Any network user can check on the status of a remote printer. However, only users who have Full Control or Manage Documents permission for a printer can manage documents other than their own. If you do not have the correct permission, some options are unavailable. Also, when you attempt to view some properties on computers running an older version of Windows NT, an error message appears.

Tip To access printers that you frequently administer quickly, create a folder on the desktop. Create shortcuts to the printers you use by dragging the printer icon from the printer folder or from Network Neighborhood to the folder you created on your desktop.

CHAPTER 6

Backing Up and Restoring Network Files

Regular backup of servers and local hard disks prevents data loss and damage caused by disk-drive failures, power outages, virus infection, and other potential network disasters. Backup operations based on careful planning and reliable equipment make file recovery a relatively painless process.

Windows NT includes the Backup program—a graphical tool that enables you to use a tape drive to back up and restore important files on either Windows NT file system (NTFS) or file allocation table (FAT) partitions. The Backup program also simplifies archiving. You can easily save data for legal or historical purposes and to remove older, unused files, safe in the knowledge that you can recover them if necessary.

The first section of this chapter, "Forming a Network Backup Plan," describes general strategies for setting up a tape backup system on your network. The remainder of the chapter describes how to use the Backup program to perform backup and restoration operations.

Additional data protection measures, such as fault tolerance and uninterruptible power supplies (UPS), are covered in Chapter 7, "Protecting Data," and in the *Windows NT Server Resource Kit* version 4.0.

Forming a Network Backup Plan

Network backup plans are most effective when they are based on both system needs and a strategy. As you formulate a tape-backup plan, you must consider the following questions:

- Which backup strategy is best suited to my environment?
- What hardware does the strategy require?
- What is the best location for a tape drive?

Strategic Considerations

Which of the following backup strategies is best suited to your environment? (If you are not sure, examine the advantages and disadvantages in the tables immediately following the list.)

- Server only or network backup. Do you plan to back up your entire network, with tapes drives attached only to certain servers where users copy their important files?
- Individual or local workstation backup. Will each workstation/user have a tape drive and be responsible for backing up his or her computer?
- Server and workstation backup. Will one individual be responsible for backing up computers for a group? (For example, will there be one tape drive for the accounting department and another for the legal department?)

Server-Only Backup

Advantages	Disadvantages
Fewer tape drives needed.	Registries and event logs of remote computers are not backed up.
Less media to manage because more backups are stored on tape.	Backups and restorations are slower due to network throughput limitations.
Depending on the size of your network, server-only backup can be less expensive than backing up each workstation individually.	Backups and restorations require greater planning and preparation. They must be scheduled when network traffic is at a minimum or when critical information can be backed up as quickly as possible.

Local Workstation Backup

Advantages	Disadvantages
Fewer network resources committed to a lengthy backup procedure	Using more tape drives is more expensive
Quicker file recovery.	

Server and workstation backup combines the advantages and disadvantages of server only and local workstation backups.

Hardware Considerations

The most common medium for backups and the one used by Windows NT Backup is magnetic tape. Tape is popular because it offers great capacity at low cost. The primary tape drive types used for backup include quarter-inch cartridge (QIC), digital audio tape (DAT), and 8-mm cassette. High-capacity, high-performance tape drives generally use small computer system interface (SCSI) controllers. For information about supported tape drives, see the Windows NT Server Hardware Compatibility List.

Tape technology changes rapidly, so it is best to research the relative merits of each type of medium before purchasing. When selecting a tape drive, consider drive and media cost, as well as reliability and capacity. Ideally, a tape drive should have more than enough capacity to back up your largest server. It should also provide error detection and correction during backup and restore operations.

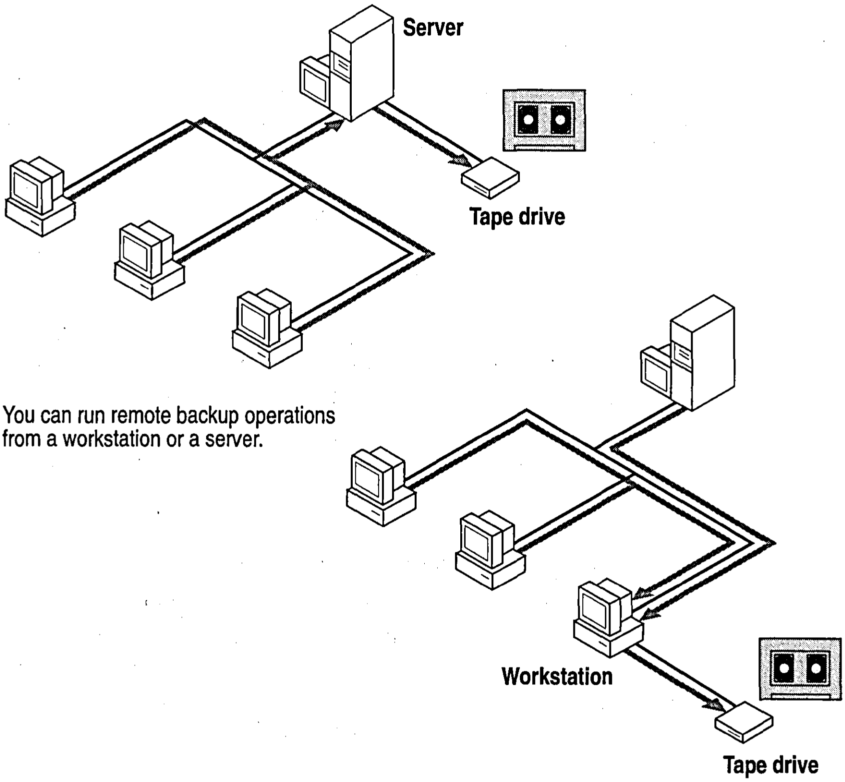
How Many Tape Drives Do You Need?

The number of drives you need depends on your overall backup strategy. Because tape cartridges are available in sizes greater than 5 gigabytes, you can probably back up your entire network with a few tapes and a single high-speed drive. However, the recent availability of less expensive tape drives makes individual workstation backups a sound option, too.

Location Considerations

You can cable your tape drive to either a workstation or to a server. There are advantages and disadvantages to either configuration:

- If you run backups from a server, you can back up and restore that server very quickly because your backups include the server's registry. On the other hand, if your network has more than one server, the speed advantage is lost.
- Servers typically operate 24 hours a day and are logical candidates to run backups during off hours. However, if a problem with backup hardware occurs, you might have to power down your server.
- As a general rule, though, if most of your information is on one server, you are better off running backups from that server.



You can run remote backup operations from a workstation or a server.

Whether you run remote backups from a workstation or a server, it makes sense to place a tape drive on the portion of your network with the greatest bandwidth (highest transmission frequency). You might also consider placing the tape drive in a secured room for data security.

Backing Up Disk Files to Tape

Because information is the most important resource on a computer or network, information backup and retrieval are an administrator's most critical functions. Plus, it is important to create backup policies and standard hardware-maintenance policies to avoid problems rather than just recover from them. You must consider the following questions when developing such policies:

- Which backup procedure is most appropriate?
- How often should backup occur?
- Where is the best place to store tapes?

The answers will determine the steps you take to protect critical data. Such steps can range from a simple backup done with the Windows NT Backup program to the use of disk fault-tolerance methods. Then decide how often you need to repeat a complete risk assessment. You will need to evaluate the continuing importance of various operations and determine likely new areas of exposure.

Note The Windows NT Server Disk Administrator program provides fault-tolerance functionality for creating mirror sets and stripe sets with parity. For more information about Disk Administrator, see Chapter 7, "Protecting Data."

Types of Backup

There are five types of backup: *normal*, *copy*, *incremental*, *differential*, and *daily*. The most common types are normal (full), incremental, and differential.

- A normal backup copies all selected files and marks each as having been backed up. With normal backups, you can restore files quickly because files on the last tape are the most current.
- A copy backup copies all selected files but does not mark each file as having been backed up. Copying is useful if you want to backup files between normal and incremental backups because copying does not invalidate these other backup operations.
- An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up. If you use a combination of normal and incremental backups, restoring requires starting with your last normal backup and then working through all the incremental tapes.
- A differential backup copies those files created or changed since the last normal (or incremental) backup. It does not mark files as having been backed up. If you are doing normal and differential backups, restoring requires only the last normal and last differential backup tape.
- A daily backup copies all selected files that have been modified the day the daily backup is performed. The backed up files are not marked as having been backed up. (This can be useful if you want to take work home and need a quick way to select the files that you worked on that day.)

The following table lists advantages and disadvantages associated with running the most common types of backup.

Backup type	Advantages	Disadvantages
Normal	Files are easy to find because they are always on a current backup of your system or on one tape or tape set.	Most time-consuming.
	Recovery requires only one tape or tape set.	If files do not change frequently, backups are redundant.
Incremental	Least data storage space required.	Files difficult to find because they can be on several tapes.
	Least time-consuming.	
Differential	Less time-consuming than normal backups.	Recovery takes longer than if files were on single tape.
	Recovery requires only the last normal backup tape and last differential tape.	If large amounts of data change daily, backups can be more time consuming than incremental.

Note Perform regular backups when the fewest people are using the network. If many files are in use, the backup might not accurately reflect your network.

How Often to Back Up

Although it is best to have three copies of important data to protect against tape failure or loss, the *frequency* with which you create these back ups depends on how often your data changes and on its value to you. Backups can consist of a weekly, a monthly, and an archive backup. The archive tape can be a simple copy rather than a complete backup.

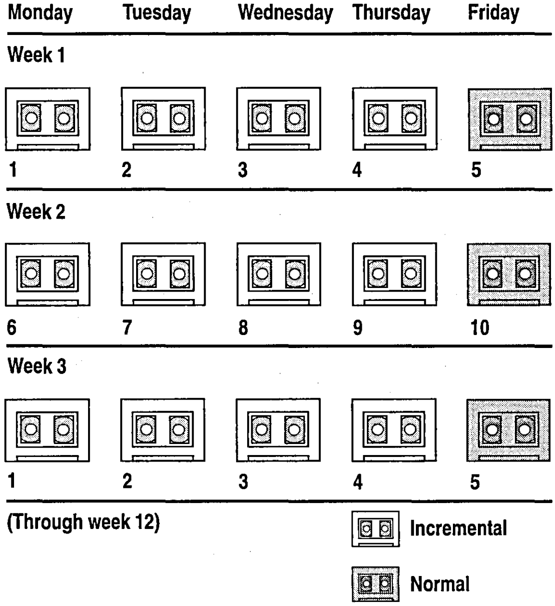
Note Backups are also a protection against virus contamination. Because some viruses take weeks to appear, keep normal backup tapes for a month or more to ensure that you can restore a system to its preinfection status.

Alternating Tapes

By alternating backup tapes you lower the backup cost. The following sections describe a 12-week and a one-year sample tape-alternation schedule. The life cycle of a tape depends on the manufacturer and storage conditions.

Backing Up Over 12 Weeks

The 12-week schedule uses a different backup tape each day for two weeks, and then the first tape is used again at the beginning of each third week. Incremental backups are performed Monday through Thursday after an initial normal backup. Normal backups are performed on Fridays with the most recent normal backup stored on-site. The normal backup of the preceding week is stored off-site. At the end of the 12 weeks, the cycle starts over with a new set of tapes.

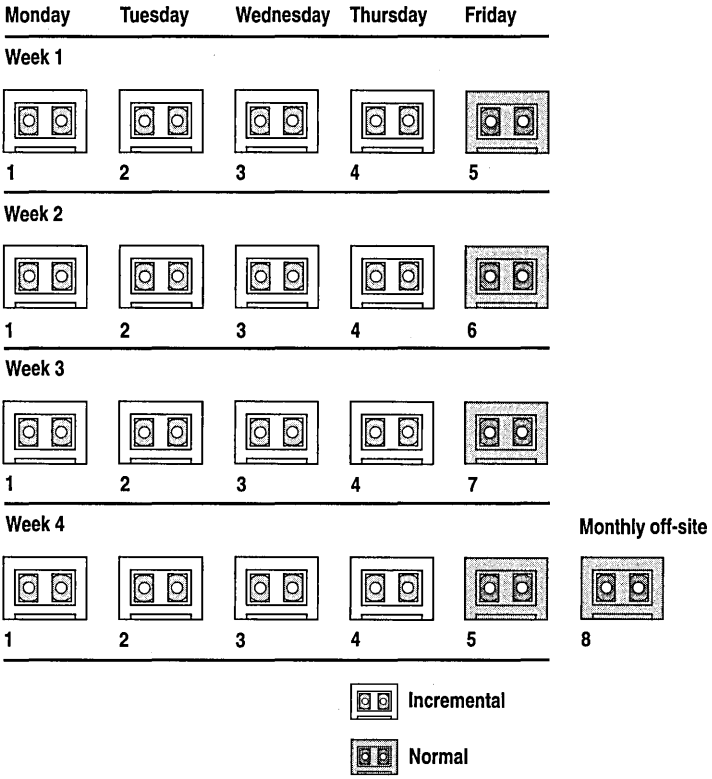


On Friday morning transfer tape 5 off-site

On Friday morning tape 10 is transferred off-site and tape 5 is returned to be used for the week's normal backup

Backing Up Over One Year

One popular tape-alternation schedule uses 19 tapes over the course of one year Four tapes are used Monday through Thursday for incremental (or differential) backups, and three tapes are used for weekly normal backups (performed each Friday). The remaining 12 tapes are used for monthly normal backups and are stored off-site.



Verifying Backups

A *verify operation* compares files on disk to files that have been written to tape. It occurs after all files are backed up or restored and takes about as long as the backup procedure itself. It is a good idea to perform a verify operation after every backup. If you are backing up to a set of tapes that will be stored for a long time, it is wise to verify them. Verifying after file recovery is also recommended.

Note If a verify procedure fails for a given file, check to see when that file was last modified. If someone changes a file between a backup and verify operation, the verify procedure fails.

Storing Backup Tapes

You must find an off-site location for storage of backup and archive tapes. The location can be a vault or other place that can protect the tapes from fire, water, theft, and other hazards. If you use a fireproof safe, make sure it is specifically designed to protect magnetic media.

Tapes last longer in cool, humidity-controlled locations. Your storage area should also be free of magnetic fields, such as those found near the backs of computer terminals and analog telephones.

Documenting Backup Operations

Accurate backup records are essential to finding missing information quickly, particularly if you have accumulated large numbers of high-volume tapes. Records can include tape labels which should be accompanied by a log book, catalogs, and log files.

Tape Labels

Tape labels should contain a date, the type of backup (normal, incremental, or differential), and complete information regarding tape contents. Indicating the type of backup is important. If you are restoring from differential or incremental backup tapes, you need to locate the last normal backup tape and either the last differential tape or all incremental tapes created since the last normal backup. Alternatively, you can label tapes sequentially and keep a log book of tape contents.

Catalogs

Most backup software include a mechanism for cataloging backup files. Windows NT Backup stores backup catalogs on tape, temporarily loading them into memory during program sessions. Catalogs are created for each *backup set* (a collection of files from one drive that is backed up). Catalogs cannot be printed or saved to disk.

Log Files

In addition to an online catalog, all operation information can be logged to a file. The log file can include the names of all files and directories successfully backed up and restored. For information about how to log backup operations, see “Setting the Log Options” in Backup Help.

Using Windows NT Backup

The Windows NT Backup program is located in the Administrative Tools folder.

The following list describes how you can use the Backup program to protect data:

- Back up and restore both local and remote files on an NTFS or a FAT partition from your own computer using an attached tape drive.
- Select files for backing up or restoring by volume, directory, or individual file name, and view detailed file information, such as size or modification date.
- Select the verification pass option to ensure reliable backups or restorations.
- Perform any of the following common types of backup operations: normal, copy, incremental, differential, and daily.
- Place multiple backup sets on a tape, and either append new backup sets or overwrite the whole tape with the new ones.
- Span multiple tapes with both backup sets and files because there is no file-size restriction.
- Create a batch file to automate repeated backups of drives.
- Review a full catalog of backup sets and individual file and directory information so you can select files to be restored.
- Control a restore operation's destination drive and directory.
- Save log information about tape operations to a file. Also view tape-operation information in Event Viewer.

Selecting Hardware

The system automatically checks for a tape drive when you start Windows NT and initializes the hardware each time you start Backup. The tape drive must be cabled to the computer where the program is run. Notice, however, that to ensure the drivers load properly, the tape drive must be turned on before you start Windows NT. If you have more than one tape backup device, use the **Hardware Setup** command from the **Operations** menu to select a different device.

Note If you do not have a tape drive, you can use the **backup** or **xcopy** commands to back up files to a floppy disk.

Windows NT currently supports both high-capacity SCSI tape backup devices for 4 mm DAT, 8 mm, and .25-inch drives and the less expensive mini-cartridge drives. You can have more than one tape drive cabled to your system. However, only one tape drive can be selected at a time. For more information about supported tape drives, see the Windows NT Server Hardware Compatibility List.

Inserting a higher-density tape than the tape drive is capable of using can cause the program to display "Tape Drive Error Detected" and prevent the tape from being ejected until you close Backup.

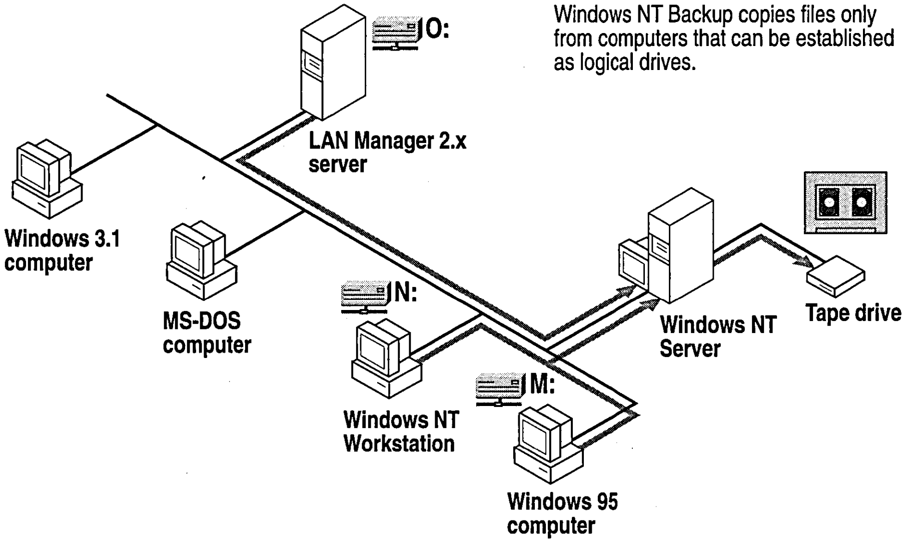
Note Only programs that support the Microsoft tape format can create Windows NT-compatible tapes.

Backing Up Other Operating Systems

You can use the Backup program to back up any computers to which you can connect remotely. Windows NT Backup does not recognize MS-DOS or Windows 3.1 workstations.

Note Windows NT Backup cannot back up Registries or event log files on remote computers.

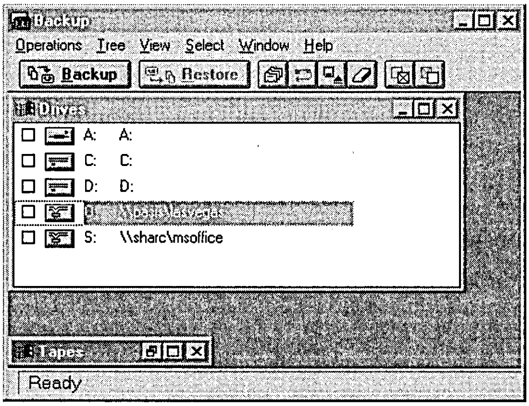
Before running the program, each computer you want to back up must be established as a logical drive (D, E, F, and so on) on the computer that the tape drive is connected to. Typically, you would incorporate logical drive connections into the batch file you use to run your backups.



Windows NT Backup copies files only from computers that can be established as logical drives.

Backup Menu Commands

Click the Backup folder in the Administrative Tools (Common) folder to display the main Backup window with the Drives window open and a minimized Tapes window. (You can also type **ntbackup** or **start ntbackup** at the command prompt.)



Each time you start Backup, the program scans for and detects new or additional tape drives. If a new drive is detected, you are prompted to use the Tape Devices option in Control Panel to install the driver.

For information about how to load a tape driver, see "Loading a Tape Driver" in Help.

The following most commonly used commands from the **Operations** and **Select** menus are also available on the toolbar.

Backup
Restore
Catalog

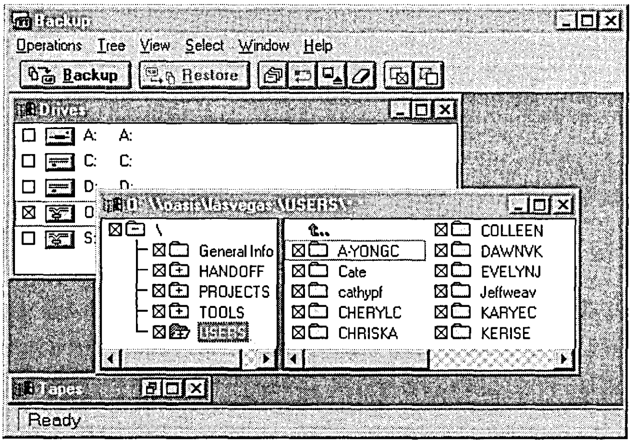
Retention Tape
Eject Tape
Erase Tape

Check
Unchecked

The **Tree**, **View**, and **Window** menus provide commands for manipulating your windows the same as in the Windows NT Explorer. The **View** menu also enables you to display or hide the status bar and toolbar and to change your font selection. For more information about **Backup** menu commands, see Backup Help .

Choosing Files to Back Up

You can specify which files to back up. To specify all files, click the **Check** button on the toolbar. To select individual files, select the check box for each file name.



The Drives window is normally open when you start the Backup program.

If you connect to another network drive while using Backup, choose **Refresh** from the **Window** menu to update the Drives window and view the additional network drive.

For information about how to select files to backup, see "Backing up all the Files" or "Backing up Individual Files" in Help.

Note When a disk drive is selected, the program will not back up those files and directories that the user does not have security permission to read. Hidden files with read permission will be backed up and are displayed with an exclamation point in the file's icon. During Backup, all file attributes, including permissions, are preserved.

Files That Are Not Backed Up

Windows NT Backup does not indiscriminately backup and restore all files. Instead, it follows rules that protect system security and data integrity.

The following file types are not automatically backed up when you run Windows NT Backup:

- Files you do not have permission to read. Only persons with backup rights can copy files they do not own.
- Paging files. (These are temporary files used to represent virtual address space.)

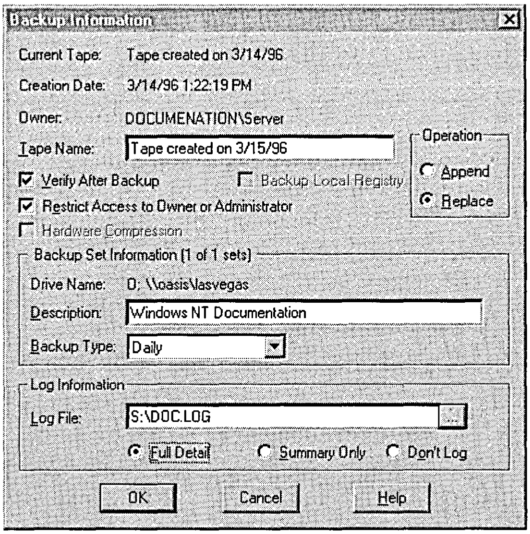
- Registries on remote computers. Windows NT backs up only the local registry.
- Files exclusively locked by application software. Windows NT Backup cannot copy files locked by application software. However, it supports backup of all files that are part of the operating system. Windows NT locks two types of files: event logs and registry files.

If Windows NT Backup encounters a file that is open in share/read mode, it backs up the last saved version of the file.

For information about backing up registries on remote computers, see the *Windows NT Workstation Resource Kit* version 4.0.

Setting Tape Options

After selecting one or more disk drives or files to back up, click the **Backup** button to open the **Backup Information** dialog box. The upper section provides information about the tape that you loaded and enables you to specify backup options. The lower section displays information about the *backup set* and enables you to create a log file of the backup.



Backup Information

Current Tape: Tape created on 3/14/96

Creation Date: 3/14/96 1:22:19 PM

Owner: DOCUMENATION\Server

Tape Name: Tape created on 3/15/96

☑ Verify After Backup □ Backup Local Registry

☑ Restrict Access to Owner or Administrator

□ Hardware Compression

Operation

○ Append

● Replace

Backup Set Information (1 of 1 sets)

Drive Name: D: \\oasis\lasvegas

Description: Windows NT Documentation

Backup Type: Daily

Log Information

Log File: S:\DOC.LOG

● Full Detail ○ Summary Only ○ Don't Log

The following table describes the options in the upper section of the Backup Information dialog box. For more information about the lower section of the dialog box, see the sections that follow the table.

Item	Description
Current Tape	The current tape's name is shown here unless there is no tape loaded, it is blank, or it has an unrecognized format.
Creation Date	The creation date of the original backup set or the date when it was last replaced is automatically displayed here.
Owner	The owner of the tape, that is, whoever put the first backup set on the tape, is automatically displayed here.
Tape Name	You can use up to 32 characters to create or change a current tape name.
Append	This operation adds the backup sets to the end of the last backup set on the active tape. Tape Name and Restrict Access To Owner Or Administrator are unavailable with this operation.
Replace	This operation overwrites all the information on the tape. However, if you do not confirm the choice, another message gives you the option of appending instead.
Verify After Backup	You can specify whether or not to perform a verification comparison of the files that are written to tape and the files on the disks.
Restrict Access To Owner Or Administrator	You can designate the tape as "secure." Only the tape owner or a member of the Administrators or Backup Operators group can read, write, or erase the tape using the Windows NT Backup program. To restore it on another computer in the same domain, you must be logged on with the same user account name for that domain. Members of the Administrators or Backup Operators group can read, write, or erase a tape on any computer and in any domain.
Hardware Compression[1]	You can request that the tape drive compress the data onto the tape media. However, do not select this option if you want to move this tape later to another tape drive that does not support hardware compression. This option is available only if the tape drive supports selectable hardware compression.
Backup Local Registry	You can include a copy of the local Windows NT Registry files in the backup set. This option is available only if the drive containing the registry is selected. Windows NT Backup does not back up configuration information or event logs located on remote computers.

[1] Keep in mind, however, that moving tapes between different brands of tape drives can cause problems if one brand supports compression and the other one does not. Depending on the tape drive, the program could display messages such as "Tape Drive Error Detected," "Tape Drive Not Responding," or "Bad Tape." To erase a tape that is causing one of these problems, start Windows NT Backup from the command prompt with the **/nopoll** parameter. However, be careful not to use Backup with the **/nopoll** parameter to perform anything other than erasing the tape.

Granting Backup and Restore Privileges

In Windows NT, file access is limited by NTFS file permissions (No Access, List, Read, Add, Add and Read, Change, Full Control, Special Directory Access, Special File Access), share permissions (No Access, Read, Change, Full Control), and file attributes (Read Only, Hidden, System). FAT does not provide file permissions.

However, the permissions and attributes can be overridden if you are granted certain user rights in User Manager for Domains. Two of the user rights, **Backup files and directories** and **Restore files and directories,** are used by the Backup program to enable you to backup or restore regardless of the permissions or attributes set on the files.

If the rights are not granted, you cannot backup or restore files and directories that you do not have access to unless you are a member of the Administrators or Backup Operators group. The Administrators and Backup Operators groups are granted these rights by default.

Backup and restore rights are independent of each other. However, it is recommended that backup rights be granted along with the restore rights. Use caution in granting restore rights because normal file-permission conflicts are ignored during restoration and existing files can be overwritten.

Reserve backup and/or restore rights for those few individuals who have regular responsibility for backing up your network. Large sites might want to create two groups of backup operators:one with only backup rights; the other with backup and restore rights.

For more information about user rights and groups, see Chapter 2, "Working with User and Group Accounts."

Setting the Backup Set Information

The second section of the **Backup Information** dialog box shows how many backup sets have been selected. If you select multiple disk drives, Backup provides a scroll bar for moving between backup sets so that you can enter separate descriptions (up to a length of 32 characters) and select different backup types for each.

When deciding which backup type to use, one of the criteria should be whether or not it will mark the files as having been backed up. Windows NT maintains a marker (called the *archive bit*) for each file that allows backup programs to mark the files after backing them up. When the file changes, Windows NT marks the file as needing to be backed up again.

With Windows NT Backup, you choose to back up only those files that have this marker set, and you choose whether or not to mark files as having been backed up.

- The normal (or full) backup type is best when a large amount of data changes between backups or to provide a baseline for the other backup types.
- The incremental backup type is good if you need to record the progression of frequently changed data. The differential backup type simplifies the process for restoring files.
- To provide for long-term storage with fewer tapes, you can use a combination of a normal backup plus either incremental or differential backups.

For more information about types of backup, see the "Types of Backup" section earlier in this chapter.

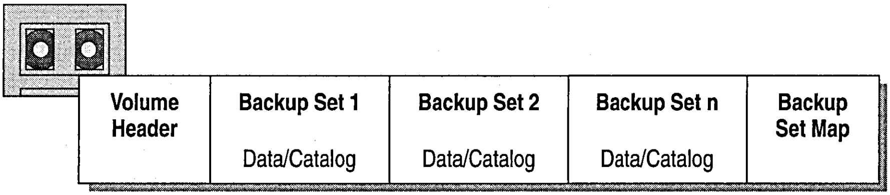
Setting Log Options for Backup and Restore

In the bottom section of the **Backup Information** and the **Restore Information** dialog boxes, you can specify not to log information or to create a log that contains either a summary of major operations or full details on all operations.

Select	To
Full Detail	Log all operations information including the names of all files and directories that are backed up.
Summary Only	Log only major operations such as loading a tape, starting the backup, and failing to open a file.
Don't Log	Log no information.

How Windows NT Backup Keeps Track of Files

Each tape used for backup can consist of several backup sessions or sets. At the end of each backup set, Windows NT Backup stores a summary of file and/or directory information in a backup set *catalog*. At the end of each tape is a *backup set map* that maintains the exact tape location of the backup set's data and catalog. This information is temporarily cached from tape to disk when you run the Backup program.



Windows NT Backup Command Prompt Parameters

Backup operations can also be performed at the command prompt using the **ntbackup** command. Most of the command's parameters do not require user input and can therefore be implemented in batch files. However, a few of the parameters require user input.

The following parameters require user input:

Syntax

ntbackup [/nopoll] [/missingtape]

/nopoll
Specifies that the tape should be erased.

Caution Do not use **/nopoll** with any other parameters.

/missingtape
Specifies that a tape is missing from the backup set when the set spans several tapes. Each tape becomes a single unit as opposed to being part of the set. For more information about the **missingtape** parameter, see "Building Partial Tape and Backup Set Catalogs" later in this chapter.

You can create a batch file to back up one or more drives regularly. However, using batch files enables you to back up directories only (not individual files). Also, wildcard characters cannot be used in the batch files.

The following parameters do not require user input and are useful in batch files.

Syntax

ntbackup *operation path* **[/a][/v][/r][/d** "*text*"**][/b][/hc:**{**on** | **off**}]
[**/t** {*option*}][**/l** "*filename*"][**/e**][**/tape:**{*n*}]

Parameters

operation
Specifies the operation, **backup** or **eject**.

Note Each of the following parameters, with the exception of **/tape** must be used only with the **backup** operation parameter.

path
Specifies one or more paths of the directories to be backed up.

/a

Causes backup sets to be added or appended after the last backup set on the tape. When **/a** is not specified, the program overwrites previous data. When more than one drive is specified but **/a** is not, the program overwrites the contents of the tape with the information from the first drive selected and then appends the backup sets for the remaining drives.

/v
Verifies the operation.

/r
Restricts access. The **/r** parameter is ignored if **/a** is also specified.

/d "*text*"
Specifies a description of the backup contents.

/b
Specifies that the local registry be backed up.

/hc:on or **/hc:off**
Specifies that hardware compression is on or off.

/t {*option*}
Specifies the backup type. *Option* can be one of the following:

normal	copy
incremental	differential
daily	

For more information about the types of backup, see "Types of Backup" earlier in this chapter.

/l "*filename*"
Specifies the file name for the backup log.

/e
Specifies that the backup log include exceptions only.

/tape:{*n*}
Specifies the tape drive to which the files should be backed up. *N* is a number from 0 to 9 that corresponds to the number the drive was assigned when the tape drive was installed.

Examples Using Backup from the Command Prompt

When the append (**/a**) parameter is not specified in a backup batch file, the Backup program overwrites the tape contents. Specifying append causes backup sets to be added after the last backup set on the tape. When more than one drive is specified in the batch file and the append parameter is not, the program overwrites the contents of the tape with the information from the first drive selected and then appends the backup sets for the remaining drives.

Three of the following examples show how to implement the append (**\a**) parameter.

Example 1

This example shows you how to perform the following activities:

- Perform a normal backup of drives C, D, and E.
- Restrict access to the owner or administrator.
- Apply the description "Full Backup of drives C, D, and E" to all three backup sets.
- Perform a verification pass upon completion of the backup.
- Record the results of the session in the log file named C:\LOG\LOG.TXT.

To do this, type the following at the command prompt:

```
NTBackup Backup C: D: E: /t Normal /v /r /d "Full Backup of drives C, D,
and E" /l "C:\LOG\LOG.TXT"
```

Example 2

This example shows you how to perform the following activities:

- Perform a copy backup of the files in C:\EXCEL\PERSONAL.
- Do not restrict access.
- Use the description "Copy of Personal Excel Directory."
- Perform a verification pass upon completion of the backup.
- Record the results of the session in the log file named C:\LOG.TXT.
- Write the backup to tape drive number 1, which is the second tape drive.

To do this, type the following at the command prompt:

```
NTBackup Backup C:\EXCEL\PERSONAL /t Copy /v /d "Copy of Personal Excel
Directory" /l "C:\LOG.TXT" /tape:1
```

Example 3

This example shows you how to perform the following activities:

- Perform an incremental-type backup of drives C, D, E, and the registry.
- Have the tape drive compress the data on the tape.
- Apply the description "Compressed Incremental Backup of drives C, D, and E including Registry."
- Perform a verification pass upon completion of the backup.
- Record the results of the session in the log file named C:\WEEKLY.LOG.

To do this, type the following at the command prompt:

```
NTBackup Backup C: D: E: /t Incremental /b /hc:on /v /d "Compressed
Incremental Backup of drives C, D, and E    including Registry" /l
"C:\WEEKLY.LOG"
```

Example 4

This example shows you how to eject a tape from drive one.

To do this, type the following at the command prompt:

```
NTBackup Eject /tape:1
```

Maintaining Tapes

The Windows NT Backup program provides three commands on the **Operations** menu to help you maintain your backup tapes: **Erase Tape**, **Retension Tape**, and **Format Tape**.

Erase Tape

The **Erase Tape** command erases the entire tape. A warning message in the **Erase Tape** dialog box advises that all information on the tape will be destroyed. It also provides the name of the tape and its date of creation.

You can do either a Quick Erase (rewrite the tape header) or a Secure Erase (overwrite the entire tape). A Secure Erase can take several hours to complete, depending on the drive technology and tape length. Categorize the information on the backup tapes by which method of erasing to use, and then create and maintain a list for easy reference.

Retension Tape

The **Retension Tape** command eliminates loose spots on the tape by fast forwarding to the end of the tape and then rewinding. This procedure winds the tape evenly so it will run more smoothly past the tape drive heads.

To reduce tape slippage, manufacturers of tape backup drives recommend that you retension .25-inch tape once every 20 uses. Note that 4 mm and 8 mm tapes do not require retensioning, and so the command is unavailable. The time required to forward and rewind media depends on the device technology. For specific retensioning requirements, see the manufacturer's documentation.

Format Tape

The **Format Tape** command formats an unformatted minicartridge tape. This type of tape must be formatted before it can be used. If you do not have a minicartridge drive installed and activated, this command is unavailable.

Restoring Tape Files to Disk

Backed-up information is useless if it cannot be restored. Windows NT provides a **Restore** command to give access to tapes, backup sets, and files for restoring as they are needed.

Restoration policies for everyday maintenance, not to mention for emergency recovery, are as important as backup policies. Practice ahead of time on spare drives, though, so you do not risk overwriting real data. You should also periodically do trial restorations to check whether files have been backed up properly. Such trials check for possible hardware problems that do not show up with the software or whose symptoms are not easily recognized. For that reason, keep a backup status log, and check it regularly for error messages.

When restoring a large number of files, you should consider what backup you used. If you did differential or incremental backups, first restore the selected files from the most recent normal backup, then files from all subsequent incremental backups of those files, and finally the most recent differential backup performed after the last incremental backup.

For tape-management purposes, the following information is associated with each tape:

- A user-specified tape name
- An original tape-creation date plus the date and time that each backup set was created
- The computer name and the user name of the user who created the tape
- A tape-sequence number in the case of tape sets

Choosing What You Want to Restore

You can restore the current tape, one or more backup sets, or individual files. Open the Tapes window and make your selections the same way you would for backing up.

All catalog information is maintained on the corresponding tape for that backup set. Family sets have the information on the last tape.

The tape name appears in the left panel of the Tapes window to the right of each tape icon. The following information is shown in the right panel of the Tapes window:

- Drive backed up
- Backup set number
- Tape number and what number it is in a set of tapes

- Backup type
- Date and time of backup
- Backup description

When you insert a tape to restore information, only information about the first backup set is displayed in the right panel until you load the tape's catalog. To restore the entire tape, you must load the tape's catalog first to display a complete list of other backup sets on the tape. Otherwise, when you select an entire tape, you are really selecting only those sets that are already displayed. To know which files are in each backup set, you must load the individual catalogs for each backup set.

For information about how to load a catalog of the backup sets, restore tapes or backup sets, and restore individual files see "Loading Catalogs," "Restoring Tapes or Backup Sets," and "Restoring Individual Files" in Backup Help.

Files That Are Not Automatically Restored

Windows NT Backup restores all files except the following:

- Tape files that are older than a disk file. If a file being restored already exists on disk, and the disk file is newer than the tape file, the Backup program asks you to confirm replacement.
- A file to be restored into a directory for which you do not have access. Likewise, if you do not have write access to a file, you cannot restore over it. These conditions do not apply if you have restore rights.

Building Partial Tape and Backup Set Catalogs

If a backup operation spans several tapes and you choose to restore a single backup set, you are prompted to insert the last tape to load the tape catalog information and receive a complete list of all the backup sets and their locations. However, if the last tape in such a family set is missing or damaged, you can force Backup to deal with the data on each remaining tape as if it were a single unit rather than a member of a family set. To do so, start Backup from the command prompt with the **/missingtape** parameter. However, this process will take additional time.

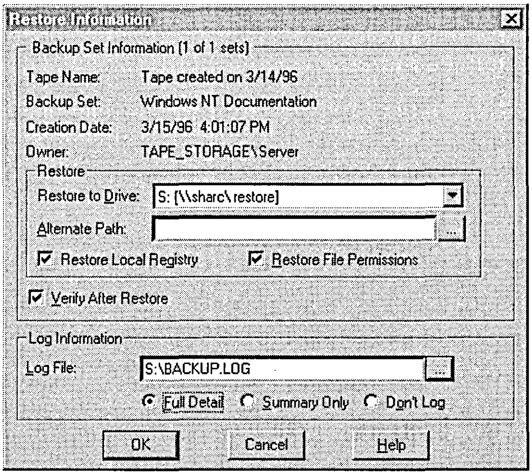
For information about how to build catalogs from a partial tape set, see "Building Partial Tape and Backup Set Catalogs" in Backup Help.

Restoring Files from Third-Party Backup Programs

At times you might want to restore from a tape with files that were not backed up with the Windows NT Backup program. If the tape is in the Microsoft tape format (MTF), Windows NT Backup can read it. However, be aware that the tape might not have the full on-tape catalog (OTC) information that Windows NT Backup produces. Also, some older tape backup devices may not support creating full on-tape catalogs with the Windows NT Backup program.

Setting Restore Options

After selecting one or more tapes, backup sets, or files to restore, choose the **Restore** command from the **Operations** menu to open the **Restore Information** dialog box. The first section provides information about the backup sets on the loaded tape and indicates the number of tapes in that family set. For each backup set, you must specify the drive to which you want the information restored.



Restore Information

Backup Set Information (1 of 1 sets)

Tape Name: Tape created on 3/14/96

Backup Set: Windows NT Documentation

Creation Date: 3/15/96 4:01:07 PM

Owner: TAPE_STORAGE\Server

Restore

Restore to Drive: S: [\\sharc\restore]

Alternate Path:

☑ Restore Local Registry ☑ Restore File Permissions

☑ Verify After Restore

Log Information

Log File: S:\BACKUP.LOG

● Full Detail ○ Summary Only ○ Don't Log

You can also specify an alternate directory path to place a backup set's files into a different directory instead of into the original one on the default drive. This might be done to compare them to the files on the disk. The **Browse** button at the end of the **Alternate Path** box can help you find the correct path.

To compare the contents of the restored files against the files on tape and log any exceptions, select the **Verify After Restore** check box.

When you select the **Restore File Permissions** check box, the system restores the permissions information along with the file if the files are being restored to an NTFS partition. Otherwise, the files inherit the permissions information of the directory into which they are restored.

To restore Registry files, select the **Restore Local Registry** check box. However, you will need to restart the computer for the restored information to take effect.

File permissions (or security settings), such as ownership or access permissions, can be restored only when the restored files were backed up from an NTFS volume and restored to an NTFS volume. However, you should restore file access permissions only if you are restoring files to computers in the same domain as that of the original owner's account. For example, you could restore files to other computers in a domain if the original permissions on the files allowed access to a user account in that domain.

Note Do not restore file permissions in the following situations:

- If you are using the backup tape to transfer files to another computer outside the original domain.
- If you are restoring files to a computer that has not been completely restored following the corruption of the operating system.

Restoring the Local Registry

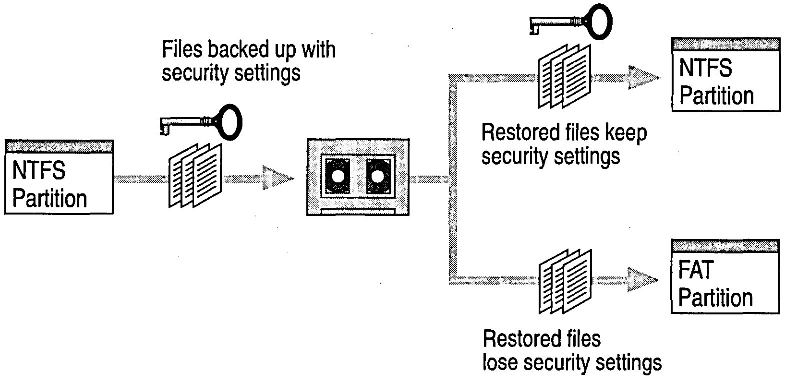
Be aware of these steps before you try to restore the registry:

- After restoring the registry, you must restart your computer, which means you lose any configuration changes made since the last Registry backup.
- To restore a registry onto a new computer (if, for example, your hard drive breaks), you must first reinstall Windows NT on the new computer and then restore a full backup tape of your hard drive.

For more information about the registry, see Appendix A, "Windows NT Registry," or the *Windows NT Resource Kit* version 4.0.

Restoring File Security Settings

Windows NT files may have permissions, ownership, and audit flags associated with them. Windows NT Backup preserves this information on files restored to NTFS partitions but not on files restored to FAT partitions. It is not possible to secure information on FAT file systems.


Files backed up with security settings
NTFS Partition
Restored files keep security settings
NTFS Partition
FAT Partition
Restored files lose security settings

When you restore files to a new computer (a new hard drive), you do not have to restore security information. (The files inherit the permissions of the directory in which they are placed.) If the directory has no permissions, the file retains its previous permissions, including ownership.

Backup Example

The following example illustrates how to backup a small network comprised of clients running different operating systems.

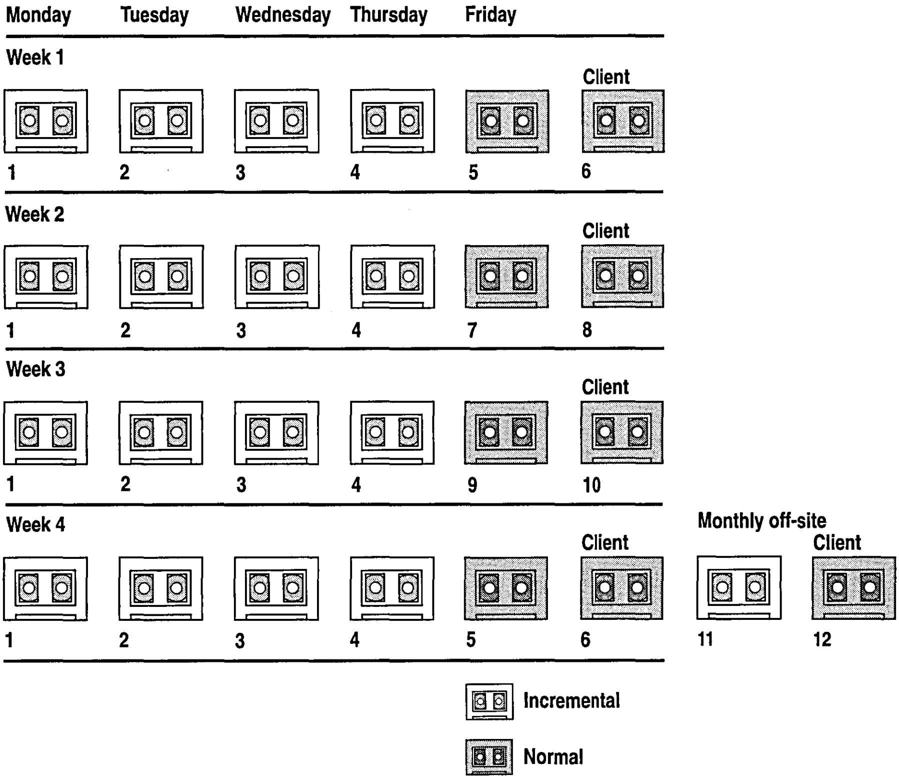
Setting Up a Backup Program for a Small Network

Suppose you need to back up a Windows NT Server computer and 20 client computers. The clients are a mix of computers running MS-DOS, Windows for Workgroups, Windows 95, and Windows NT. You plan to purchase one tape drive and controller card and use Windows NT Backup.

You can work out a solution by following four steps:

1. Research and select a tape drive based on reliability, speed, capacity, cost, and Windows NT compatibility. The drive should support tape cartridges with more than enough space to back up your entire server.
2. Locate your tape drive at the server so that you can back up the server registry and so that server backups take place as quickly as possible. From the server, you can back up user files on remote computers running only Windows for Workgroups, Windows 95, and Windows NT.

3. Install the tape controller card in the server, and attach the tape drive. Be sure that the tape drive is turned on before powering up the server; otherwise, the SCSI tape driver will not be loaded properly.
4. Specify a tape alteration schedule that includes backing up computers running Windows for Workgroups, Windows 95, and Windows NT Workstation. To conserve tapes, back up client computers less frequently than your server and, space permitting, encourage users to copy extremely important files to the server at the end of the day. The following illustration shows a possible rotation schedule.



Because Windows NT Backup does not back up files on MS-DOS computers, consider reserving some space on the server where MS-DOS and Windows 3.1 users can copy important files. These files would be backed up during regular server backups.

CHAPTER 7

Protecting Data

Windows NT Server provides several tools for managing disk resources to enhance performance and protect data. The tools include the Disk Administrator and Backup programs which are in the Administrative Tools (Common) folder, as well as the uninterruptible power supply (UPS) option in Control Panel. Only Disk Administrator and UPS are discussed in this chapter. For more information about Backup, see Chapter 6, "Backing Up and Restoring Network Files."

The tools discussed in this chapter provide data protection if one of the following occurs:

- Disk failures using fault tolerance, redundancy, and the **chkdsk** program.
- Power outages using the UPS option to configure uninterruptible power supplies
- Corrupted or missing system or boot files using the **Last Known Good Configuration** option.

This chapter also includes information about using Disk Administrator to set up and organize your hard disks to function more efficiently. The fault-tolerant options in Disk Administrator enable you to take advantage of Redundant Array of Inexpensive Disks (RAID) data management, mirror sets, stripe sets, and stripe sets with parity.

Disk Administrator Overview

Disk Administrator is a graphical tool for managing disks. Disk Administrator encompasses and extends the functionality of character-based disk management tools, such as MS-DOS Fdisk and the Microsoft LAN Manager Fault Tolerance character applications.

The following list provides an overview of what you can do with Disk Administrator:

- Create and delete partitions on a hard disk.
- Create and delete logical drives within an extended partition.
- Format and label volumes.
- Read status information about disks, such as the partition sizes and the amount of free space that is available for creating additional partitions.
- Read status information about Windows NT volumes, such as the drive-letter assignment, volume label, file system type, size, and available space.
- Make and change drive-letter assignments for hard disk volumes and CD-ROM devices.
- Create and delete volume sets.
- Extend volumes and volume sets.
- Create and delete stripe sets with or without parity.
- Regenerate a missing or failed member of a stripe set with parity.
- Establish or break disk-mirror sets.
- Save and restore disk configuration.

Note You cannot use Disk Administrator to further partition the *system* or the *boot partition* because it contains files required to operate Windows NT. Disk Administrator can be used to partition free space on an existing disk or to partition new disks only. For more information, see "Partitioning Disks" later in this chapter.

The Windows NT Server version of Disk Administrator includes the common disk organizational tools (volume sets and stripe sets) and then adds the data-protection (fault tolerance) tools (mirror sets and stripe sets with parity). For more information about fault tolerance, mirror sets, and stripe sets with parity, see "Fault Tolerance" later in this chapter.

Disk and File Terms

A *partition* is a portion of a physical disk that functions as though it were a physically separate unit. A partition is usually referred to as either a primary or an extended partition.

A *primary partition* is a portion of a physical disk that can be marked for use by an operating system. A disk can have up to four primary partitions (or up to three, if there is an extended partition) per physical disk. A primary partition cannot be subpartitioned

An *extended partition* is created from free space on a hard disk and can be subpartitioned into logical drives. Only one of the four partitions allowed per physical disk can be an extended partition, and no primary partition needs to be present to create an extended partition.

Free space is an unused and unformatted portion of a hard disk that can be partitioned or subpartitioned. Free space within an extended partition is available for the creation of logical drives. Free space within extended partitions on several disks can also be used to create volume sets or other kinds of volumes for fault tolerance purposes. Free space that is not within an extended partition is available for the creation of a partition with a maximum of four partitions allowed.

A *volume* is a partition or collection of partitions that have been formatted for use by a file system. A Windows NT volume can be assigned a drive letter and used to organize directories and files.

A *volume set* is a combination of partitions that appear as one logical drive.

A *stripe set* is saving data across identical partitions on different drives. A stripe set is not fault tolerant.

Fault tolerance ensures data integrity when hardware failures occur. In Windows NT, fault tolerance is provided by the FTDISK.SYS driver.

A *mirror set* is a fully redundant or shadow copy of data.

The system partition contains the hardware-specific files (Ntldr, Osloader.exe, Boot.ini, Ntdetect.com) needed to load Windows NT.

The boot partition contains Windows NT operating system files which are located in the *%Systemroot%* and *%Systemroot%*\System32 directory.

Managing Disks

If you use only the Windows NT operating system, you can create one partition that occupies your entire disk or as many as four partitions. If you want to use other operating systems on your hard disk (such as UNIX or MS-DOS) with file systems that are not recognized by Windows NT, you must create separate partitions for each non-Microsoft operating system. Notice, though, that MS-DOS and Windows NT can share the same partition when using the file allocation table (FAT) file system.

On an *x*86-based computer, the operating system starts from the active system partition on the first internal hard disk (that is, Disk 0). Computers using reduced instruction set computing (RISC) processors can have several system partitions that are configurable by the manufacturer's configuration program. Such partitions must be formatted for the file allocation table (FAT) file system.
For detailed information about setting up more than one system partition on a RISC-based computer, see your hardware documentation.

Note Disk Administrator cannot be used to partition a disk that contains Windows NT system files. Disk Administrator can be used to partition free space on an existing disk or to partition new disks only.

Partitioning Disks

Disk management under Windows NT is very flexible. You can create up to four partitions in the free space on a physical hard disk, create multiple logical drives in the free space of an extended partition, and delete partitions. You can also add hard disks to your system configuration, recover disk configuration information, and assign specific drive letters to each primary partition or logical drive.

Note Windows NT cannot recognize free space that was created on a FAT partition using the UNDELETE SENTRY feature in MS-DOS version 6.2. With the SENTRY method, MS-DOS reserves part of the hard disk to store deleted files and then compensates during MS-DOS queries about free space. Because Windows NT does not understand SENTRY, it reports the space on the FAT partition as used.

Each partition can have a different file system, such as (FAT) or Windows NT file system (NTFS). If you want multiple file systems and your existing hard disk has only one partition, you must create more than one partition on the hard disk before installing Windows NT.

The Windows NT Setup program can be used to partition the disk while installing Windows NT. However, if you are installing Windows NT on an existing disk and you are going to partition the disk, you should first back up the data.

Support for creating high performance file system (HPFS) partitions is not available in Windows NT version 4.0. HPFS partitions must be removed before running setup.

Partitioning the internal hard disk on a *new* computer is done (using the Setup program) during initial setup when you load the Windows NT operating system software. Making changes to that disk or partitioning a new hard disk is done using Disk Administrator.

After you partition a disk, you can either commit the changes immediately or wait until you quit Disk Administrator to save them.

Note Before you install Windows NT on a computer with other operating systems, you should use the **fdisk** program (or another comparable program) that is included with MS-DOS to determine the number of existing partitions on the disk. If the entire disk has only a single primary partition, you cannot use Disk Administrator to divide that primary partition after Windows NT is installed.

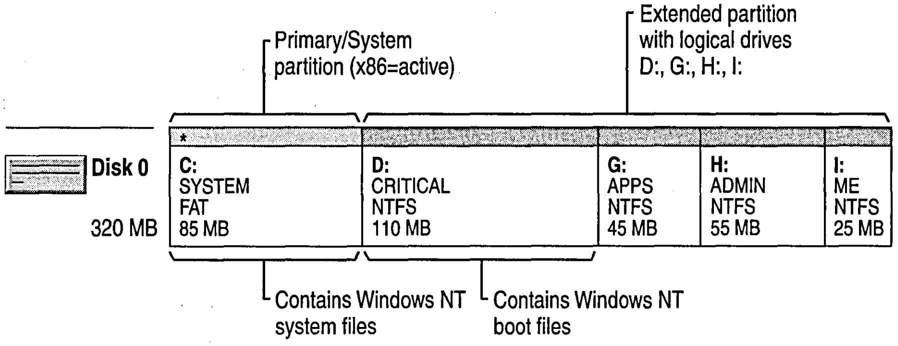
For more information about the **fdisk** program, see the Command Reference in Help.

Setting Up a New Hard Disk

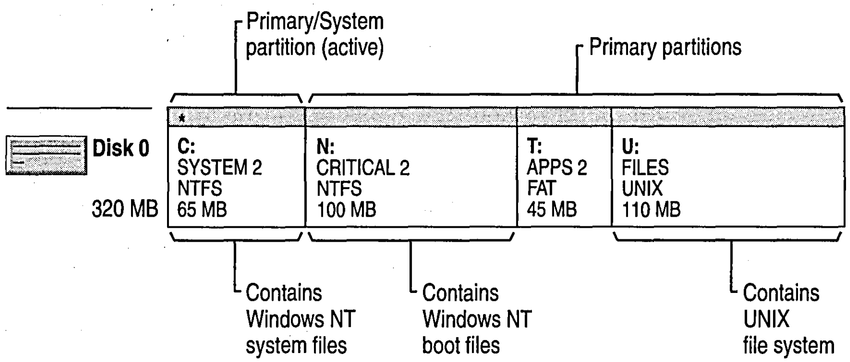
You can create any of the following in the free space on a hard disk:

- A single primary partition
- Additional partitions up to the maximum of four
- An extended partition with a number of logical drives that is limited only by the size of the partition
- Other types of Windows NT volumes, such as volume sets and stripe sets

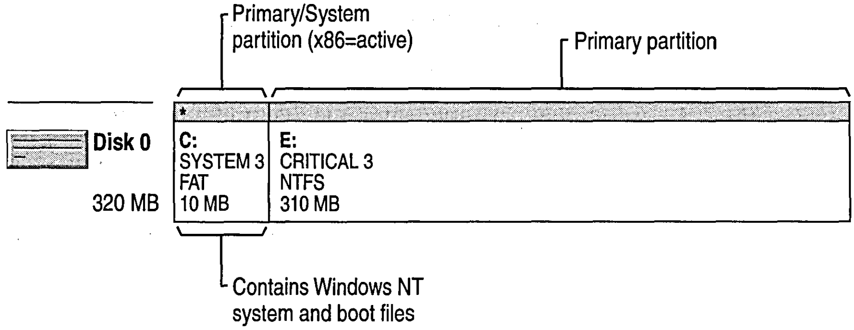
The following illustration shows examples of different disk-partitioning schemes on *x*86-based and RISC-based computers and where certain files might be located.


Primary/System partition (x86=active)
Extended partition with logical drives D:, G:, H:, I:
Disk 0
320 MB
*
C: SYSTEM FAT 85 MB
D: CRITICAL NTFS 110 MB
G: APPS NTFS 45 MB
H: ADMIN NTFS 55 MB
I: ME NTFS 25 MB
Contains Windows NT system files
Contains Windows NT boot files

***x*86 or RISC-based computers**


Primary/System partition (active)
Primary partitions
Disk 0
320 MB
*
C: SYSTEM 2 NTFS 65 MB
N: CRITICAL 2 NTFS 100 MB
T: APPS 2 FAT 45 MB
U: FILES UNIX 110 MB
Contains Windows NT system files
Contains Windows NT boot files
Contains UNIX file system

***x*86-based computers**


Primary/System partition (x86=active)
Primary partition
Disk 0
320 MB
*
C: SYSTEM 3 FAT 10 MB
E: CRITICAL 3 NTFS 310 MB
Contains Windows NT system and boot files

RISC-based computers

Creating Primary Partitions

When creating primary partitions, the system assigns space to a partition starting from the beginning of the space available. Therefore, in the beginning, there are no gaps between partitions. Gaps occur only when you delete a partition later on. For example, if you delete the second of three partitions and create a new, smaller second partition, that will leave a gap of free space between the second and third partitions.

For information about how to create a primary partition, see "Creating Primary Partitions" in Disk Administrator Help.

Creating an Extended Partition

One of the four partitions that you can create under Windows NT, if disk space allows, is an extended partition. You can use the free space in the extended partition to create multiple logical drives or use all or part of it when creating volume sets or other kinds of volumes for fault-tolerance purposes.

For information about how to create extended partitions, see "Creating an Extended Partition," and "Creating Logical Drives in an Extended Partition" in Disk Administrator Help.

Formatting and Labeling Partitions

Before you can store files and directories on the partitions that you have created, you must first commit the changes to disk and then format each partition individually to use with the file system you want to work with. You can also assign descriptive volume labels at this time.

To format and label volumes, you can use the **Format** and **Set Volume Label** commands from the Disk Administrator **Tools** menu, or you can use the **Format** and **Label** commands at the command prompt. For information about the **Format** and **Label** commands, see the Command Reference in Help.

For information about how to format and label volumes using Disk Administrator, see "Formatting and Labeling Partitions" in Disk Administrator Help.

Marking Partitions as Active

The names commonly used for the partitions containing the startup and operating system files are the system and boot partitions, respectively.

The *system partition* for Windows NT is the volume that contains the hardware-specific files needed to load Windows NT. On *x*86-based computers, it must be a primary partition that has been marked as active for boot purposes and must be located on the disk that the computer accesses when starting the system. There can be only one active system partition at a time. If you want to use another operating system, you must first mark its system partition as active before restarting the computer.

For information about how to mark a partition as active, see "Marking Partitions as Active" in Disk Administrator Help.

Partitions on a RISC-based computer are not marked active. Instead, they are configured by a hardware configuration program supplied by the manufacturer. On RISC-based computers, the system partition must be formatted for the FAT file system. On either type of computer, the system partition can never be part of a stripe set or volume set.

The *boot partition* for Windows NT is the volume, formatted for either the NTFS or FAT file system, that contains the Windows NT operating system and its support files. The boot partition can be (but does not have to be) the same as the system partition. The boot partition also cannot be part of a stripe set or volume set.

Securing System Partitions

Since the system partition on a RISC-based computer must be formatted for the FAT file system, there is no way to secure information in individual directories and files on that partition, unless the manufacturer included hardware protection. For information, see the vendor's documentation. Therefore, the only way to secure the system partition is to allow access only to members of the Administrators group. It is best to have the system and boot files on separate partitions when securing the partition.

For information about how to secure system partitions, see "Securing System Partitions" in Disk Administrator Help.

Assigning Drive Letters

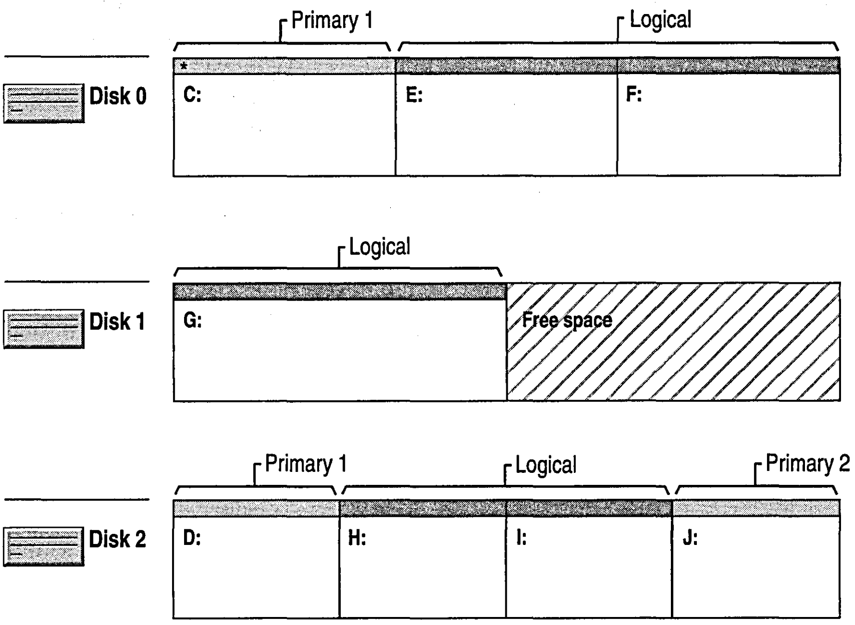
You can create more than 24 volumes with Windows NT, but you cannot assign more than 24 drive letters for accessing these volumes. Drive letters A and B are reserved for floppy disk drives. However, if you do not have a B floppy disk drive, you can use the letter B for a network drive.

Windows NT enables the static assignment of drive letters. This means that a drive letter can be permanently assigned to a specific hard disk and partition/volume. When a new hard disk is added to an existing computer system, it does not affect statically assigned drive letters.

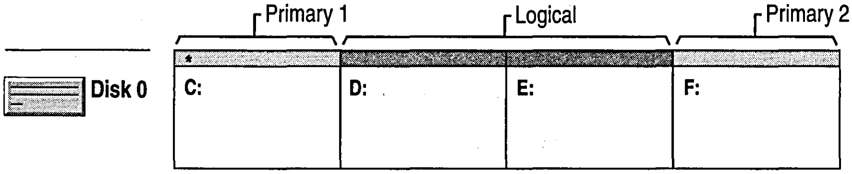
In addition to supporting the static assignment of drive letters on volumes and partitions, Disk Administrator also supports assigning a permanent drive letter to CD-ROM drives.

However, this static assignment of drive letters occurs only after Disk Administrator has been used on the computer. Until then, drive letters are assigned by Windows NT in a manner similar to that used by MS-DOS, which adheres to the following rule: first, the primary partitions on each hard disk get letters assigned starting with the letter C. Windows NT then continues assigning the next available drive letter to each of the logical drives in alphabetical order on each hard disk and then to the other primary partitions on each hard disk. The active system partition is typically the C drive.

The following is an example with three hard disks.



The following is an example with only one hard disk.



Note You should be careful when making drive-letter assignments because many MS-DOS and Windows programs make references to a specific drive letter. For example, the Path environment variable shows specific drive letters with program names.

For information about how to assign drive letters, see "Assigning Drive Letters" and "Assigning CD-ROM Drive Letters" in Disk Administrator Help.

Deleting Partitions, Volumes, or Logical Drives

Before deleting partitions, volumes, or logical drives under Windows NT, you need to ensure that the information on them has been backed up onto another storage medium and verified or is no longer needed.

Windows NT places certain restrictions on your ability to delete. It will not let you delete the volume with the system files (the system partition). Nor can you delete individual partitions that are part of a set without deleting the entire set. However, on a RISC-based computer, you can delete the system partition with the files needed to load Windows NT, so be very careful. Windows NT also requires that all the logical drives or other volumes in an extended partition be deleted before you can delete the extended partition.

Once you delete partitions, volumes, or logical drives, you must first commit the changes before anything else can be done to the partitions, volumes, or logical drives.

For information about how to delete partitions, volumes, or logical drives, see "Deleting Partitions, Volumes, or Logical Drives" in Disk Administrator Help.

Committing Changes

After you have made significant changes to your disk partitions, Disk Administrator displays a message to remind you about the irreversibility of certain changes, such as deleting a partition, and to ask whether you want to save those changes. Disk Administrator performs updates to the disks only after you agree to saving those changes and quit the program or if you commit the changes before quitting Disk Administrator.

Sometimes, after you have committed your changes, another message advises you that changes have been made that require you to restart the computer. (This happens under some circumstances, such as if you extended a volume set, locked a volume, or searched for or restored disk configuration information.) Disk Administrator initiates a complete system shutdown, closes all open applications, and restarts the computer.

Adding Hard Disks

The maximum number of hard disks that you can add to a computer depends on your hardware configuration, such as how many SCSI adapters you have attached. After adding additional hard disks to your computer, restart your computer, and then start Disk Administrator. Before the Disk Administrator window opens, a message advises you that Disk Administrator has noticed a change and will update the system configuration. However, drive letters are not changed by the system when you add new hard disks if they have already been statically assigned.

Saving and Restoring Disk Configuration Information

Disk Administrator provides options for saving and restoring the following currently defined disk configuration information: assigned drive letters, volume sets, stripe sets, stripe sets with parity, and mirror sets. You should be sure to save the disk configuration information before upgrading the operating system to a newer version to ensure that you do not lose your current configuration information.

You can also search for disk configuration information among different installed versions of Windows NT and select a specific version to replace another. However, you should be careful to update this version's information every time you make a change to your disk's configuration. Make your changes first, quit Disk Administrator, restart your computer and Disk Administrator, and then save the configuration information and quit Disk Administrator.

For information about how to save, restore, and search for disk configuration information, see "Saving Disk Configuration Information," "Restoring Disk Configuration Information," and "Searching for Disk Configuration Information" in Disk Administrator Help.

Changing the File System on a Partition

If you want to change the file system on an existing partition, you should back up the information on the partition.

If Windows NT is not installed on the partition, you can use the **Format** command from the Disk Administrator **Tools** menu to reformat that partition to another file system. Or, you can also use the format program at the command prompt. However, reformatting the partition will also destroy all existing data.

If you want to change the file system on an existing FAT partition to the NTFS format, you can use the convert program at the command prompt. Using the **Convert** program does not overwrite data on the disk. The **Convert** program cannot be used to convert an NTFS partition to FAT.

For more information about **Format** and **Convert**, see the Command Reference in Help.

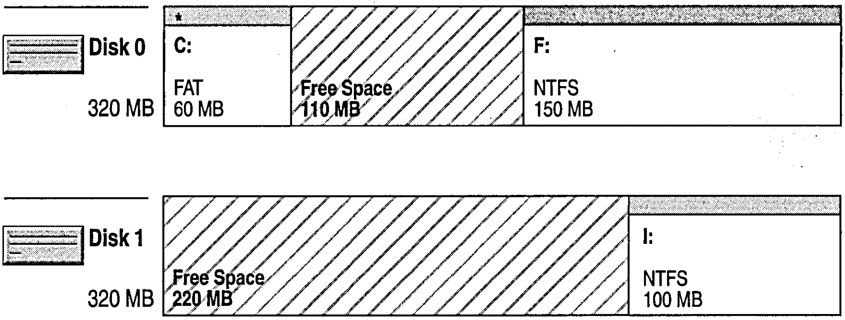
If Windows NT is installed on the partition, you cannot delete it from within Disk Administrator nor reformat the partition using **Format**. Instead, you must use the **Setup** program. For more information about using the **Setup** program, see "Formatting and labeling partitions" and *Windows NT Server Start Here.*

For information about how to reformat partitions, see "Reformatting Existing Partitions" in Disk Administrator Help.

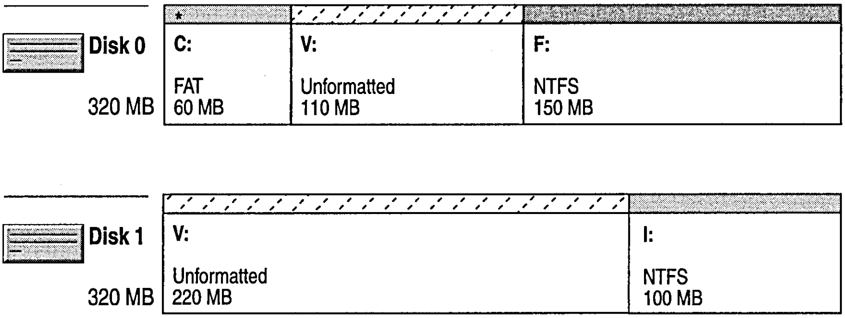
Creating and Deleting Volume Sets

Volume sets are a mechanism for more effectively using the total available free space on several disks. Volume sets are created, as shown in the following illustration, by combining various-sized areas of free space from 1 to 32 disks into one large logical volume set that is recognized as a single partition.

Note Operating systems, such as MS-DOS, that do not have volume-set functionality cannot recognize any volume sets that are created by Windows NT. Therefore, if you create a volume set on a dual-boot computer, those partitions become unusable by MS-DOS.



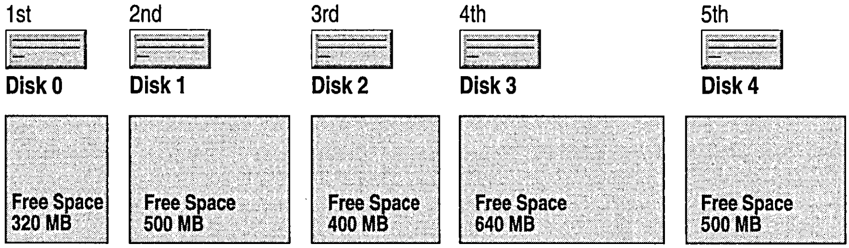
Results showing what the system sees:
volume set (V:) created from free space
on 2 disks=330 MB



The areas of free space used to create volume sets can be different sizes, as shown in the following illustration. Volume sets are organized in such a way that the space on one disk gets filled up and then, starting at the beginning of the next disk, all that space gets filled up. The process continues in the same way on each subsequent disk up to a maximum of 32 disks.

This volume set is a combination of different-sized areas of free space on 5 hard disks for a total of 2360 MB.

Information is stored in the following order:



Deleting smaller partitions and combining them into one volume set frees drive letters for other uses, enables the creation of a large volume for file system use, and can improve system performance by better balancing data input and output (I/O) across the drives. However, volume sets do not have fault tolerance.

Before making any changes to volume sets, you should first back up all the information on the volume set and only then delete the volume set because all the information contained in the set will be deleted, too.

Existing NTFS volumes and volume sets can be extended by adding free space. Disk Administrator forces the system to restart after you quit and save your changes and then formats the new area without affecting any existing files on the original volume or volume set.

For information about how to create, delete, and extend volume sets, see "Creating a Volume Set," "Deleting a Volume Set," and "Extending Volumes and Volume Sets" in Disk Administrator Help.

Creating and Deleting Stripe Sets

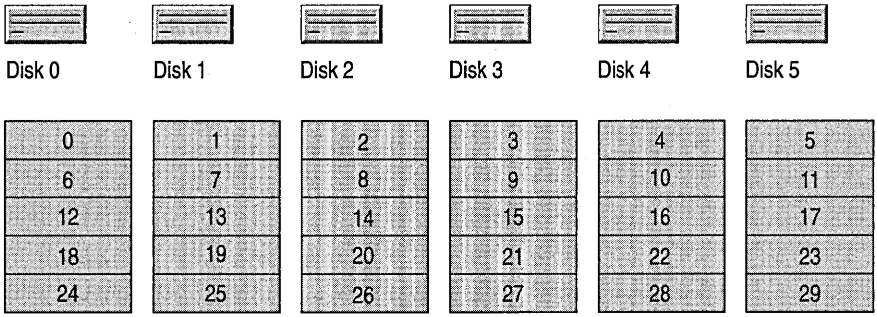
Stripe sets are created similarly to volume sets, but with more restrictions. Each member partition of the stripe set must be on a different disk up to a limit of 32 disks. Also, Disk Administrator will make all the partitions the same size.

Note Operating systems, such as MS-DOS, that do not have stripe-set functionality cannot recognize any stripe sets that are created by Windows NT. Therefore, if you create a stripe set on a dual-boot computer, those partitions become unusable by MS-DOS.

Stripe sets are created by combining areas of free space from 2 to 32 disks into one large logical volume. The partitions in stripe sets are all approximately the same size so that the data can be written in stripes across each partition. This enables I/O commands to be issued concurrently and increases throughput.

The following illustration shows a set of six hard disks and how the stripes are distributed across them.

Information is written across the 5 rows of each partition from stripe #0 to #29.



Disk 0	Disk 1	Disk 2	Disk 3	Disk 4	Disk 5
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

When you no longer want a stripe set or you have a problem with a faulty disk drive, you should first back up all the information on the stripe set and only then delete the stripe set because all the information will be deleted too. Stripe sets without parity do not provide fault tolerance.

For information about how to create and delete stripe sets see "Creating a Stripe Set" and "Deleting a Stripe Set" in Disk Administrator Help

Fault Tolerance

Fault tolerance is the ability of a system to continue functioning when part of the system fails. Normally, the expression fault tolerance is used to describe disk subsystems, but it can also apply to other parts of the system or the entire system. Fully fault-tolerant systems use redundant disk controllers and power supplies as well as fault-tolerant disk subsystems. You can also use uninterruptible power supplies (UPSs) to safeguard against local power failure. For more information about UPS, see “Managing Uninterruptible Power Supplies” later in this chapter.

Although the data is always available and current in a fault-tolerant system, you still need to make tape backups to protect the information on your disk subsystem against destructive events such as fire, earthquakes, tornadoes, floods, and user errors. Disk fault tolerance is not an alternative to a backup strategy with offsite storage. For more information about backing up to tape, see Chapter 6 “Backing Up and Restoring Network Files.”

Fault tolerance is designed to combat problems with disk failures, power outages, or corrupted operating systems which can include boot files, the operating system itself, or system files.

Fault-tolerant disk systems are standardized and categorized in six levels known as Redundant Arrays of Inexpensive Disks (RAID) level 0 through level 5. Each level offers various mixes of performance, reliability, and cost. Disk Administrator includes RAID levels 0, 1, and 5. Only levels 1 and 5 provide fault-tolerance.

RAID strategies can be implemented using hardware or software solutions. In a hardware solution, the controller interface handles the creation and regeneration of redundant information. In Windows NT Server, this activity can be performed in the software. A hardware implementation of a RAID strategy can offer performance advantages over the software implementation included in Windows NT Server.

Understanding RAID

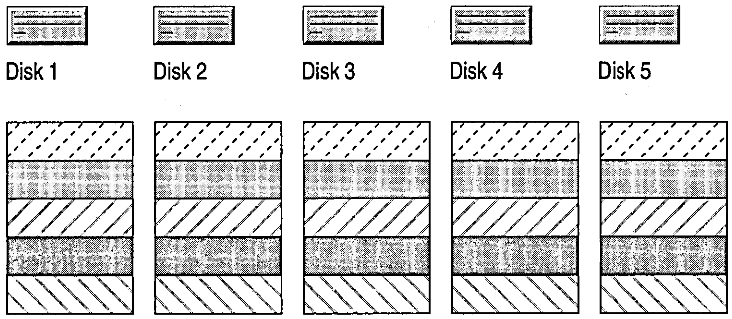
Disk arrays consist of multiple disk drives coordinated by a controller. Individual data files are typically written to more than one disk in a manner that, depending on the RAID level used, can improve performance and/or reliability.

However, there is no fault tolerance until the fault is repaired. Few RAID implementations can withstand two simultaneous failures. When the failed disk is replaced, the data can be regenerated using the redundant information. Data regeneration occurs without bringing in backup tapes or performing manual update operations to cover transactions that took place since the last backup. When data regeneration is complete, all data is current and again protected against disk failure. The ability to provide cost-effective high data availability is the key advantage of disk arrays.

Level 0: Stripe Sets

Stripe sets are created by combining areas of free space on from three to 32 disks into one large logical volume. Data is divided into blocks and spread in a fixed order among all the disks in the array.

Level 0 stripe sets do not provide any fault tolerance.



RAID Level 0

Stripe sets in Windows NT write data to multiple partitions, as is done with volume sets. However, striping writes files across all disks so that data is added to all disks in the set at the same rate.

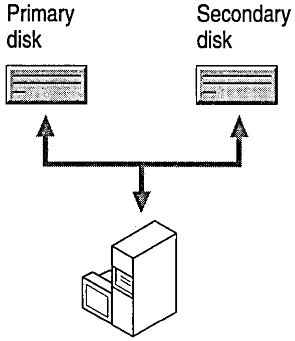
Stripe sets offer the best performance of all the Windows NT Server disk management strategies, including volume sets. However, like volume sets, it does not provide fault tolerance. If any partition in the set fails, all data is lost.

Level 1: Mirror Sets

Mirror sets provide an identical twin for a selected disk; all data written to the primary disk is also written to the shadow or mirror disk. This results in disk space utilization of only 50 percent. If one disk fails, the system uses data from the other disk. For more information about dealing with boot failures, see “Fixing a System or Boot Failure” later in this chapter.

Mirror sets protect a partition on a disk from media and, possibly, controller failure by maintaining a fully redundant copy on another disk. When a mirrored partition fails, you must break the mirror set to expose the remaining partition as a separate volume with its own drive letter. That volume then becomes the main partition, and you can create a new mirror-set relationship with unused free space of the same size or greater on another disk.

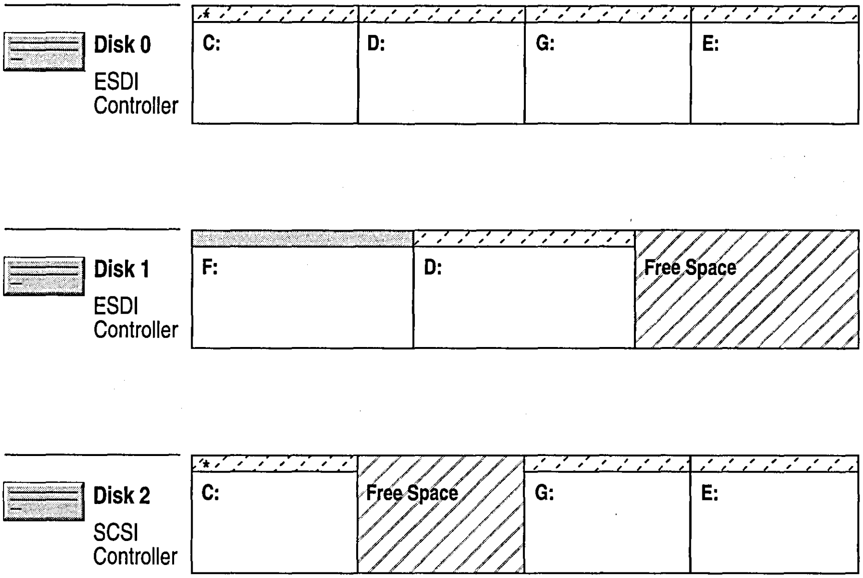
Mirror sets are created by duplicating a partition using free space on another disk. If the second partition is larger, the remaining space becomes free space. The same drive letter is used for both partitions. Any existing partition, even the system and boot partitions, can be mirrored onto another partition of the same size, or greater, on another disk using either the same or a different controller. When creating mirror sets, it is best to use disks that are the same size, model, and manufacturer.



RAID Level 1

Mirror sets have better overall read and write performance than level 5, stripe sets with parity. Another advantage of mirror sets over stripe sets with parity is that there is no loss in performance when a member of a mirror set fails. Mirror sets are more expensive in terms of dollars per megabyte because its disk space utilization is less. But its entry cost is lower because it requires only two disks, whereas stripe sets with parity require three or more disks.

The following illustration shows examples of mirror sets using the same and different controllers.



Mirror sets reduce the chance of an unrecoverable error by providing a duplicate set of data, which doubles the number of disks required and the input/output (I/O) operations when writing to the disk. However, some performance gains are achieved for reading data because of I/O load balancing of requests between the two partitions.

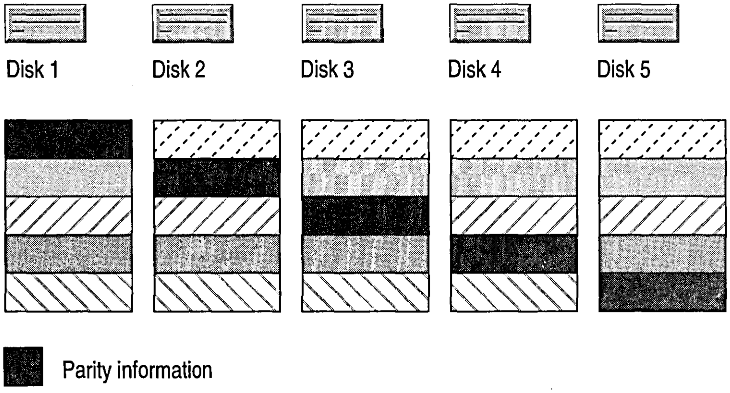
When you want to use the space in a mirror set for other purposes, you must first break the mirror set and then delete the partition. Breaking the mirror set does not delete the information, but it is still safer to do a backup first. You will then be ready to delete one of the partitions that made up the mirror set to regain free space.

In the case of an unrecoverable error on a partition within a mirror set, you need to break the mirror-set relationship to expose the remaining partition as an individual partition or logical drive. You can then reassign some free space on another disk to create a new mirror set. For more information about breaking mirror sets, see the *Windows NT Server Resource Kit* version 4.0.

For information about how to establish, break, or delete a mirror set, see "Establishing a Mirror Set" and "Breaking a Mirror Set," in Disk Administrator Help.

Level 5: Stripe Sets with Parity

Level 5 is commonly known as *striping with parity*. The data is striped in large blocks across all the disks in the array. Level 5 differs because it writes the parity across all the disks. The data redundancy is provided by the parity information. The data and parity information are arranged on the disk array so that the two are always on different disks.



RAID Level 5 Configuration

Stripe sets with parity have better read performance than mirror sets. However, when a member is missing, such as when a disk has failed, the read performance is degraded by the need to recover the data with the parity information.

Nevertheless, this strategy is recommended over mirror sets for applications that require redundancy and are primarily read-oriented. Write performance is reduced by the parity calculation. Also, a write operation requires three times as much memory as a read operation during normal operation. Moreover, when a partition fails, reading requires at least three times the memory as would normally be used, both caused by parity calculation.

Understanding Windows NT Parity Usage

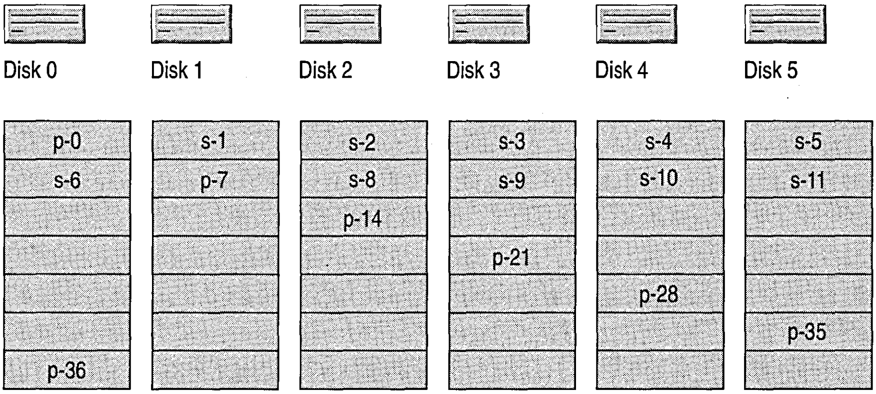
The data redundancy method used in Windows NT Server for striping with parity is a function of the Boolean operation called *exclusive OR*, also referred to as **XOR**. The important concept to remember about parity is that regeneration uses the parity information with the data on the good disks to re-create the data on the failed disk. The Windows NT Server stripe-sets-with-parity form of fault tolerance maintains an XOR of the total data. This enables the reconstruction of missing data (on a failed disk or sector) from the remaining disks in the stripe set with parity.

Note Using stripe sets with parity require more system memory than using mirror sets. The recommended minimum RAM is 16 MB or greater.

Stripe sets with parity include one parity strip per row. Therefore, you must use at least three, rather than two, disks to allow for the parity information. Parity strips, as shown in the following illustration, are distributed across all the partitions to balance the I/O load. The protection provided here is as complete as with disk mirroring. This technique provides data redundancy at a cost of only one additional disk for the set. Recovery from the failure of a disk in a parity stripe set is more time consuming, though, than for mirror sets.

The following illustration shows a set of six hard disks and how the parity stripes are distributed across the partitions.

Parity information starts at the first stripe on Disk 0, continues at the second stripe on Disk 1, the third stripe on Disk 2, and so on until the sixth stripe on Disk 5, after which it starts over again on Disk 0.



When you want to recover the space in a stripe set with parity for other purposes, be sure to do a backup first if you want to reuse that information and then delete the stripe set.

For information about how to create and delete stripe sets with parity, see "Creating a Stripe Set with Parity" and "Deleting a Stripe Set with Parity" in Disk Administrator Help.

Windows NT RAID Strategy Summary

In Windows NT Server, stripe sets provide the best performance but provide no fault tolerance (that is, data redundancy).

When compared to stripe sets with parity, a mirror-set implementation has a lower entry cost, requires less system memory, provides the best overall performance, and does not show performance degradation during a failure. However, its cost-per-megabyte is higher than that for stripe sets with parity.

A stripe-set-with-parity implementation has better read performance and a lower cost-per-megabyte, but it requires more system memory and loses its performance advantage while a member is missing.

Stripe sets with parity are a good solution for data redundancy in a computing environment in which most activity consists of reading data. For example, if your network has a server on which you maintain all copies of the programs used by the people at that site, this might be a good case for using a stripe set with parity. This would enable you to protect the programs against the loss of a single disk in the stripe set. In addition, the read performance would improve due to concurrency of the reads across the disks making up the stripe set with parity.

In an environment in which frequent updates to the information occur, it can be better to use mirror sets. However, you can use a stripe set with parity if you want redundancy and if the storage overhead cost of a mirror is prohibitive.

Notice that operating systems, such as MS-DOS, that do not have fault-tolerance functionality cannot recognize the partitions that Windows NT Server creates for fault tolerance. Therefore, if you mirror your MS-DOS system partition on a dual-boot computer, MS-DOS cannot use or start either partition. Also, as a precaution, you should be sure to create a recovery disk so that you can start your computer from the mirrored partition if the system partition is lost. For information on creating and using such a recovery disk, see "Creating a Recovery Disk on x86-based Systems" later in this chapter.

Managing Uninterruptible Power Supplies

An uninterruptible power supply (UPS) provides power when the local power fails. It is usually rated to provide a specific amount of power for a specific period of time. This power comes from batteries that are kept charged while main power is available. The main power is converted from an AC voltage to a DC voltage used to charge the battery. When needed, the DC power is converted to an AC voltage compatible with the computer power supply. Usually, all that is needed from a UPS is time to shut down the system in an orderly fashion by quitting processes and closing sessions.

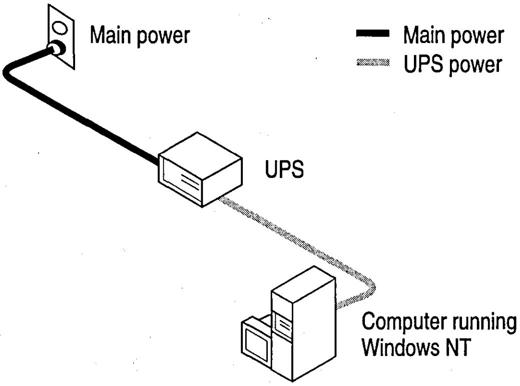
To minimize downtime from power failures and provide some advance warning before total power loss, Windows NT provides the UPS option in Control Panel for managing an uninterruptible power supply.

Before purchasing a UPS device to use with Windows NT, confirm with the UPS manufacturer that both the device and its serial cable are compatible with Windows NT.

Understanding UPS Types

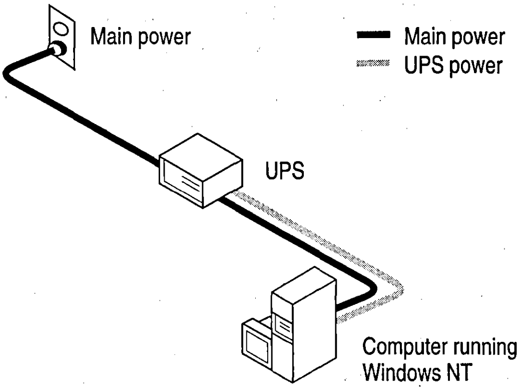
Uninterruptible power supplies fall into two categories: *online* and *standby.*

You connect an online UPS between the main power and the computer to constantly supply your computer system with power. Connecting it to the main power keeps its battery charged. This method provides *power conditioning*, which means that it removes spikes, surges, sags, and noise.



Configuration of an Online UPS

A standby UPS is configured to provide either the main power or its own power source and to switch from one to the other as necessary. When the main power is available, the UPS device connects the main power directly to the computer and monitors the main power voltage level. The UPS power supply is kept in standby mode (that is, ready to provide power but using very little), and the battery is kept charged. When the main power fails or the voltage falls below an acceptable level, the UPS device switches the power fed to the computer from the main power to its own power. This should occur so quickly that the computer power supply can provide uninterrupted service. A standby UPS can also provide power conditioning during regular service if it is built into the main power path, but it is not a function of the conversion process of the UPS power supply.



Configuration of a Standby UPS

Hybrid versions of these two types can also exist. Check the reliability and failure-handling mechanism of the UPS device before buying or installing it.

Understanding How a UPS Interacts with Operating Systems

Many UPS devices can interface with operating systems, enabling the operating system to notify users automatically of the pending shutdown process or provide notification that the power has been restored and a shutdown is no longer necessary.

During a power failure, the UPS service immediately pauses the Server service to prevent any new connections and sends a message to notify users of the power failure. The UPS service then waits a specified interval of time before notifying users to quit their sessions. If power is restored during the interval, another message is sent to inform users that power has been restored and normal operations have resumed.

Setting Up the Uninterruptible Power Supply

You can use the UPS option in Control Panel to set the following options:

- The serial port where the UPS device is connected.
- Whether the UPS device sends a signal if the regular power supply fails.
- Whether the UPS device sends a warning when battery power is low.
- Whether the UPS service sends a signal telling the UPS device to shut off.
- A command file to execute at shutdown time.
- The expected life and recharge time for the battery.
- The timing for warning messages.

The actual options for configuring the UPS service depend on the specific UPS hardware installed on your system. Incorrect settings can cause undesirable operation of your UPS hardware. For details about possible settings, see the documentation for your UPS device.

For information about how to set up a UPS, see "Configuring the Uninterruptible Power Supply (UPS)" in Help.

After configuring UPS options, be sure to test that your computer is protected from power failure. For information about how to test the configuration of your UPS, see "Testing your UPS Configuration" in Help.

Understanding How the Windows NT UPS Service Works

The UPS option in Control Panel enables the UPS service to communicate with a UPS device through a serial port with the following signals.

Signal	Pin	Asserted by
Power Failure	CTS (Clear To Send)	UPS hardware
Low Battery	DCD (Data Carrier Detect)	UPS hardware
UPS Shutdown	DTR (Data Terminal Ready)	Windows NT UPS service

The assertion of each of these pins can be either positive or negative, depending on the UPS device's implementation. Use the **UPS** dialog box to specify the polarity used by the UPS hardware. For configuration details, see the vendor's manual.

To support contact-closure type UPS devices, the UPS service always does the following:

- TXD (Transmit Data) pin 6 is set permanently low.
- RTS (Request To Send) pin is set permanently high.

When the UPS service is started, it verifies the settings in the **UPS** dialog box by assuming that the system is not starting during a power failure and by ensuring that the signal polarity on the CTS and DCD pins is opposite to that specified as the failure condition in the **UPS** dialog box. For example, if the **UPS** dialog box specifies that the UPS device supports a Power Failure Signal (CTS pin) with a positive signal, the UPS service checks to make sure that this pin is not already asserted positive (which would not happen unless you had started the system during a power failure).

This has some important implications. With an online UPS, the UPS device can shut itself off immediately if the configuration is incorrect. With a standby UPS, an incorrect configuration typically shuts the UPS device off as soon as a power failure is detected, effectively circumventing the purpose of the UPS. This is why it is important to configure and test your UPS device to ensure that it operates correctly.

When the UPS service starts, it waits until the CTS pin is asserted by the UPS. If you have indicated in the **UPS** dialog box that your UPS device does not support a Low Battery signal, the UPS service uses the parameters specified in the **UPS Characteristics** box of the **UPS** dialog box to estimate the charge level of your battery in terms of minutes. Each time you start the UPS service, the charge level of your battery is reset to 0 minutes. As time elapses, the Battery Recharge parameter is used to estimate the battery life to a maximum time specified by the Expected Battery Life parameter. The UPS service requires at least two minutes to perform a graceful shutdown. Therefore, if your battery does not have more than two minutes of life remaining, a shutdown is performed immediately. Since it is important that the parameters in the **UPS Characteristics** box be set accurately, it is best to use worst-case estimates.

When a power failure occurs, the UPS service uses the parameters in the **UPS Service** box of the **UPS** dialog box to decide how to respond. For noisy power (that is, power that fluctuates regularly), the first parameter should be set for a few seconds. The first parameter is the time between power failure and the initial warning message. Setting the first parameter minimizes messages being broadcast.

The UPS device continually sends messages at an interval specified in the second parameter of the **UPS Service** box. The second parameter specifies the delay between warning messages. The second parameter should be set very low if you want to ensure that users are aware of the power failure or set high if it is not important to let users know about the power failure. When the UPS battery is low, the service initiates a shutdown and then turns off the UPS device (if this feature is supported).

Using a UPS Device with Windows NT

You should use the following Windows NT services in combination with the UPS device that you select for your computer:

- UPS
- Alerter
- Messenger
- Event Log

The following are some basic points to be aware of to ensure that your UPS is installed correctly and to protect your computer from the hazards of a power failure.

A UPS device supplies power to your computer and peripherals (for example, the monitor and printer) when the main power supply is interrupted or fails completely. Some UPS devices can supply power for only a few minutes, while others can supply power for many hours. In any case, you should configure UPS properly to work with Windows NT so that the UPS can track power fluctuations and take appropriate actions. For example, if a power failure is prolonged, the UPS might not be able to supply power for the entire duration of the failure. In this case, Windows NT warns users of the power failure. When the UPS reaches a critical state, the operating system shuts down, and the UPS device is turned off. Therefore, you should ensure that your UPS device guarantees at least two minutes to enable the operating system to perform a graceful shutdown.

To select a UPS device that works with Windows NT, see the *Windows NT Server Hardware Compatibility List.* This usually means ordering the correct serial cable from the UPS manufacturer. This cable is designed to follow the UPS interfacing specification for Windows NT. If you are upgrading your computer to Windows NT and already have a UPS, check with the manufacturer to ensure that the existing cable works with Windows NT. Unexpected results can occur if the wrong cable is used.

UPS manufacturers can have their own software that can be purchased separately to take advantage of the unique features of their UPS device. In this case, you should not use the UPS service that comes with Windows NT. Follow the instructions that come with the UPS manufacturer's software.

The UPS service is configured using the UPS option in Control Panel. You should base the configuration on the features supported by the UPS device that you are using. The three features that Windows NT supports are:

- Main-power failure detection.
- Low battery detection.
- UPS shutdown capability.

To determine the correct settings, read the user's manual for your UPS device carefully, or contact the manufacturer. Based on the features supported by the UPS, you might have to enter additional parameters in the **UPS Characteristics** box of the **UPS** dialog box.

The UPS service can be controlled in several ways. One way is to configure the settings in the **UPS** dialog box and click **OK**. A message appears and asks if you want to start the UPS service. Another way to start the service is by using the Services option in Control Panel.

The Alerter and Messenger services are started automatically when Windows NT starts. The Alerter service sends alerts to selected users, and the Messenger service sends messages to your local Windows NT computer and to other users on the network. All detected power fluctuations and power failures are recorded in the event log, along with UPS service start failures and server shutdown initiations.

To ensure that the computer is protected from power failures, test it by simulating a power failure (that is, by disconnecting the main power supply to the UPS device). Your computer and peripherals connected to the UPS device should remain operational, and messages should be displayed and events logged. Wait until the UPS battery reaches a low level to verify that a graceful shutdown occurs. Restore the main power to the UPS device, and check the event log to ensure that all actions were logged and there were no errors.

Running a Command File upon UPS Shutdown

The Windows NT UPS service supports the running of a command file the administrator defines. You should specify a command file only if your system requires special actions prior to a system shutdown. For example, you can have a custom application running that is connected to another computer. You can use the command file to end the session and log off the connected computer automatically prior to system shutdown.

You cannot specify a command file that causes a dialog box to appear because dialog boxes can require user input and would therefore impede a graceful system shutdown.

The command file must reside in your *Systemroot*\System32 directory and have one of the following extensions: .exe, .com, .bat, or .cmd. After you have created the file and placed it in the proper directory, use the **UPS** dialog box to activate its use upon UPS shutdown. Select the **Execute Command File** option, type the file name, and click **OK**.

Note The command file must finish running in 30 seconds. A run time that is greater than 30 seconds threatens the capability of Windows NT to complete a graceful system shutdown. You should test the operation of the command file under a worst-case scenario.

System Diagnosis, Recovery, and Repair

These system diagnosis, recovery, and repair methods are described in this section:

- Use Windows NT Diagnostics to diagnose configuration problems.
- Use the **Recovery** box (**Startup/Shutdown** tab) in the System option of Control Panel to specify how Windows NT Server records and responds to severe errors.
- Restore the previous working configuration using the Last Known Good Configuration.
- Restore corrupt or missing system files, as well as the boot sector, and configuration information using the Repair process in Windows NT Setup. Depending on what you need to repair, you might need to use the Emergency Repair Disk. You can also use the Emergency Repair Disk program (Rdisk.exe) to update your system information or create a new Emergency Repair Disk.
- Create and use a recovery disk to start the computer after failure of the primary partition.

A list of other error detection tools available in Windows NT Server appears at the end of this section.

Using Windows NT Diagnostics for System Diagnosis

You can use Windows NT Diagnostics (Winmsd.exe), the diagnostic tool for Windows NT Server, to view and print configuration information for a local or remote computer. Windows NT Diagnostics is located in the Administrative Tools folder. With Windows NT Diagnostics, you can view the following:

- Operating system information, such as the version number and system boot options, plus process, system, and user environment variables

- Hardware details such as BIOS information, video resolution, CPU type, and CPU steppings
- Physical memory, paging file information, and DMA usage
- The current state of each driver and service on the computer
- Drives and devices installed on the computer, plus related interrupt (IRQ) and port information
- Network information, including transports, configuration settings, and statistics
- Printer settings, fonts settings, and system processes that are running

Using System Recovery in Control Panel

When a severe error (called a *STOP error*, or *fatal system error* or *blue screen*) occurs, by default the system does the following:

- Writes an event to the system log.
- Alerts administrators.
- Dumps system memory to a file you can use for debugging.
- Automatically restarts the server.

Because Windows NT Server automatically restarts rather than waiting for administrator intervention, fatal system errors cause less server down time than they would otherwise.

The dump of system memory to a log file can be valuable for debugging the cause of the STOP error. If you contact your technical support representatives about the error, they might ask for the log file. Notice that Windows NT writes the log file to the same file name (Memory.dmp, by default) each time a STOP error occurs. To preserve log files, you should copy them to a new file name after the computer restarts.

If you want to change how Windows NT reacts to a STOP error, use the System option (**Startup/Shutdown** tab) in Control Panel. For information about how to configure the System option, see “Configuring System Recovery Options” in Help.

Using the Last Known Good Configuration

If you encounter difficulty starting Windows NT Server after you installed a new driver or changed a driver configuration, you can choose to start Windows NT Server using the Last Known Good Configuration.

▷ To use the Last Known Good Configuration

1. Start your computer and press the SPACEBAR immediately when the words "OS Loader V4.00" appear.

   A Hardware Profile/Configuration Recovery menu appears that lets you select one of the following:

   - A hardware profile to be used when starting the computer
   - Switch to the Last Known Good configuration
   - Restart computer

2. Select **L** to use the **Last Known Good Configuration** to start Windows NT Server as it was before you made the changes that prevented it from starting.

   All configuration changes that were made since your system was last successfully started are lost.

Using the Repair Process

If your system files or boot partition are corrupt and you are unable to start the computer using the Last Known Good method, you can use the Repair process in Windows NT Setup to restore your system.

To repair a Windows NT Server installation, Windows NT Setup needs either the configuration information that is saved in the *Systemroot*\Repair directory or on the Emergency Repair Disk created when you installed Windows NT (or created later using the **rdisk** program).

For information about how to use or create an Emergency Repair Disk, see "Repair Disk Utility" in Help.

If your system becomes corrupt and you cannot repair it using the Emergency Repair Disk or using the information in the \Repair directory, you must reinstall Windows NT Server from the original installation source. For more information about restoring your system, see the *Windows NT Server Resource Kit* version 4.0.

▷ To restore Windows NT Server on an *x*86-based computer using the repair process in Windows NT Setup

1. If you installed Windows NT Server using the original Setup floppy disks or CD-ROM or using Winnt.exe, start Setup just as you did originally. That is, insert the Setup Boot Disk in drive A and start the computer.
2. In the text-based Setup screen that asks whether you want to install Windows NT Server or repair files, type **r** to indicate that you want to repair your Windows NT Server files.

3. Windows NT Setup asks you for the Emergency Repair Disk. If you do not have one, Setup presents a list of the Windows NT installations that it found on your computer and lets you select the one you want to repair.
4. Follow the instructions on the screen, inserting the Emergency Repair Disk (if you have one) in drive A and providing any other Windows NT Setup disks as requested.
5. When the final message appears, remove the Emergency Repair Disk from drive A, and then press CTRL+ALT+DEL to restart your computer.

▷ **To restore Windows NT Server on a RISC-based computer with an Emergency Repair Disk**

1. Start the Windows NT Setup program as instructed in your manufacturer-supplied documentation. (How you start Windows NT Setup depends on the type of RISC-based computer you have.)
2. In the text-based Setup screen that asks whether you want to install Windows NT Server or repair files, type **r** to indicate that you want to repair your Windows NT Server files.
3. Follow the instructions on the screen, inserting the Emergency Repair Disk (if you have one) in drive A if Setup asks for it.
4. When the final message appears, remove the Emergency Repair Disk, and then press ENTER to restart your computer.

   The repair process in Windows NT Setup enables you to select what you want to repair.

Note The Emergency Repair Disk program (**rdisk**) does not backup user accounts or file security unless you specify the **/s** parameter with the **rdisk** command at the command prompt.

Caution Be sure to update the system repair information in the \Repair directory on your hard disk and to create and maintain an up-to-date Emergency Repair Disk. This way, your system repair information will account for new configuration information such as drive letter assignments, stripe sets, volume sets, mirrors, and so on. Otherwise, drives can be inaccessible in the event of a system failure.

You can use the **rdisk** program to update your system repair information and to a create a new Emergency Repair Disk. For more information about **rdisk** see *Windows NT Server Start Here.*

Recovering From Disk and Sector Failures

The Windows NT Server fault-tolerance tools enable you to recover quickly and easily from problem situations. Mirror sets enable you to have instant access to another disk with a redundant copy of the information on a failed disk. Using stripe sets with parity enables you to regenerate data by using the parity strip if a disk fails. Bad-sector mapping capabilities enable the system to fix sector failures without user intervention.

This section briefly discusses how to recover data from the following types of error situations:

- Failed disk in a stripe set with parity
- Sector failures
- Failed disk in a mirror set

Fixing Mirror Sets and Stripe Sets with Parity

When a member of a mirror set or a stripe set with parity fails, it becomes an *orphan*. The fault-tolerance driver (Ftdisk.sys) then determines that it can no longer use it and directs all new reads and writes to the remaining members of the fault-tolerance volume.

When a member of a mirror set is orphaned, you must first break the mirror-set relationship to expose the remaining partition as a separate volume. The remaining, working member of the mirror set receives the drive letter that was previously assigned to the complete mirror set. The orphaned partition receives the next available drive letter or whatever letter you want to assign.

You can then create a new mirror-set relationship from unused free space on another disk. When you restart the computer, the data from the good partition is copied to the new member of the mirror set.

For information about how to break a mirror set, see "Breaking a Mirror Set" in Help.

When a member of a stripe set with parity is orphaned, you can regenerate the data for the orphaned member from the remaining members. In Disk Administrator, select a new area of free space that is the same size as or greater than, the other members of the stripe set with parity, and then regenerate the data. If you are required to restart the computer, the fault-tolerance driver reads the information from the strips on the other member disks and then re-creates the data of the missing member and writes it to the new member.

Regenerating a stripe set requires the volume be locked by the operating system. All network connections to the volume are lost when a volume is regenerated.

For information about how to regenerate a recoverable stripe set with parity, see "Regenerating a Recoverable Stripe Set with Parity" in Help.

Fixing Sector Failures

The file system verifies all sectors when it formats a volume. All faulty sectors are spared from service. Windows NT Server fault-tolerance services add sector-recovery capabilities to the system.

When there is a sector I/O failure in a fault-tolerant system with redundant copies of the data, the fault-tolerance driver attempts to spare the bad sector from use. This includes performing a device control asking the disk device driver to spare the sector from use. Small Computer System Interface (SCSI) devices can do this, but AT devices, such as Integrated Device Electronics (IDE) and Enhanced Small Device Interface (ESDI), cannot.

When the sector cannot be spared, the correct information obtained from the redundant copy is returned to the file system with a status message stating that there is a faulty sector in the I/O. The file system then attempts to locate the failure and spare the bad sectors by removing them from the sector map of the file system. An error is logged in Event Viewer about the potential for data loss if the partition containing the redundant copy also fails. For more information about Event Viewer, see Chapter 9, "Monitoring Events."

Disk Administrator also enables you to check for errors on your disk. Click **Check For Errors** on the **Tools** menu. For information about how to check your disk for errors, see "Checking for Errors" in Help.

Fixing a System or Boot Failure

If the system or boot partition of a disk fails, the system will not start. The process used to recover from a startup failure depends on the disk configuration and the computer system's microprocessor type. If the system or boot partition on the disk is not part of a mirror set, the system-backup copies should be restored to the replacement disk.

For a system or boot partition configured as part of a mirror set, which is the only fault-tolerant method that can be applied to the boot and system partitions, the recovery procedure depends on whether the computer is *x*86-based or RISC-based. Both use a recovery disk for startup protection, and both use Advanced RISC Computing (ARC) names to describe the path to the boot partition. You should create and test the recovery disk in advance of any failure, or you cannot start your computer from the mirror if the primary partition is lost.

Understanding ARC Names

To set up the boot information for recovery in the Windows NT environment, you must understand ARC names and how they are constructed. ARC names are a generic method of identifying devices within the ARC environment. For disk devices, ARC names are constructed as follows:

<component>(x)disk(y)rdisk(z)partition(a)

where *<component>* identifies the hardware adapter for the device. The two valid values for this field are **scsi** and **multi**, where **scsi** indicates a SCSI disk and **multi** indicates a disk interface other than SCSI. (Multi can also be used for SCSI disk interfaces if the BIOS is enabled on the disk controller.) For Windows NT, this could be a disk supported by the AtDisk driver or one supported by AbiosDsk.

x is the ordinal number of the adapter. For example, if there are two SCSI adapters in the system, the first to load and initialize is assigned the ordinal **0** and the next number assigned is **1**. This continues for all adapter drivers that initialize.

y is, for **scsi**, the SCSI bus number for multiple-bus SCSI adapters. For **multi**, this is always **0**.

z is, for **scsi**, always **0**. For **multi**, this is the ordinal for the disk on the adapter, which determines the order the disk appears in Disk Administrator.

a is the partition ordinal for the partition used on the disk. All partitions receive a number, beginning with 1, except type 5 (MS-DOS Extended) and type 0 (unused) partitions.

For example, if the Windows NT tree is located on the fourth partition on a SCSI disk with the target ID of 3 on the second SCSI controller in the system, the ARC name is:

scsi(1)disk(3)rdisk(0)partition(4)

Starting Windows NT Server on an x86-based Computer

Windows NT Server starts in the following sequence on an *x*86-based computer:

1. When Windows NT Server is installed, it alters the system's boot sector to look for and run a program called Ntldr.
2. Ntldr reads Boot.ini and builds a menu of the operating systems that you can start. (The Boot.ini file is described following this list.)

3. Ntldr runs Ntdetect.com, which builds a list of the system's hardware components.
4. You can select an operating system from the menu, or let the time-out count down to 0 to start the default operating system.

   If you don't see the menu and the default operating system automatically starts, the time-out value has been set to 0 in Boot.ini.
5. The low-level components of Windows NT Server load, and then Windows NT Server initializes the drivers and starts the services based on information stored in the registry.
6. The high-level components of Windows NT Server load, and then the Welcome screen is displayed so you can log on.

Editing Boot.ini

If Windows NT Server does not start, make sure that the statements in Boot.ini (found in the root directory of your system partition) refer to the correct path for the *Systemroot* directory.

Boot.ini is a system text file that has two sections: the first specifies the default operating system to start and a time-out value specifying how long to wait before starting automatically, and the second specifies the operating systems that you can start. For example, if your system is configured to run either Windows NT Server or MS-DOS, Boot.ini typically looks like this:

```
[boot loader]
timeout=30
default=SCSI(0)disk(0)rdisk(0)partition(1)\winnt40

[operating systems]
SCSI(0)disk(0)rdisk(0)partition(1)\winnt40="Windows NT Server"
c:\="MS-DOS"
```

You can edit the text displayed in quotes to customize the operating system choices, but you must first change the read-only, hidden, and system attributes of Boot.ini.

To view and change the attributes of the Boot.ini files, see "Viewing all file and filename extensions" and "Changing file or folder properties" in Help. Attributes can also be changed using the **attrib** command at the command prompt. For more information about **attrib,** see the Command Reference in Help.

Creating a Recovery Disk on x86-based Systems

For *x*86-based systems, a Boot.ini file is located on the system partition. This file contains a menu selection and the ARC-name location for the Windows NT boot partition.

In this example, the system contains one Adaptec SCSI adapter and two Future Domain SCSI adapters. The adapter controller is the first on the SCSI chain. The boot partition is mirrored on the Future Domain adapter. The ARC names are as follows:

scsi(0)disk()rdisk()partition() would be for the Adaptec SCSI devices.
scsi(1)disk()rdisk()partition() would be for the first Future Domain adapter.
scsi(2)disk()rdisk()partition() would be for the second Future Domain adapter.

Create the recovery disk by formatting a floppy disk using the Windows NT operating system and then copying the following files to the disk. The files are located in the root directory of the system partition:

- Ntldr
- Ntdetect.com
- Ntbootdd.sys (required only if the boot partition is on a SCSI disk and BIOS is not enabled on the controller; this file is the SCSI miniport driver used to find the mirror disk)
- Boot.ini (with an alternate path pointing to the mirrored copy of the system partition, specified using ARC naming conventions)
- Bootsect.dos (only on multiple-boot computers)

Creating a Recovery Disk on RISC-based Systems

RISC-based systems have information equivalent to the Boot.ini files in nonvolatile RAM. The process for creating a recovery disk for RISC systems using the Microsoft firmware is to copy the following files to the Windows NT-formatted blank floppy disk:

- Osloader.exe
- Hal.dll

The vendor firmware provides for boot maintenance operations through menu selections. To set up a boot selection for the boot disk, set the OSLOADER value to **scsi(0)disk(0)fdisk(0)\Osloader.exe** and the SYSTEMPARTITION value to **scsi(0)disk(0)fdisk(0)**. The value for **fdisk(***x***)** can be changed to 1 to use the second floppy disk in the system. You also need to set appropriate values for the following selections:

- OSLOADPARTITION, which is the ARC name that specifies the secondary mirrored partition

- OSLOADFILENAME, which is the path to the *Systemroot* directory for Windows NT (for example, \Winnt40 or \Windows) on the secondary mirrored partition

After the Windows NT boot loader program, Osloader.exe, has finished loading Windows NT and the configured drivers, the fault-tolerant services are present and can perform the remaining corrective actions for starting the system. Notice, however, that RISC-based systems can access only SCSI devices connected to the built-in SCSI adapter during the firmware boot process. Therefore, to protect the boot or system partition on a RISC-based system, both drives used must be connected to the internal SCSI adapter.

Testing Your Newly Created Recovery Disk

To test your recovery disk, use it to boot the system from the shadow partition. Test the disk both with the primary disk powered on and then with the primary disk powered off. In both cases, if you can log on, the recovery disk works.

Maintaining Your Recovery Disk

You should update the recovery disk every time partitions are changed. For example, if you are using partition 2 to start and you delete partition 1, you must change the ARC name to start using partition 1. Likewise, if you are starting on partition 2 and you delete partition 1 and repartition it into partitions 1 and 2, you must change the ARC name to start using partition 3. For more information about ARC names, see "Understanding ARC Names" earlier in this chapter.

Maintaining the Boot Configuration

Once Windows NT Server starts successfully, back up the configuration directory (*Systemroot*\System32\Config), and maintain current backups as you change the configuration and accounts. The registry is made up of the files in the configuration directory. For more information about backing up the registry, see Chapter 6 "Backing Up and Restoring Network Files."

If you have to use the Repair option in Windows NT Setup to restore the registry files, you can restore the configuration from your backup.

For *x*86-based systems, do not delete Boot.ini, Ntldr, Bootsect.dos, Ntdetect.com, or Ntbootdd.sys (if Windows NT Server is installed on a SCSI disk) in the root directory of the system partition. For RISC-based systems, do not delete Hal.dll or Osloader.exe in \OS\NT. If these hidden system files are deleted, Windows NT Server will not start. Use the Emergency Repair Disk to recover these files.

If you made changes to a system that previously started Windows NT Server successfully and it now does not start, you can return to your previous configuration by selecting Last Known Good Configuration at system boot. If Windows NT Server still will not start, use the Repair process in Windows NT Setup to restart the system. Once the system is restarted, you can restore data using backup tapes.

Other Error Detection Tools

Some other ways in which Windows NT Server reports errors and preserves your system configuration and data include the following:

- If your system uses NTFS, Windows NT Server logs all file transactions, replaces bad clusters automatically, and stores copies of key information for all files on the NTFS volume.
- Services and applications record events, including errors, in the event logs that you can view in Event Viewer. For information about Event Viewer, see Chapter 9, "Monitoring Events."
- The Alerter and Messenger services work together to provide warnings on printer, security, and user session problems. These services also provide server shutdown warnings if the system uses the UPS service. For information, see "Managing Uninterruptible Power Supplies" earlier in this chapter.
- Performance Monitor can be configured to create an alert log for monitoring performance and generating network alerts. For information about Performance Monitor, see Chapter 8, "Monitoring Performance."
- **Chkdsk** examines disk space and use for the NTFS and FAT file systems. If there are errors on the disk, **chkdsk** alerts you and corrects the errors if the **/f** switch is used. If files are open when **chkdsk** is attempting to correct disk errors, **chkdsk** lets you specify to have it automatically check the disk and correct errors the next time the computer restarts. For more information, see the Command Reference in Help.

  The **chkdsk** program can also be run using the **Check for Errors** command from the Disk Administrator **Tools** menu.

  Caution Using **chkdsk** to repair file system errors or bad sectors on very large volumes can render the volume inaccessible for a several days.

- Dr. Watson for Windows NT can be used to detect, diagnose, and log application errors for use by technical support personnel. To run Dr. Watson, type **start drwtsn32** at the command prompt. Press F1 for Help on setting up and using Dr. Watson.

Repairing Config.nt and Autoexec.nt

If Windows NT Server displays an error message concerning these files, or if you have problems running MS-DOS–based applications, check whether Config.nt or Autoexec.nt is incorrect or missing. The files are located in the *Systemroot*\System32 subdirectory.

If the files are incorrect or missing, you can copy new versions from the Emergency Repair Disk to the \System32 subdirectory, as described earlier in this section.

Recovering a Windows NT Server

The most common failures requiring system recovery are hardware failure (irreparable physical disk damage) and accidental deletion or modification of data. These failures can happen on your system partition, boot partition, or data partition.

If a failure occurs on a critical server, you will want to recover and get running as soon as possible. Information in the following sections should help you formulate a recovery plan.

In general, the steps outlined next also apply to recovering a Windows NT Workstation.

Making Recovery Easier

When you first set up a server, you can reduce the time needed for system recovery by putting the Windows NT Server system and boot partitions and the data partition(s) on separate drives. This will greatly simplify recovery if a disk is damaged.

If you use Disk Administrator to create stripe or mirror sets, you should save the disk configuration data each time you change the configuration. You can save the configuration to the server's Emergency Repair Disk or to a separate disk.

Note Always run the Emergency Repair Disk (**rdisk**) program just before and after you make any changes to the disk configuration. Doing so enables you to return to a stable configuration that was in place before changes were made. For information about how to use the **rdisk** program see "Repair Disk Utility" in Help.

Another helpful record to have during disk recovery is a written list of disk partitions and their sizes. Attach this information to the front of each disk drive.

The Emergency Repair Disk contains configuration information needed to recover a server if the system partition is lost. If system recovery of a server requires reinstallation of system software, you can use the Emergency Repair Disk to start the system and then select the Repair option in the Setup program to automatically restore this information.

How to Recover a Server

If a server has a disk failure on the disk containing the server's system partition, use the following steps to recover the server from tape.

1. If there was a disk failure, replace the disk.
2. If the failed disk contained the system partition, reinstall Windows NT Server on the new disk. You can recover the server's system partition and part of its registry information using the server's Emergency Repair Disk to start the system and then using the Setup program's **Repair** option.

   However, if a backup tape is more current than the Emergency Repair Disk, restore the registry from the backup tape.
3. Restart the server.
4. From a tape drive attached to the server (not over the network), restore the system partition from the last normal backup.

   The system partition contains hardware-specific files needed to load Windows NT. Therefore, drivers that were installed after the first Windows NT installation will not be restored unless you restore the system partition from tape. The files on the system partition are not stored or updated on the Emergency Repair Disk.
5. Restore any applicable incremental or differential backup sets. Be sure to select the **Restore Local Registry** option to recover the rest of the registry information.
6. Restart the server.

   It is now ready for normal use.

There can be a significant delay if the server performs time-critical functions and you use step 2 (reinstalling Windows NT Server on the new disk). To minimize the time necessary to recover the server, you can create a *recovery drive*. This is an external SCSI drive, as small as 100 MB. It can be a dedicated disk drive, which sits on the server's SCSI chain but is powered off to prevent accidental modification. It can also be a pooled portable drive, which you can then cable to any server that fails.

To prepare the recovery drive for future use, install Windows NT Server on the drive, and configure a local paging file and tape driver on it. Then create a recovery disk containing the files needed to load and initialize Windows NT Server. Be sure that the Boot.ini file points to the SCSI address of the recovery drive. For more information about the files needed to load and initialize Windows NT Server and creating a recovery disk, the *Windows NT Server Resource Kit* version 4.0.

When a system failure occurs, cable the recovery drive to the server (or power it on if it is already attached to the server). Restart the server using the recovery disk you created for the recovery drive.

If the recovery drive has the minimal software and user accounts to run your server, you can operate the server with the recovery drive until the next scheduled maintenance period and then make a full restore from tape.

Depending on the size of the recovery drive, you can either make the recovery drive your new system drive and restore from tape. Or, you can replace the failed drive and restore to the new drive in the background while the recovery drive keeps the server running.

CHAPTER 8

Monitoring Performance

Windows NT Server includes two tools for tracking computer performance:

- *Performance Monitor* enables you to look at resource use for specific components and application processes using charts and reports. With Performance Monitor, you can gauge your computer's efficiency, identify and troubleshoot possible problems (such as unbalanced resource use, insufficient hardware, or poor program design), and plan for additional hardware needs. You can also use alerts to notify you when resource use reaches a specified value.

  For comprehensive documentation on monitoring Windows NT Server performance, see the *Windows NT Server Resource Kit* version 4.0.

- *Task Manager* gives you a quick view of how each application, application component, or system process is using CPU and memory resources, as well as a summary of overall CPU and memory usage.

  To run Task Manager, right-click the toolbar, and then click **Task Manager**. For more information on using Task Manager, see Task Manager Help.

Conceptual Overview

Performance Monitor uses a series of counters that track data, such as the number of processes waiting for disk time, the number of network packets transmitted per second, and the percentage of processor utilization. With this data, you can create charts, set alerts, and format reports that enable you gauge and tune system performance. Data can be displayed as it is collected, stored in logs for later use and comparison, or both.

With Performance Monitor, you can:

- View data from any number of computers simultaneously.
- Receive immediate feedback on how changes that you make affect the computer.
- View and dynamically change charts reflecting current-activity counter values.
- Export data from charts, logs, alert logs, and reports to spreadsheet or database programs for further manipulation and printing.

- Create an alert log that lists (and, optionally, notifies you) when a counter's value has passed a user-configured threshold.
- Create log files containing data about various objects from different computers so you can view information gathered over time. You can use these log files to record typical or usual resource use, look for trends, and project hardware requirements (capacity planning).
- Append to one file selected sections of other existing log files to form a long-term archive.
- View current-activity reports or create reports from existing log files.
- Save individual chart, alert, log, or report settings, or the entire workspace setup, and reuse when needed.

Despite its wide applicability, Performance Monitor does not answer every performance-tuning question. As a broad-based tool, it provides an overview of the computer's performance. Sometimes it can isolate the problem; at other times, you will use it to indicate which specialized tool (such as a profiler, a working set monitor, or a network analyzer, also called a sniffer) to use next.

Starting and Quitting Performance Monitor

Start Performance Monitor from the **Administrative Tools** submenu on the **Start** menu or from the command line. When you start Performance Monitor from the command line, you can specify a *settings file*. If you do not specify a settings file, Performance Monitor searches the current working folder for the default chart file, Default.pmc. The following table shows the settings file types supported by Performance Monitor and the extensions they use.

Settings file type	Settings file extension
Alert	.pma
Chart	.pmc
Log	.pml
Report	.pmr
Workspace	.pmw

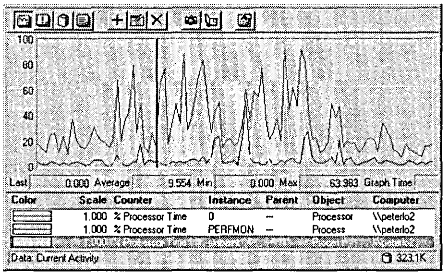
You can also specify a computer name in addition to, or instead of, a settings file. That computer then appears as the default computer when you click the **Add To** command or the **Add Counter** button.

To quit Performance Monitor, click **Exit** on the **File** menu. You can save performance monitor settings for a particular view (chart, alert, log, or report), or you can save the entire workspace.

For information about saving settings, see "Saving Settings" in Performance Monitor Help.

Organizing Your Screen

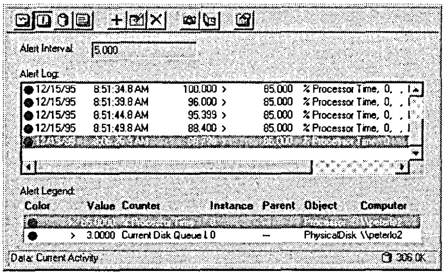
Performance Monitor consists of four main windows, which you display by choosing to view Chart, Alert, Log, or Report. The same objects and counters are available for monitoring in all four views.



Last 0.000 Average 9.554 Min 0.000 Max 63.983 Graph Time

Color	Scale	Counter	Instance	Parent	Object	Computer
▭	1.000	% Processor Time	0	--	Processor	\\peterlo2
▭	1.000	% Processor Time	PERFMON	--	Process	\\peterlo2
▭	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]

Data: Current Activity 323.1K



Alert Interval: 5.000

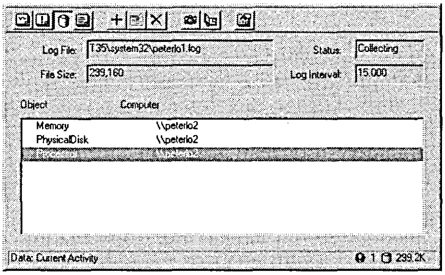
Alert Log:

```
● 12/15/95   8:51:34.8 AM   100.000 >   85.000  % Processor Time, 0,  , I
● 12/15/95   8:51:39.8 AM    96.000 >   85.000  % Processor Time, 0,  , I
● 12/15/95   8:51:44.8 AM    95.399 >   85.000  % Processor Time, 0,  , I
● 12/15/95   8:51:49.8 AM    88.400 >   85.000  % Processor Time, 0,  , I
```

Alert Legend:

Color	Value	Counter	Instance	Parent	Object	Computer
●	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]
●	> 3.0000	Current Disk Queue L	0	--	PhysicalDisk	\\peterlo2

Data: Current Activity 306.0K

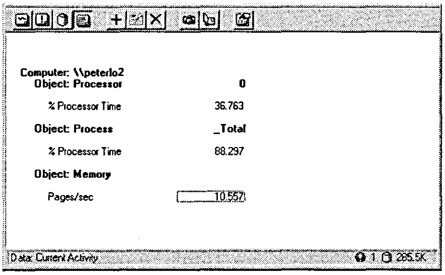


Log File: T35\system32\peterlo1.log Status: Collecting

File Size: 239,160 Log Interval: 15.000

Object	Computer
Memory	\\peterlo2
PhysicalDisk	\\peterlo2
[illegible]	[illegible]

Data: Current Activity 1 299.2K



Computer: \\peterlo2

Object: Processor	**0**
% Processor Time	36.763
Object: Process	**_Total**
% Processor Time	88.297
Object: Memory	
Pages/sec	10.557

Data: Current Activity 1 285.5K

Tip To ensure that Performance Monitor is visible over any other window on your screen, click Always On Top on the Options menu.

When selecting an object to monitor in Log view, all counters for that object and all instances of that object are monitored when you start collecting data in a log file. Later, when you view the results in one of the other view windows, you can selectively view those counters and instances that are of interest to you.

The **Data From** command on the **Options** menu enables you to manipulate an existing log file rather than view current activity (the default).

The status bar indicates the data source (current activity or the name of the log file), the size of the log file (if you are logging data), and the number of alerts that have occurred since you were last in Alert view (if you have set alerts).

For more information on working in the Performance Monitor views, see "Using Performance Monitor" later in this chapter.

For information on how to organize your screen, see "Organizing Your Screen" in Performance Monitor Help.

Understanding Counter Organization

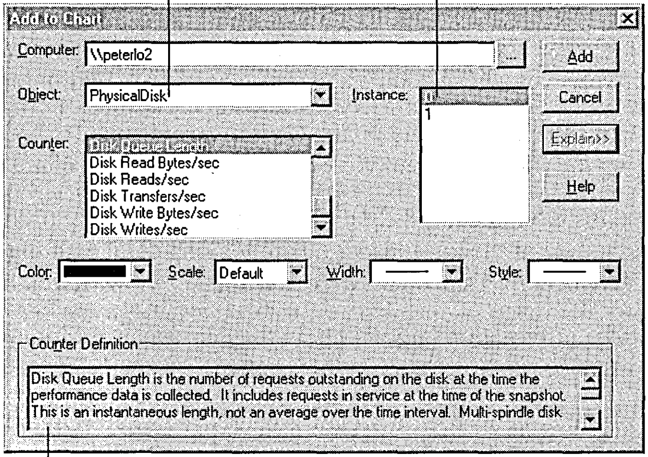
When monitoring a system, you actually monitor the behavior of its *objects*. Windows NT Server uses objects to identify and manipulate system resources. Windows NT Server contains objects to represent individual processes, sections of shared memory, and physical devices.

Performance Monitor groups counters by *object type*. A unique set of counters exists for the processor, memory, cache, hard disk, processes, and other object types that produce statistical information. Certain object types and their respective counters are present on all systems; other counters, such as transport protocol counters, appear only if the computer is running the associated software. The following object types are available on most computers running Windows NT Server.

Cache
LogicalDisk
Memory
Objects
Paging File
PhysicalDisk
Process
Processor
Redirector
Server
System
Thread

Some object types have several *instances*. For example, the Processor object type will have multiple instances if a system has multiple processors. The Physical Disk has two instances if a system has two disks. Some object types (the Memory and Server) do not have instances. If an object type has multiple instances, you can add counters to track statistics for each instance, or in many cases, for all instances at once.

Instances 0 and 1 refer to the server's two disk drives.



Computer: \\peterlo2

Object: PhysicalDisk

Instance: 0
1

Counter: Disk Queue Length
Disk Read Bytes/sec
Disk Reads/sec
Disk Transfers/sec
Disk Write Bytes/sec
Disk Writes/sec

Color: ■ Scale: Default Width: —— Style: ——

Counter Definition

Disk Queue Length is the number of requests outstanding on the disk at the time the performance data is collected. It includes requests in service at the time of the snapshot. This is an instantaneous length, not an average over the time interval. Multi-spindle disk

Performance Monitor supplies an explanation for each counter.

Two object types, *processes* and *threads*, have a particularly close relationship.

- Processes consist of an executable program, a set of virtual memory addresses, and a thread. When a program runs, a Windows NT *process* is created. A process can be an application (Microsoft Word for Windows, Corel® Draw), a service (Event Log, Computer Browser), or a subsystem (print spooler, POSIX).
- Threads are objects within processes that run program instructions. They allow concurrent operations within a process and enable one process to run different parts of its program on different processors simultaneously. Each thread running on a system shows up as an instance for the Thread object type and is identified by association with its parent process. (For example, if Windows NT Explorer has two active threads, Performance Monitor identifies them as Thread object instances Explorer= =>0 and Explorer= =>1.)

Note Instances of the Process object type appear as numbers if they are internal system processes. Other types of processes are identified by the name of the executable file. Only 32-bit processes normally appear in the **Instance** box, and 16-bit applications running in a Virtual DOS Machine (VDM) appear only if they are started in a separate memory space.

The displayed counter values are either an average over the last two data reads or the last value for the counter. For example, counters that cover a time span, such as Memory Pages/sec, are averaged over the last two data reads (separated by the length of the time interval); whereas threshold counters, such as Process Thread Count, indicate the last value that was read.

When you first start using Performance Monitor, the number of performance counters might seem overwhelming. It is not necessary to be familiar with all performance counters. Some are appropriate only for programmers writing Windows NT platform-based applications; others are useful for vendors who need to test hardware performance.

Tip For help understanding a selected counter, click the **Explain** button in the **Add To** dialog box to display the **Counter Definition** box.

Looking for Specific Performance Problems

System throughput problems usually occur when the demand for resources (such as microprocessors, memory, hard disks, and networking hardware and software) exceeds supply. Isolating performance problems starts with determining how users, applications, and the operating system interact with each resource. The remainder of this section focuses on counters of interest to system administrators, specifically those counters that indicate something about system and network throughput.

Watching How Applications Use System Resources

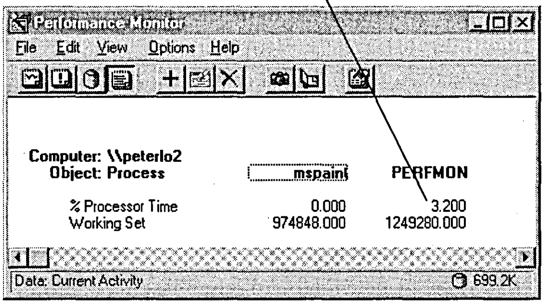
You can learn a lot about a system by seeing how various applications use memory. Focus on the %Processor Time and Working Set counters. These counters, which belong to the Process object type, are defined as follows:

% Processor Time
: The percentage of elapsed time that a processor is busy executing a thread for a particular process. (Notice that % Processor Time is high for the Idle process when the system is not busy.)

Working Set
: The current number of physical memory bytes used by or allocated to a process. This value can be larger than the minimum number of bytes actually *needed* by the process.

Using these counters, you can generate a report that focuses on all or a subset of the applications running on a computer. The sample report shown below illustrates activity for two applications: Performance Monitor (perfmon) and Paint (mspaint).

Processor activity occurs every time Performance Monitor retrieves data.



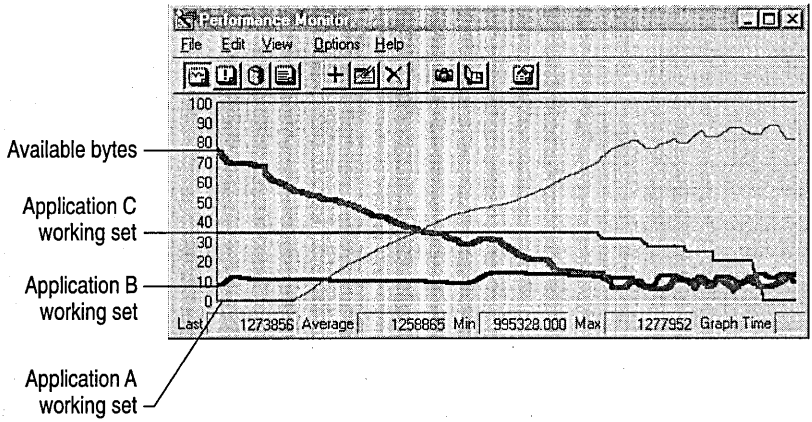
```
Computer: \\peterlo2
  Object: Process                 mspaint      PERFMON

     % Processor Time               0.000        3.200
     Working Set               974848.000  1249280.000
```

This example represents a snapshot of system activity. In a real-time report or chart, certain counter values, such as Working Set, are relatively static, whereas others, such as % Processor Time, change constantly. For example, at application startup, it's normal to see the % Processor Time value climb sharply, decrease, and then level off.

The processor activity for Performance Monitor occurred when it was time to read a new set of counter values. Counters are read at regular intervals set by the user. If you were to double the data retrieval interval and then rerun the sample Report, the % Processor Time counter would decrease by half to approximately 1.20 percent.

Although there was no activity in the Paint program, the operating system allotted memory to it because the program was started. Every program running can use a portion of physical memory—its *working set.* This counter value changes slowly over time depending on the activity of the application. The working set value is of particular interest when the Available Bytes counter falls below a certain threshold. (The Available Bytes counter belongs to the Memory object type.) This signifies that Windows NT Server is gradually beginning to take memory from the working sets of running applications to ensure that a certain amount of free memory exists. If large numbers of bytes are reallocated, an application's performance decreases.

The following figure shows how Windows NT Server satisfies the memory requirements of Application A by using free (available) bytes. It then begins to replenish the lack of available bytes by gradually taking memory from the working sets of less active programs (Applications B and C).


Performance Monitor
File Edit View Options Help
100
90
80
70
60
50
40
30
20
10
0
Available bytes
Application C working set
Application B working set
Application A working set

Last 1273856 Average 1258865 Min 995328.000 Max 1277952 Graph Time

You can expand sample reports and charts to include more applications and more counters. To understand system activity, watch these and other counter values while changing system activity levels.

Making Sure You Have Enough Memory

Memory usage is perhaps the most important factor in system performance. When memory demand exceeds supply, Windows NT Server moves blocks of code and data, called *pages*, from random access memory (RAM) to disk to free up space for a process. Some paging is acceptable because it enables Windows NT Server to use more memory than actually exists in physical memory (RAM). Constant paging, however, is a drain on system performance.

When you start Windows NT Server, it automatically creates a paging file (Pagefile.sys) on your system. Windows NT Server uses the paging file to provide virtual memory. The recommended size for the paging file is equivalent to the amount of RAM available on your system plus 12 megabytes (MB). However, the size of the file also depends on the amount of free space available on your hard disk when the file is created. You can change virtual memory settings (paging file size) using the **Performance** tab of the System option in Control Panel.

Depending on requirements and available disk space, the paging file can expand upward to a user-specified maximum size (also set through the Control Panel). If memory demands decrease, the paging file might shrink back to its original size. When running a large number of applications, it might be necessary to expand the paging file size. (It is more efficient to expand initial paging file size than to extend maximum file size; forcing Windows NT Server to allocate more paging file space slows the start of applications and fragments the disk.)

Checking for Excessive Paging

To confirm whether excessive paging is occurring, add the Avg. Disk sec/Transfer (a physical disk counter) and Pages/sec counter values. If the product of these counters exceeds 0.1, paging is taking more than 10 percent of disk access time. If this occurs over a long period, you probably need more memory.

Next, check for excessive paging due to running applications. If possible, stop the application with the highest working set value, and see if that dramatically changes the paging rate. If you suspect excessive paging, check the Pages/sec counter in Performance Monitor. This counter, which is part of the Memory object type, shows the number of pages that had to be read from disk because they were not in physical memory. (Notice the difference between this counter and Page Faults/sec, which indicates only that data was not immediately available in the specified working set in memory.)

Checking Paging File Size

To see if your paging file is approaching its upper limit, check the actual file size and compare it to the maximum paging file size setting in the System option in Control Panel. If these two numbers are close in value, consider increasing initial paging file size or running fewer applications.

Paging file counters offer another way to see if the size of the Pagefile.sys file is appropriate. The two counters of interest are % Usage and Usage Peak (bytes) under the Paging File object type. If the Usage Peak value approaches the maximum paging file setting, or if % Usage nears 100 percent, consider increasing the initial file size.

If multiple paging files are spread across multiple disk drives, the counter path name of each file appears as an instance of the Paging File object type. You can either add a counter for each paging file or select the Total instance to look at combined usage data for all your paging files.

Monitoring Processor Activity

A process is made up of one or more threads. Each process thread requires a certain number of processor cycles when it runs. If demand exceeds supply, long processor queues develop and system response suffers. To gauge the activity of the processor, check the % Processor Time counter (under the Processor object type). The % Processor Time counter shows the percentage of elapsed time that a processor is busy executing a non-idle thread.

If processor activity is 100 percent, you can assume that a faster processor will improve performance. However, 100 percent processor usage is not necessarily bad, unless the processor queue length is excessive. For example, one application performing a processor-intensive process can easily use 100 percent of the processors time. However, if many processes are queued up waiting for processor time, performance will suffer for all applications. To determine how many process are contributing to processor utilization, use the System Object Processor Queue Length counter. If more than a couple of application processes are contending for the majority of processor time, you might need to install a faster processor or another processor if you are using a multiprocessor system.

Acceptable processor usage can depend on computer activity. If a system is used for computational work, it is reasonable to see heavy processor usage. On servers that are busy processing many requests, sustained 100 percent processor usage is unacceptable.

The Interrupts/sec counter, which measures the rate of service requests from I/O (input/output) devices, is also an important Processor counter. If this counter value increases dramatically without a corresponding increase in system activity, it can indicate a hardware problem.

Monitoring Disk Activity

Disk usage statistics help you balance the workload of network servers. By monitoring disk activity, you can identify the most popular share points and move them to the best-performing equipment. Monitoring disk performance is also important. With proper disk I/O, strain on virtual memory is minimized, and programs run faster. Performance Monitor provides two types of disk counters:

- *Physical disk counters* are important for troubleshooting and capacity planning.
- *Logical disk counters* provide statistics on free space and help pinpoint the source of activity on a physical volume.

Activating Physical and Logical Disk Counters

Windows NT can provide performance data on many aspects of the system. Most of this data is collected automatically and does not require you to issue a command. The one exception is information on the performance of physical and logical disk activity on your own or another computer. Because disk counters can increase disk access time by approximately 1.5 percent on some older *x*86 computers, Windows NT does not automatically activate the counters at system startup.

For specific instructions on activating the physical and logical disk counters, see "Activating the Physical and Logical Disk Counters" in Performance Monitor Help.

Determining Workload Balance

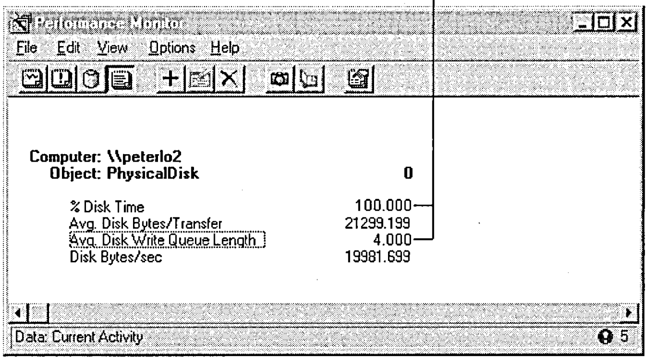
To balance loads on network servers, you need to know how busy server disk drives are. Use the % Disk Time counter (under the Physical Disk object), which indicates the percentage of time a drive is active. If % Disk Time is high (over 90%), check the Current Disk Queue Length counter to see how many system requests are waiting for disk access. The number of waiting I/O requests should be sustained at no more than 1.5 to 2 times the number of spindles making up the physical disk. Most disks have one spindle, although Redundant Array of Inexpensive Disks (RAID) disks usually have more. A hardware RAID device appears as one physical disk in Performance Monitor, while RAID device created through software appear as multiple drives (instances). You can either add the Physical Disk counters for each non-RAID physical drive listed in the **Instance** box, or you can select _Total instance to monitor data for all the computer's drives.

If Current Disk Queue Length and % Disk Time values are consistently high, consider upgrading the disk drive or moving some files to an additional disk or server.

Note If you are using a RAID device, the % Disk Time counter can indicate a value greater than 100 percent. If it does, use the Avg. Disk Queue Length counter to determine how many system requests are waiting for disk access.

Tracking Disk Performance

The Avg. Disk sec/Transfer counter reflects how much time a disk takes to fulfill requests. A high value might indicate that the disk controller is continually retrying the disk because of failures. For most disks, high average disk transfer times correspond to values greater than 0.3 seconds. A missed disk revolution typically adds 16 milliseconds to average disk transfer time.



```
Computer: \\peterlo2
   Object: PhysicalDisk                          0

      % Disk Time                          100.000
      Avg. Disk Bytes/Transfer           21299.199
      Avg. Disk Write Queue Length           4.000
      Disk Bytes/sec                     19981.699
```

Data: Current Activity 5

These values indicate disk saturation.

You can also check the value of Avg. Disk Bytes/Transfer. A value greater than 20K indicates that the disk drive is generally performing well; low values result if an application is accessing a disk inefficiently. Applications that access a disk at random also raise Avg. Disk sec/Transfer times because random transfers require increased seeking time.

Monitoring Network Activity

At a minimum, network monitoring typically consists of two activities: watching server performance and measuring overall network traffic. On a Windows NT network, use Performance Monitor to track server performance and to troubleshoot if a problem occurs. If you enable the *Network Monitor Agent*, you can use network-related objects with Performance Monitor to analyze overall network performance.

For information on monitoring overall network traffic, see Chapter 10, “Monitoring Your Network.”

Watching Server Throughput Statistics

Windows NT Workstation and Windows NT Server include networking software that enables them to act as a client or a server. Redirector software (Rdr.sys) transmits requests; Server software (Srv.sys) receives and interprets incoming messages. (Redirector and Server software are represented in the user interface as the workstation and server services, respectively.) Each computer running Windows NT also uses at least one type of protocol software to handle packet formatting and routing. Windows NT supports several protocols, including NetBEUI and TCP/IP.

The Redirector (Rdr.sys), Server (Srv.sys), and protocols (NetBEUI and TCP/IP if installed) each generate a set of statistics that appear as Performance Monitor counters. (Other protocols can also generate counters.) Abnormal network counter values often indicate problems with a server's memory, processor, or disks. For that reason, the best approach to monitoring a server is to watch network counters in conjunction with previously discussed counters, such as % Processor Time, % Disk Time, and Pages/sec.

For example, if a dramatic increase in Pages/sec is accompanied by a decrease in Bytes Total/sec handled by a server, the computer is likely running short of physical memory for network operations. Most network resources, including network adapter cards and protocol software, use nonpaged memory. If a computer is paging excessively, it could be because most of its physical memory has been allocated to network activities, leaving a small amount of memory for processes that use paged memory. To verify this situation, check the computer's system event log for entries indicating that it has run out of paged or nonpaged memory.

The following table lists various network counters. By observing these counter values over a period of time, you can gain knowledge of network operations.

Object type	Counter	Description
Server	Bytes Total/sec	The number of bytes sent and received from the computer each second. This counter indicates the computer's rate of activity.
Server Work Queues	Queue Length	The current length of the server work queue for this CPU. A sustained queue length greater than four indicates possible processor congestion. This counter is an instant read, not an average over time.
NetBEUI	Frame Bytes Received/sec Frames Received/sec	Bytes and frames sent to this computer's network address. The ratio of Frame Bytes to Frames Received (the number of bytes per frame) should remain fairly constant.
	Frames Rejected/sec	Frames received by the computer that were incorrect and therefore had to be resent. The ratio of Frames Rejected to Frames Received should be low.
NetBEUI Resource	Times Exhausted	A cumulative counter that indicates the number of times since system startup that certain network resources were unavailable. A sharp and consistent increase in values for instances 0 through 4 (links, addresses, address files, connections, and requests) usually indicates network problems.

Monitoring Overall Network Traffic

If network traffic exceeds local area network (LAN) capacity, performance typically suffers across the network. To prevent this situation, it is important to monitor network-wide traffic levels, particularly on larger networks with bridges and routers, using the Network Segment object. When monitoring network traffic, three network segment counters are of special interest.

Counter	Description
% Network utilization	Indicates how close the network is to full capacity. The threshold depends on your network infrastructure and topology. If the value of the counter is above 40 percent, collisions can cause problems.
Total frames received/second	Indicates when bridges and routers might be flooded.
Broadcast frames received/second	Can be used to establish a baseline if monitored over time. Large variations from the baseline can be investigated to determine the cause of the problem. Because each computer processes every broadcast, high broadcast levels mean lower performance.

To analyze these statistics for your network segment, install the Network Monitor Agent. The Network Monitor Agent collects statistics from the computer's network adapter card by putting it in *promiscuous mode*, a state in which the network adapter card can be directed by a device driver to pass on to the operating system all the frames that pass over the network. To determine if your card supports promiscuous mode, see the documentation that accompanies the card.

For instructions on installing Network Monitor Agent, see "Installing the Network Monitor Agent" in Performance Monitor Help.

Using Performance Monitor with TCP/IP Services

When Transmission Control Protocol/Internet Protocol (TCP/IP) services are installed, performance objects are added for all elements of the TCP/IP protocol suite. The following table describes the performance objects for each element.

TCP/IP Object Type	Description
FTP Server	The File Transfer Protocol (FTP) Server connection and files transfer statistics.
ICMP	The send and receive rates of Internet Control Message Protocol (ICMP) messages. The counters also describe various error counts for the ICMP protocol.

(continued)

TCP/IP Object Type	Description
IP	The send and receive rates of Internet Protocol (IP) datagrams. The counters also describe various error counts for the IP protocol.
Network Interface	The send and receive rates of bytes and packets over a Network TCP/IP connection.
TCP	The send and receive rates of Transmission Control Protocol (TCP) segments. In addition, these counters describe the number of TCP connections in each of the possible TCP connection states.
UDP	The send and receive rates of User Datagram Protocol (UDP) datagrams. These counters also describe various error counts for the UDP protocol.
WINS Server	The rates at which Windows Internet Name Service (WINS) queries, conflicts, renewals, registrations, and releases occur.

To view counters specific to TCP/IP processes, select the appropriate object in the **Add To Chart** dialog box in Performance Monitor. For information about specific performance counters, click **Explain.**

Important To use TCP/IP performance counters in Performance Monitor, you must install the Simple Network Management (SNMP) service. The FTP Server, DHCP Server, WINS Server, and DNS Server performance objects are available only when you install both the service and the SNMP service. For more information on installing SNMP, see "Installing SNMP Service" in Help.

The FTP Server and WINS Server performance counters are cleared each time you start and stop the respective service.

Summary of Counters to Watch

The threshold values of your particular system depend on many factors:

- Network infrastructure and topology
- Server use (application or a file and print services)
- Resource use (computational operation or disk I/O operations)

Counter values that exceed the following guideline thresholds can indicate a performance problem:

Object	Counter	Threshold
Processor	% Processor Time	85%
Server	Sessions Errored Out[1]	5
	Work Item Shortages	3
	Pool Paged Peak	Amount of physical RAM
LogicalDisk	% Free Space	85%
	% Disk Time	90%
Paging File	% Usage[2]	99%
Redirector	Network Errors/sec[1,3]	5 per second
	Reads Denied/sec	5 per second
	Writes Denied/sec	5 per second
	Server Sessions Hung	5
	Current Commands	Number of NICs installed plus 2
Physical Disk	Current Disk Queue Length[4]	Number of spindles plus 2
Server Work Queues	Queue Length[4]	4
System	Processor Queue Length[4]	2

[1] To reset this counter, you must restart the server.

[2] There is other information stored in the paged file that can make this counter difficult to interpret.

[3] Generally indicates problems with the redirector that the server is trying to communicate with, not the computer you are monitoring.

[4] Observe this counter over several intervals.

Note If you are using a RAID device, the % Disk Time counter can indicate a value greater than 100 percent. If it does, use the Avg. Disk Queue Length counter to determine how many system requests are waiting for disk access.

Solving Performance Problems

As noted earlier, performance problems usually occur because of excessive demand for resources (typically microprocessors, disks, memory, and network components). In addition, resource shortages can occur because:

- Resources are not sharing workloads evenly.
- A resource is malfunctioning.
- An application is monopolizing a particular resource.
- A resource is incorrectly configured.

Because Windows NT Server is a self-tuning system, most performance problems are resolved by correcting one of the problems mentioned in the preceding list.

When a user complains of a performance problem, try to identify which resource is in short supply by examining key performance counters and checking event logs for possible errors. Compare the performance of network and non-network applications to see if you can isolate the source of the problems.

The objects and counters discussed in "Looking for Specific Performance Problems" should allow you to isolate the problem. Once you've identified it (there might be more than one), try to determine whether the resource is just overused, broken, or the victim of a badly written application. Take a careful look at the sources of system activity: Which processes are most active? Is one application or thread monopolizing the resource?

If you cannot solve the performance problem by changing resource use, you might be able to correct the problem by tuning Windows NT Server. If you believe you need to add or upgrade your hardware to correct a performance problem, see "Improving Performance by Upgrading Hardware" later in this chapter.

Tuning Windows NT Server Settings

An obvious way to solve performance problems is to add more resources. This method is often an unsatisfactory solution, however, because it is expensive and might not fix your problems. Before adding memory or disk drives, experiment with the following alternatives:

- Create multiple paging files—one for each physical disk and controller on a system. Spreading paging files across multiple disk drives and controllers improves paging performance because each disk can issue I/O commands concurrently. If you have two disks and one paging file, put Windows NT system files on one disk and your paging file on the other. Use the System option in Control Panel to create new paging files.

- Determine the correct size for your paging file. In response to paging activity, Windows NT Server expands paging file size to a user-specified maximum size (set through the System option in Control Panel). However, it is better to make sure initial paging file size matches system application requirements. Forcing Windows NT Server to expand file size slows the start of applications and fragments the disk.
- Run memory-intensive applications at times when the system is not busy, or run them on your highest-performance computers.
- Make sure the load on network servers is balanced. Distribute applications among servers until each computer displays reasonably equivalent values for the counters listed in the preceding table.
- Configure your network so that systems shared by the same group of people are on the same subnetwork.
- On servers, use Disk Administrator to create stripe sets on multiple disks. This solution increases throughput because I/O commands can be issued concurrently.
- Unbind infrequently used network cards by clicking the **Bindings** tab in the Network option in Control Panel.
- If there are no wide area network (WAN) links in the network, and if there is no need to connect to any devices other than computers running Windows NT Server, equip your servers with a small, fast protocol such as NetBEUI. If you need WAN internet capability, add the TCP/IP protocol. With both stacks supported on all servers, you can benefit from NetBEUI performance when connecting to local computers and still be able to connect over WANs to other networks. You can install additional protocols using the Network option in Control Panel.
- If you are using more than one protocol, you can set the order in which the Workstation and NetBIOS software bind to each protocol (you can find the list order by choosing the **Bindings** button in the Network option in Control Panel). You can change the list order for one of the following reasons:
  - If the protocol you use most frequently is first in the binding list, average connection time decreases.
  - Some protocols are faster than others for certain network topologies. Putting the faster protocol first in the bindings list improves performance.

Note There is no reason to reorder Server bindings because the Server accepts incoming connections on the basis of the protocol chosen by the client computer.

- Configure server memory settings to match network activity. This step is discussed in more detail in the following section, "Tuning Memory Settings."

For tuning suggestions related to the TCP/IP protocol and other supported protocols, see the *Windows NT Server Networking Supplement.*

Tuning Memory Settings

You can increase network responsiveness by tuning the memory Windows NT Server allocates for server operations. Memory settings are changed using the Network option in Control Panel.

Four memory settings are available:

- Minimize Memory Used

  Allows memory to be allocated for up to approximately 10 network connections.
- Balance

  Provides memory for up to approximately 64 connections (default).
- Maximize Throughput for File Sharing

  Allocates maximum memory for file sharing operations.
- Maximize Throughput for Network Applications

  Optimizes server memory for distributed applications that do their own memory caching, such as Microsoft SQL Server.

Consider changing memory settings if network interactions seem slow or if entries in a computer's system event log indicate that there is not enough memory for network operations. If physical memory is abundant, there is little penalty for increasing the amount of memory available for network operations. However, if physical memory is limited, such memory allocation can diminish overall system performance. Unlike user applications, which use a portion of memory that can be temporarily transferred to disk, network operations generally use *nonpaged memory*. The more nonpaged memory allocated to the network, the more such memory becomes scarce for the operating system and other processes that require it.

Improving Performance by Upgrading Hardware

If you isolate the source of a performance problem but cannot resolve it with one of the previously mentioned configuration changes, you might be able to improve performance by adding or upgrading hardware.

- Make sure you have enough memory. Depending on the size of your network, server memory requirements range from 16 MB on up.
- Install faster hard disks or disk controllers (or both).
- Install a high-performance network adapter card in the server. If your server uses an 8-bit adapter card, you can significantly increase performance by replacing it with a high-performance 16-bit or 32-bit card.
- Use multiple network adapter cards. Windows NT Server supports multiple adapter cards for a given protocol and multiple protocols for a given card. Although this configuration can create distinct networks that cannot communicate with one another, it is a way to increase file-sharing throughput.

Planning for Additional Resources

Unanticipated network growth can result in overused resources and poor levels of network service. By characterizing system performance over time, you can justify the need for new resources before you get into a panic situation.

Capacity planning starts with daily measurement tracking. Initially, you might log at five-minute intervals throughout the day and then relog the files with the intervals increased to 15 minutes and the time window focused on the most active two hours of the days. Append these two hours' worth of information to an ongoing archive log you created.

Tracking the measurements in the following list provides a good starting point for resource planning.

Object type	Counter
Processor	% Processor Time, Interrupts /sec
System	File Read/write operations/sec
Memory	Pages/sec, Available Bytes
Server	Bytes Total/sec
Physical Disk	% Disk Time, Avg. Disk sec/Transfer
Logical Disk	% Free Space

For more information on relogging log files, see "Working With Log Files," later in this chapter.

Running Performance Monitor

No matter which view you select—Chart, Alert, Report, or Log—there is a standard approach to accessing and working with information. From either your computer or another computer on the network that is running Network Monitor Agent, you can:

- Delete either a full screen of information or a selected counter.
- Update the display manually, set the automatic updating frequency, or switch to only manual updates.
- Select the automatic updating frequency.
- Press ALT+PRINTSCREEN to capture a graphical view of the current window.

- Use the **Export** command to save the data in a tab-delimited (.tsv) or comma-delimited (.csv) text file so that you can manipulate the data in a spreadsheet or database program.

Note The time-interval settings affect the amount of memory and processor time used by Performance Monitor. Monitoring is a burden on processor time or memory only if you retrieve a lot of data very frequently from a large number of computers.

For information on	See this topic in Performance Monitor Help
Exporting data to a spreadsheet or database program	Exporting Data
Printing a snapshot of the window display	Printing a Snapshot of the Window Display
Updating the screen in any view and changing the updating method within each view	Updating the Display
Clearing the values displayed on the screen and deleting a selection	Clearing the Display vs. Deleting Selections

Charting Current Activity

Customized charts that monitor the current performance of selected counters and instances are useful when:

- Investigating why a computer or application is slow or inefficient
- Continuously monitoring systems to find intermittent performance problems
- Discovering why you need to increase capacity

For information on using the chart view, opening an existing chart settings file, and creating a new blank chart, see "Working with Charts" in Performance Monitor Help.

Adding Counters to a Chart

Different problems require different settings. Creating charts to reflect these different requirements is a simple matter of selecting the computer to be monitored and adding the appropriate objects, counters, and instances. You can then save these *selections* under a file name for viewing whenever you want an update on their performance.

To enhance the readability of graphs, vary the scale of the displayed information and the color, width, and style of the line for each counter as you add it to the chart. You can also modify these properties after you add a selection.

The following table shows which options can be changed by editing the chart line

To	Select an option under
Use colors to reflect your personal preferences	Color
Change the scale at which the information is displayed	Scale
Make the line thicker or thinner	Width
Use a different style with a thin line	Style

You can change the scale at which you graph the counter information to display the activity more in the center of the chart. The scale factor is applied to all currently selected counters. The factor displayed is multiplied by the counter value, and the product is charted. However, the value bar continues to show the actual value, not the scaled value.

Performance Monitor also has a *chart-highlighting feature* that enhances the visibility of a selected counter by changing its on-screen color to white. To select and clear this feature, press CTRL+H.

For information on adding selections to a chart and saving chart selections in a settings file, see "Adding Chart Selections" in Performance Monitor Help.

For information on changing how a selected counter is represented on the chart, see "Changing Chart Selections" in Performance Monitor Help.

Using Chart Options

Using Chart Options, you can customize your charts and change the method used for updating the chart values. Click **Chart** on the **Options** menu, or click the **Options** button on the toolbar to see the **Chart Options** dialog box. In this dialog box, you can:

- Specify whether to display or hide horizontal and vertical grid lines, vertical labels, the value bar, and the legend and legend-information area.
- Change the vertical maximum value of the displayed graph labels and the time interval used for graphing the information from the counters. (The selected graph-time interval is reflected in the value bar, which also displays the last, average, minimum, and maximum values for the data visible in the chart.)
- Change the display from a graph format to a histogram bar-type representation (useful for viewing the simultaneous behavior of many instances of the same object).

For information on how to change chart options, see "Changing the Chart Options" in Performance Monitor Help.

Setting Alerts on Current Activity

The Alert View enables you to continue working while Performance Monitor tracks events and notifies you as requested. Use it to create an alert log that monitors the current performance of selected counters and instances for objects on Windows NT Server.

With the alert log, you can monitor several counters at the same time. When a counter exceeds a given value, the date and time of the event are recorded in the Alert view. One thousand events are recorded, after which the oldest event is discarded when the next new one is added. An event can also generate a network alert. When an event occurs, you can have a specified program run every time or just the first time that it occurs.

For specific instructions on using the Alert view, opening and existing alert log settings file, and creating a new blank alert log file, see "Working with Alerts" in Performance Monitor Help.

Adding Counters in the Alert View

You can create alert logs to warn yourself about problems in different situations. You can then save these selections under a file name and reuse them when you want to see if the problems have been fixed.

Adding counters in alert view is similar to adding counters in other views. However, when you set an alert, you specify under what conditions an alert is logged by selecting alert logging if any counter is over or under a value you specify. You can also have Performance Monitor run a program either the first time or every time the alert is logged.

Note When you configure Performance Monitor to run a program when an alert occurs, the program might not work properly or error messages can appear. This problem occurs because Performance Monitor passes the Alert condition as a parameter to the program. If a program run from Performance Monitor does not work properly, create a one-line batch file that runs the program, and call the batch file from Performance Monitor.

When Performance Monitor is logging alerts, a list of your selections appears in the **Alert Legend** box at the bottom of the window. Performance Monitor displays the resulting alerts in the **Alert Log** box.

If an alert occurs while you are not using the Alert view, an alert symbol appears in the status bar showing the number of alerts that have occurred since you were last in the Alert view.

When a remote computer that is being monitored shuts down, an alert occurs and creates a comment in the alert log. Another alert occurs (with another corresponding comment) when that computer later reconnects.

For information on adding selections to an alert log and saving alert log selections in a settings file, see "Adding Alert Selections" in Performance Monitor Help.

For information on how to change the way a selected counter is represented in the alert log or update alert log selections that have been saved in a settings file, see "Changing Alert Selections" in Performance Monitor Help.

Using Alert Options

Choosing the **Alert** command on the **View** menu enables you to specify not only the alert interval but also the alert method. Specify one or all of the following:

- Switch to the Alert view
- Log the event in the Event Viewer Application log
- Send a network alert message to yourself or someone else

Note To send a network alert message to yourself or someone else, the Messenger service must already be started and the network name defined on the recipient's computer.

For information on how to change alert options, see "Changing the Alert Options" in Performance Monitor Help. For more information on starting the Messenger service or adding a network name, type **net start messenger /?** and **net name /?**.

Creating Reports

The Report view lets you display constantly changing counter and instance values for selected objects. Values appear in columns for each instance. You can adjust report intervals, print snapshots, and export data.

For information on using the Report view, opening an existing report settings file, or creating a new blank report file, see "Working with Reports" in Performance Monitor Help.

Using Report Selections and Options

Creating reports using current activity can help you gain a better understanding of object behavior:

- Create a report on all the counters for a given object, and then watch them change under various loads.

- Create reports to reflect the same information that you are charting or to monitor other specific situations. Then save these selections under a file name, and reuse them when you need an update on the same information.

After you add selections to a report, a list of your selections by computer and object appears in the report area. Performance Monitor displays the changing values of your selections in the report.

For information on how to add objects, counters, and instances to a report or to save report selections in a settings file, see "Adding to a Report" in Performance Monitor Help.

For information on how to change the reporting time interval, see "Changing the Report" in Performance Monitor Help.

Logging Current Activity

By *logging,* you record information on the current activity of selected objects and computers for viewing later. You can also collect data from multiple systems into a single *log file,* which contains detailed data for detecting performance problems or other detailed analysis. For capacity planning, you must view trends over a longer period, which requires the capability to create a log file and to produce reports from that file. For example, create different logs to accumulate information on the performance of selected objects on various computers to be studied later. Save these selections under a file name, and reuse them when you want to create another log of the same type of information for comparison.

Setting Logging Options

The Log view has a display area for listing objects and the corresponding computers you selected with the **Add To Log** command on the **Edit** menu. All counters and instances are logged for a selected object.

Clicking the **Log** command on the **Options** menu enables you to start or stop logging and to change the method used for updating the log values.

The Log view displays a list of objects and computers along with the current file size. You can specify the following in the **Log Options** dialog box:

- Complete path and name of the log file.
- Log Interval in seconds, from 1 to 3600 seconds (1 hour).
- Status, either Collecting or Closed.

After you start logging, a log symbol with the changing total file size appears on the right side of the status bar and remains there in all four views.

When a remote computer from which you are logging data shuts down, a bookmark comment is added to the log file. Another bookmark comment is added when that computer later reconnects and logging starts again.

For information on how to change log options or start or stop logging, see "Working with Information from Log Files" in Performance Monitor Help.

For information on adding selections for logging or saving your log selection settings, see "Adding to a Log" in Performance Monitor Help.

Adding Bookmarks

Log files become more usable when you add *bookmarks* at various points while logging. With bookmarks, you can highlight major points of interest or describe the circumstances under which the file was created. You can then easily return to these locations when you work with the log file. The **Bookmark** command becomes available when you start logging.

To add a bookmark, click **Bookmark** on the **Options** menu or the **Bookmark** button on the toolbar.

Working with Input from Log Files

Log files can provide a wealth of information for troubleshooting or planning. Whereas charting, setting alerts, and creating reports on current activity provide instant feedback, working with log files enables you to track counters over a long period of time, allowing you to examine information more thoroughly, and document system performance.

The fundamental approach to analyzing data is the same, whether your data source is current activity or a log file. You can still create charts, set alerts, and create reports. However, you can also move around in a log file (that is, change the start and stop times) by clicking the **Time Window** command on the view's **Edit** menu. The times selected apply to all four views. After you open a log file, the **Time Window** command on the **Edit** menu is available. The time window enables you to use the following methods to specify how much information you want to display:

- Change the starting and stopping points by moving the corresponding end of the time interval slide bar. This method is the easiest way to adjust the time interval if you don't have bookmarks set in your log for the purpose of adjusting the time window.

- Use bookmarks as starting or stopping points.

For information on	See this topic in Performance Monitor Help
Selecting an existing log file	Selecting an Existing Log File
Charting an input log file	Working with Information from Log Files
Setting alerts on an input log file	Setting Alerts on Input Log Files
Creating a report from an input log file	Reporting Based on Input Log Files
Moving around in a log file	Changing the Time Window

Relogging Input Log Files

When your data source is an existing log file, you can relog the data to another log file or to the same log file. By changing certain options when relogging, you can significantly condense large log files.

You can relog with a longer time interval either all or only selected objects in an existing log file. You can also change the start and stop times and relog only the data within that time frame.

When you direct output to an existing log file, the output is appended to the end of the file. You can use this feature to create a single archive file to manage your log files. For example, if you collected data at a one-minute interval and relogged it at a five-minute interval, you condense your data to use only 20 percent of the disk space.

Note To enable the **Relog File** button, you must first provide a file name and select objects to log.

For information on how to relog an input log file, see "Relogging Input Log Files" in Performance Monitor Help.

Enabling Windows NT Event Error Logging

To log Performance Monitor errors to the Event Viewer Application log, use the Registry Editor to create or assign the following registry key value:

Subtree	HKEY_CURRENT_USER
Key	\Software\Microsoft\PerfMon
Name	ReportEventsToEventLog
Type	REG_DWORD
Value	1

The change takes effect the next time Performance Monitor is started. You can update the Emergency Repair Disk to reflect these changes.

If ReportEventsToEventLog is set to 1 (the default is 0), Performance Monitor logs an error in the application event log every time it receives a counter value that is inconsistent or in error. For example, when Performance Monitor truncates a value to 0 or 100, it logs an event. The Performance Monitor events can be used to explain unexpected counter values.

For information on how to enable error logging, see "Enabling Windows NT Event Error Logging" in Performance Monitor Help.

CHAPTER 9

Monitoring Events

An *event* is any significant occurrence in the system (or in an application) that requires users to be notified. Some critical events, such as a full disk drive or an interrupted power supply, are noted in an on-screen message. Those events not requiring immediate attention are noted in an *event log*. Event logging starts automatically each time you start Windows NT Server. With an event log and a tool called *Event Viewer*, you can troubleshoot various hardware and software problems and monitor Windows NT Server security events. You can also archive logs in various file formats.

Overview

Windows NT Server records events in three kinds of logs:

- The *system log* contains events logged by the Windows NT Server system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows NT Server.
- The *security log* can contain valid and invalid logon attempts as well as events related to resource use, such as creating, opening, or deleting files or other objects. For example, if you use User Manager for Domains to enable logon and logoff auditing, attempts to log on to the system are recorded in the security log.
- The *application log* contains events logged by applications. For example, a database program might record a file error in the application log. Application developers decide which events to monitor.

System and application logs can be viewed by all users; security logs are accessible only to system administrators.

Enabling Security Logging

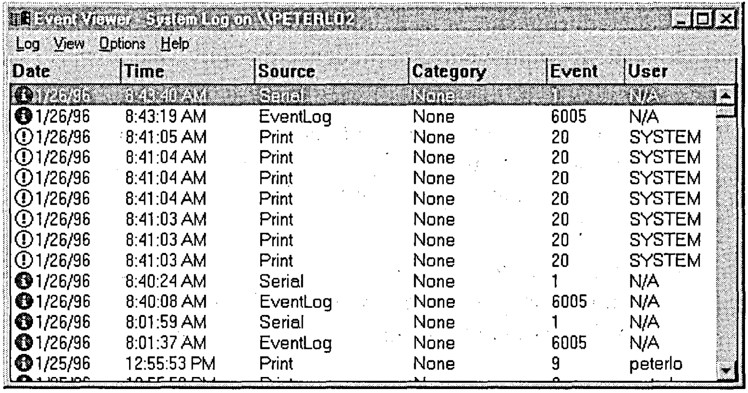
By default, security logging is turned off. To enable security logging, run User Manager for Domains to set the Audit policy. For the security log, the administrator can also set auditing policies in the registry that cause the system to halt when the security log is full. For more information, see "Halting the Computer When the Security Log Is Full" later in this chapter.

Note The *Windows NT Server Resource Kit* includes Crystal Reports Event Log Viewer, a full-featured report writer that provides an easy way to extract, view, save, and publish information from event logs in a variety of formats. For more information on Crystal Reports Event Log Viewer, see Readme.hlp in the \Crystal\Disk1 folder on the *Windows NT Server Resource Kit* 4.0 compact disc.

Interpreting an Event

Event logs consist of a *header*, a *description* of the event (based on the event type), and, optionally *additional data*. Most security log entries consist of the header and a description.

Event Viewer displays events from each log separately. Each line shows information about one event, including date, time, source, event type, category, Event ID, user account, and computer name.



Date	Time	Source	Category	Event	User
1/26/96	8:43:40 AM	Serial	None	1	N/A
1/26/96	8:43:19 AM	EventLog	None	6005	N/A
1/26/96	8:41:05 AM	Print	None	20	SYSTEM
1/26/96	8:41:04 AM	Print	None	20	SYSTEM
1/26/96	8:41:04 AM	Print	None	20	SYSTEM
1/26/96	8:41:04 AM	Print	None	20	SYSTEM
1/26/96	8:41:03 AM	Print	None	20	SYSTEM
1/26/96	8:41:03 AM	Print	None	20	SYSTEM
1/26/96	8:41:03 AM	Print	None	20	SYSTEM
1/26/96	8:40:24 AM	Serial	None	1	N/A
1/26/96	8:40:08 AM	EventLog	None	6005	N/A
1/26/96	8:01:59 AM	Serial	None	1	N/A
1/26/96	8:01:37 AM	EventLog	None	6005	N/A
1/25/96	12:55:53 PM	Print	None	9	peterlo

For more information about Windows NT Server events, see the Messages Database Help file on the *Windows NT Server Resource Kit* 4.0 compact disc.

The Event Header

The event header contains the following information.

Information	Meaning
Date	The date the event occurred.
Time	The (local) time the event occurred.
User	The username of the user on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process, or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. (Impersonation occurs when Windows NT Server allows one process to take on the security attributes of another.)
Computer	The name of the computer where the event occurred. The computer name is usually your own, unless you are viewing an event log on another Windows NT computer.
Event ID	A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems.
Source	The software that logged the event, which can be either an application name, such as "SQL Server," or a component of the system or of a large application, such as a driver name. For example, "Elnkii" indicates the EtherLink II driver.
Type	A classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log. In Event Viewer's normal list view, these are represented by a symbol.
Category	A classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in the **User Manager for Domains Audit Policy** dialog box.

Event Description

The format and contents of the event description vary, depending on the *event type.* The description is often the most useful piece of information, indicating what happened or the significance of the event.

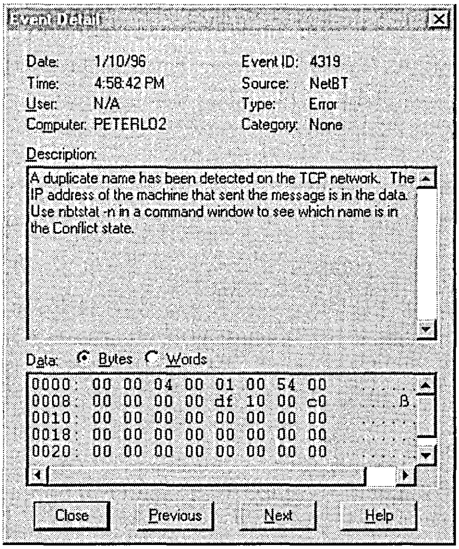
Event Types

The symbol on the left side of the Event Viewer screen indicates the event type:

Symbol	Event Type	Meaning
🛑	Error	Significant problems, such as a loss of data or loss of functions. For example, an Error event might be logged if a service was not loaded during Windows NT Server startup.
ⓘ	Warning	Events that are not necessarily significant but that indicate possible future problems. For example, a Warning event might be logged when disk space is low.
ℹ	Information	Infrequent significant events that describe successful operations of major server services. For example, when a database program loads successfully, it might log an Information event.
🔒	Success Audit	Audited security access attempts that were successful. For example, a user's successful attempt to log on to the system might be logged as a Success Audit event.
🔑	Failure Audit	Audited security access attempts that failed. For example, if a user tried to access a network drive and failed, the attempt might be logged as a Failure Audit event.

Additional Data

The optional data field, if used, contains binary data, which can be displayed in bytes or words. This information is generated by the application that was the source of the event record. Because the data appears in hexadecimal format, its meaning can be interpreted only by a support technician familiar with the source application.



Date:	1/10/96	Event ID:	4319
Time:	4:58:42 PM	Source:	NetBT
User:	N/A	Type:	Error
Computer:	PETERL02	Category:	None

Description:

A duplicate name has been detected on the TCP network. The IP address of the machine that sent the message is in the data. Use nbtstat -n in a command window to see which name is in the Conflict state.

Data: ● Bytes ○ Words

```
0000: 00 00 04 00 01 00 54 00   ......
0008: 00 00 00 00 df 10 00 c0   ....ß.
0010: 00 00 00 00 00 00 00 00   ......
0018: 00 00 00 00 00 00 00 00   ......
0020: 00 00 00 00 00 00 00 00   ......
```

When viewing an error log on a LAN Manager 2.*x* server, only the date, time, source, and event ID are shown. When viewing an audit log on a LAN Manager 2.*x* server, only the date, time, category, user, and computer are shown.

Using Event Viewer

You determine which event log to view by switching between the system, security, and application logs. You can also use Event Viewer to view logs on other computers.

Selecting a Log

Use the **Log** menu to select a log for event viewing. Although the system log of the local computer appears the first time you start Event Viewer, you can choose to view the security or application log.

Selecting a Computer

When you first start Event Viewer, the events for the local computer appear.

To view events for another computer, click **Select Computer** on the **Log** menu. (It can be a Windows NT Workstation computer, a server or domain controller running Windows NT Server, or a LAN Manager 2.*x* server.)

If the computer you select is across a link with slow transmission rates, select **Low Speed Connection**. If this option is selected, Windows NT Server does not list all the computers in the default domain, thereby minimizing network traffic across the link. (If slow transmission rates are commonplace, click **Low Speed Connection** on the **Options** menu.)

If you select a LAN Manager 2.*x* server for viewing, Event Viewer can display its error (system) log and its audit (security) log.

For information on how to select a computer for event viewing, see "Select Computer" in Event Viewer Help.

Refreshing the View

When you first open a log file, Event Viewer displays the current information for that log. This information is not updated automatically. To see the latest events and to remove overwritten entries, choose the **Refresh** command.

For more information , see "Refresh" in Event Viewer Help.

Changing the Font

You can change the font used in Event Viewer. Changing this font affects only the display of the list of events in the main Event Viewer window.

For more information, see "Changing the Font Selection" in Event Viewer Help.

Viewing Specific Logged Events

After you select a log to view in Event Viewer, you can:

- View descriptions and additional details that the event source logs.
- Sort events from oldest to newest or from newest to oldest.
- Filter events so that only events with specific characteristics are displayed.
- Search for events based on specific characteristics or event descriptions.

Viewing Details About Events

For many events, you can view more information than is displayed in Event Viewer by double-clicking the event.

The **Event Detail** dialog box shows a text description of the selected event and any available binary data for the selected event. This information is generated by the application that was the source of the event record. Because the data appears in hexadecimal format, its meaning can be interpreted only by a support technician familiar with the source application. Not all events generate such data. For more information , see "Viewing Event Details" in Event Viewer Help.

To control the types of security events that are audited, click **Audit** on the **Policies** menu in User Manager for Domains. To control the auditing of file and folders access, click **Auditing** on the **Security** tab in the **Windows NT Explorer Properties** dialog box. For more information, see "Monitoring Windows NT Security Events" later in this chapter.

Sorting Events

By default, Event Viewer lists events by date and time of occurrence from the newest event to the oldest. To change the order from oldest to newest, click **Oldest First** on the **View** menu. If the **Save Settings On Exit** command on the **Options** menu is checked when you quit, the current sort order is used the next time you start Event Viewer.

When a log is archived, the sort order affects the order in which event records are archived in a text format or comma-delimited text format file; sort order does not affect the order of event records archived in log file format. For more information, see "Using Archived Log Files" later in this chapter.

For information on how to specify the sort order, see "Sorting Events" in Event Viewer Help.

Filtering Events

By default, Event Viewer lists all events recorded in the selected log. To view a subset of events that have specific characteristics, click **Filter Events** on the **View** menu. When filtering is on, a check mark appears by the **Filter** command on the **View** menu and "(Filtered)" appears on the title bar. If **Save Settings On Exit** on the **Options** menu is checked when you quit Event Viewer, the filters remain in effect the next time you start Event Viewer.

Filtering has no effect on the actual contents of the log: It changes only the view. All events are logged continuously, whether the filter is active or not. If you archive a log from a filtered view, all records are saved, even if you select a text format or comma-delimited text format file. For more information on archiving, see "Using Event Viewer with Archived Log Files" later in this chapter.

The following table describes the options available in the **Filter** dialog box.

Use	To filter for
View From	Events after a specific date and time. By default, this is the date of the first event in the log file.
View Through	Events up to and including a specific date and time. By default, this is the date of the last event in the log file.
Information[1]	Infrequent significant events that describe successful operations of major server services. For example, when a database program loads successfully, it might log an Information event.
Warning[1]	Events that are not necessarily significant but that indicate possible future problems. For example, a Warning event might be logged when disk space is low.
Error[1]	Significant problems, such as a loss of data or loss of functions. For example, an Error event might be logged if a service was not loaded during Windows NT Server startup.
Success Audit[1]	Audited security access attempts that were successful. For example, a user's successful attempt to log on to the system might be logged as a Success Audit event.
Failure Audit[1]	Audited security access attempts that failed. For example, if a user tried to access a network drive and failed, the attempt might be logged as a Failure Audit event.
Source[2]	A source for logging events, such as an application, a system component, or a driver.
Category[3]	A classification of events defined by the source. For example, the security event categories are Logon and Logoff, Policy Change, Privilege Use, System Event, Object Access, Detailed Tracking, and Account Management.
User[3]	A specific user that matches an actual user name. This field is not case sensitive.
Computer[3]	A specific computer that matches an actual computer name. This field is not case sensitive.
Event ID[2]	A specific number that corresponds to an actual event.

[1] This option is not available for LAN Manager 2.*x* servers.

[2] This option is not available for audit logs on LAN Manager 2.*x* servers.

[3] This option is not available for error logs on LAN Manager 2.*x* servers.

For information on how to filter for events and turn off filtering of events, see "Filtering Events" in Event Viewer Help.

For information on how to return to the default criteria, see "Reset to Default Settings" in Event Viewer Help.

Searching for Events

To search for events that match a specific type, source, or category, click **Find** on the **View** menu. Searches can be useful when you are viewing large logs: For example, you can search for all Warning events related to a specific application, or search for all Error events from all sources.

Your choices in the **Find** dialog box are in effect throughout the current session. If **Save Settings On Exit** on the Event Viewer **Options** menu is checked when you quit, the current filter settings are available the next time you start Event Viewer.

For more information, see "Searching for Events" in Event Viewer Help.

Setting Options for Logging Events

Logging starts automatically when you start the computer. Logging stops when an event log becomes full and cannot overwrite itself—either because you've set it for manual clearing or because the first event in the log is not old enough.

Use the **Log Settings** command on the **Log** menu to define logging parameters for each kind of log. You can set the maximum size of the log and specify whether the events are overwritten or stored for a certain period of time.

The **Event Log Wrapping** option lets you define how events are retained in the log selected in the **Change Settings For** dialog box. (The default logging policy is to overwrite logs as needed, provided events are at least seven days old.) You can customize this policy for different logs.

The options include the following.

Use	To
Overwrite Events As Needed	Have new events continue to be written when the log is full. Each new event replaces the oldest event in the log. This option is a good choice for low-maintenance systems.
Overwrite Events Older Than [ ] days	Retain the log for the number of days you specify before overwriting events. The default is 7 days. This option is the best choice if you want to archive log files weekly. This strategy minimizes the chance of losing important log entries and at the same time keeps log sizes reasonable.
Do Not Overwrite Events	Clear the log manually rather than automatically. Select this option only if you cannot afford to miss an event, for example, for the security log at a site where security is extremely important.

Note When a log is full (when no more events can be logged), you can free the log by clearing it. Reducing the amount of time you keep an event also frees the log if it allows the next record to be overwritten.

For information on how to set the Audit policy, see "To manage the Audit Policy" in User Manager for Domains Help.

For information on how to clear a log, see "Clearing All Events" in Event Viewer Help.

Although you can increase (to the capacity of the disk and memory) or decrease the maximum log size, each log file has an initial maximum size of 512K. Before decreasing a log's size, you must clear the log.

Using Event Logs to Troubleshoot Problems

Careful monitoring of event logs can help you predict and identify the sources of system problems. For example, if log warnings show that a disk driver can only read or write to a sector after several retries, the sector will likely go bad eventually. Logs can also confirm problems with application software: If an application crashes, an application event log can provide a record of activity leading up to the event.

The following are suggestions to help you use event logs to diagnose problems:

- Archive logs in log format. The binary data associated with an event is discarded if you archive data in text or comma-delimited format.
- If you suspect a hardware component is the origin of system problems, filter the system log to show only those events generated by the component.
- If a particular event seems related to system problems, try searching the event log to find other instances of the same event or to judge the frequency of an error.
- Note Event IDs. These numbers match a text description in a source message file. This number can be used by product-support representatives to understand what occurred in the system.

Monitoring Windows NT Security Events

You enable auditing from the **User Manager for Domains Auditing Policy** dialog box. Through auditing, you can track Windows NT Server security events. You can specify that an audit entry is to be written to the security event log whenever certain actions are performed or files are accessed. The audit entry shows the action performed, the user who performed it, and the date and time of the action. You can audit both successful and failed attempts at actions, so the audit trail can show who actually performed actions on the network and who tried to perform actions that are not permitted.

Events are not audited by default. If you have Administrator permission, you can specify what types of system events are audited through User Manager for Domains. The Audit policy determines the amount and type of security logging Windows NT Server performs. For file and object access, you can then specify which files and printers to monitor, which types of file and object access to monitor, and for which users or groups. For example, when **File and Object Access** auditing is enabled, you can use the **Security** tab in a file or folder's **Properties** dialog box (accessed through Windows NT Explorer) to specify which files are audited and what type of file access is audited for those files.

Note You can audit file and folder access on only Windows NT File System (NTFS) drives.

Managing the Audit Policy

Windows NT Server 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.

You use the Audit policy to select the types of security events to be audited. When such an event occurs, an entry is added to the computer's security log. The security log can be viewed with Event Viewer.

Because the security log is limited in size, 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 more information on setting the Audit policy, see Chapter 1, "Managing Windows NT Server Domains" and "Managing the Audit Policy" in User Manager for Domains Help.

Auditing File and Folder Access

You can audit the access of files and folders on NTFS volumes to identify who took various types of actions with the files and folders and hold those users accountable for their actions.

When you audit a file or folder, an entry is written to the Windows NT security log whenever the file or folder is accessed in a certain way. You determine which files and folders to audit, whose actions to audit, and exactly what types of actions are audited.

To set auditing on a file or folder, use User Manager for Domains to enable auditing of File and Object Access, and then use Windows NT Explorer to specify which files to audit and which type of file access events to audit. To view audit entries, use the Event Viewer.

You can audit successful and failed attempts of the following types of directory and file access:

Types of directory access	Types of file access
Displaying names of files in the directory	Displaying the file's data
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file's owner and permissions
Creating subdirectories and files	Changing the file
Going to the directory's subdirectories	Changing file attributes
Displaying the directory's owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory permissions	Changing the file's permissions
Changing directory ownership	Changing the file's ownership

To audit the following activities on a directory, select the events shown.

● Event audits action ○ Event does not audit action	Read	Write	Execute	Delete	Change Permissions	Take Ownership
Displaying filenames	●	○	○	○	○	○
Displaying attributes	●	○	●	○	○	○
Changing attributes	○	●	○	○	○	○
Creating subdirectories and files	○	●	○	○	○	○
Going to the directory's subdirectories	○	○	●	○	○	○
Displaying owner and permissions	●	●	●	○	○	○
Deleting the directory	○	○	○	●	○	○
Changing directory permissions	○	○	○	○	●	○
Changing directory ownership	○	○	○	○	○	●

To audit the following activities on a file, select the events shown.

● Event audits action ○ Event does not audit action	Read	Write	Execute	Delete	Change Permissions	Take Ownership
Displaying the file's data	●	○	○	○	○	○
Displaying attributes	●	○	●	○	○	○
Displaying the file's owner and permissions	●	●	●	○	○	○
Changing data	○	●	○	○	○	○
Changing attributes	○	●	○	○	○	○
Running the file	○	○	●	○	○	○
Deleting the file	○	○	○	●	○	○
Changing the file's permissions	○	○	○	○	●	○
Changing the file's ownership	○	○	○	○	○	●

Note To audit files and directories, you must be logged on as a member of the Administrators group.

For more information on setting the audit policy for printers, see Chapter 5, "Setting Up Print Servers."

Halting the Computer When the Security Log is Full

If you have set the security log either to "Overwrite Events Older than *n* Days" or "Do Not Overwrite Events (Clear Log Manually)", you can prevent auditable activities while the log is full. No new audit records can be written. To do so, use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Value:	1

The changes take effect the next time the computer is started. You can update the Emergency Repair Disk to reflect these changes.

If Windows NT Server halts as a result of a full security log, the system must be restarted and reconfigured to prevent auditable activities from occurring again while the log is full. After the system is restarted, only administrators can log on until the security log is cleared. For more information on recovering after Windows NT halts, see the "Recovering After Windows NT Halts Because it Cannot Generate an Audit Event Record" in Event Viewer Help.

Using Event Viewer with Archived Log Files

You can archive an event log in log-file format so that you can reopen it in Event Viewer later. Or the log can be saved in text format or comma-delimited text format so that you can use the archived information in other applications.

For example, you can archive security logs so that you can monitor security events over a period of time. Or you can archive application logs so that you can track the Warning and Error events that occur for specific applications.

When you archive a log file, the entire log is saved, regardless of any filtering options specified in Event Viewer. If you changed the sort order in Event Viewer, event records are saved exactly as displayed if you archive the log in a text or comma-delimited text file.

Archiving a Log

When you archive an event log, you save it in one of three file formats:

- *Log file format*, which enables you to view the archived log again in Event Viewer.
- *Text file format*, which enables you to use the information in an application, such as a word processor.
- *Comma-delimited text file format*, which enables you to use the information in an application, such as a spreadsheet or a flat-file database.

The binary event data is saved if you archive a log in log file format, but it is discarded if you archive the log in text file format or in comma-delimited text file format. The event description is saved in all archived logs. When you archive a sorted log, the sort order affects the order in which event records are archived in a text file format or comma-delimited text file format. However, sort order does not affect the order of event records in a log archived in log file format. In either case, the sequence of data within each individual event record is record in the following order:

1. Date[1]
2. Time
3. Source
4. Type
5. Category
6. Event
7. User
8. Computer
9. Description

[1] Depends on the sort order specified on the **View** menu.

Archival has no effect on the current contents of the active log. To clear the original log, you must click **Clear All Events** on the **Log** menu. To remove an archived log file, delete the file as you would other kinds of files.

For information on how to archive an event log, see "Archiving Event Logs" in Event Viewer Help.

Viewing a Log Archived in Log File Format

You can view an archived file in Event Viewer *only* if the log was saved in event log-file format. You cannot click the **Refresh** or **Clear All Events** commands to update the display or to clear an archived log.

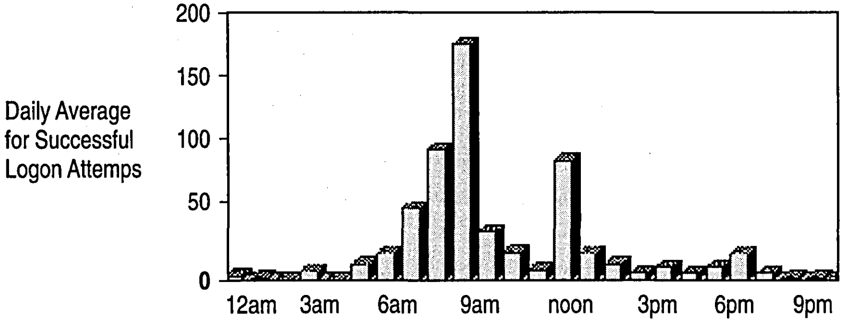
Note If you do not specify the correct log type (application, security, or system), the Description displayed for the archived log in the **Event Detail** dialog box will not be correct.

For information on how to display an archived log in Event Viewer, see "Viewing a Log Archived in Log File Format" in Event Viewer Help.

Using Logs Archived in a Text Format

An event log saved in text- or comma-delimited text format can be opened in other applications. These applications can be used to filter, sort, and format the archived event records. You can also combine event records from two or more archived text files to create reports.

For example, you can copy lines of text from an archived log to include as supporting information in an electronic mail message. Or you can archive a security log in comma-delimited format so that you can place the information in a spreadsheet and produce a chart showing the archived information.



Logon Activity by Time of Day, Engineering Domain, February 1996

CHAPTER 10

Monitoring Your Network

Network administrators can use Microsoft Windows NT Network Monitor to capture and display frames (also called *packets*) to detect and troubleshoot problems on local area networks (LANs). For example, you can use Network Monitor to diagnose hardware and software problems when two or more computers cannot communicate. You can also capture network activity and then send the capture file to professional network analysts or support organizations.

Network application developers can use Network Monitor to monitor and debug network applications as they are developed.

Note To use Network Monitor effectively, you must understand network protocol formats, protocol procedures, and network operating systems. Although that information is beyond the scope of this chapter, it is available from other publishers. For additional resources, see "Network Monitor Guide to Books on Networking" and the "Network Monitor Guide to Reports on Networking" in Network Monitor Help.

Install Network Monitor and the Network Monitor Agent using the **Services** tab of the **Network** option in Control Panel by choosing **Network Monitor Tools** and **Agent**. After you install Network Monitor, you can start it from the **Programs**, **Administrative Tools** (Common) menu on the **Start** button, or from the command line.

Editing and Transmitting Frames

Microsoft Systems Management Server (SMS) also includes a version of Network Monitor. In addition to the functionality described in this chapter, the SMS version can also capture frames sent to or from any computer on the network, edit and transmit frames on the network, and remotely capture frames (for example, over a dial-up network connection) from other computers on the network running Network Monitor Agent (including computers running Windows NT Workstation and Windows 95).

Network Monitor Overview

Network Monitor monitors the network *data stream*, which consists of all information transferred over a network at any given time. Prior to transmission, this information is divided by the network software into smaller pieces, called *frames* or *packets*. Each frame contains the following information:

- The source address of the computer that sent the message
- The destination address of the computer that received the frame
- Headers from each protocol used to send the frame
- The data or a portion of the information being sent

To ensure that security is maintained on your Windows NT network, Windows NT Network Monitor displays only those frames sent to or from your computer, broadcast frames, and multicast frames. For more information, see "Network Monitor Security" later in this chapter

Network Monitor can capture only as much information as fits in available system memory. Fortunately, you usually need to capture only a small subset of the frames traveling on your network. To single out a subset of frames, design a *capture filter*, which functions like a database query. You can filter on the basis of source and destination addresses, protocols, protocol properties, or by specifying a pattern offset. For more information on filters, see "Capture Filters" later in this chapter.

To have a running capture respond to events on your network as soon as they are detected, design a *capture trigger.* A capture trigger performs a specified action, (such as starting an executable file) when Network Monitor detects a particular set of conditions on the network. For more information on triggers, see "Capture Triggers" later in this chapter.

Network Monitor supports dozens of popular protocols, including NetBIOS (NetBEUI), IPX, SPX, and many TCP/IP-related protocols. For a complete list, see "Supported Protocol Parsers" later in this chapter.

After you have captured data (and have optionally saved the data to a capture file), you can view it. Network Monitor does much of the data analysis for you by translating the raw capture data into its logical frame structure. For more information, see "Capturing and Displaying Frames" later in this chapter.

The core functionality of Network Monitor, as described in this chapter, is supported by Microsoft Product Support Services. Network-dependent tasks, such as interpreting data that you capture from your network, are not supported.

For more information on capturing frames, see "Capturing Network Data" later in this chapter.

For more information on displaying previously captured data that has been saved in a capture file, see "Displaying Captured Data" later in this chapter.

Network Monitor Security

For security reasons, Windows NT Network Monitor captures only those frames, including broadcast and multicast frames, sent to or from the local computer. Network Monitor also displays overall network segment statistics for broadcast frames, multicast frames, network utilization, total bytes received per second, and total frames received per second.

Windows NT Network Monitor uses a new network driver interface specification (NDIS) version 4.0 feature to copy all frames it detects to its *capture buffer* (a resizable storage area in memory). The process by which Network Monitor copies frames is referred to as *capturing*.

Note Because Network Monitor uses NDIS 4.0 instead of *promiscuous mode* (where the network adapter card passes on all frames sent on the network), you can use Network Monitor even if your network adapter card does not support promiscuous mode. Networking performance is not affected when you use an NDIS 4.0 driver to capture frames. (Putting the network adapter card in promiscuous mode can put an additional 30 percent or more load on the CPU.)

In addition, to help protect your network from unauthorized use of Network Monitor installations, Network Monitor provides:

- Password protection
- The capability to detect other installations of Network Monitor on the local segment of your network

Setting Capture and Display Passwords

Use the Monitoring Agent icon in the Windows NT Control Panel to change the capture and display passwords for Network Monitor or for the Network Monitor Agent:

- A *capture password* allows the user to capture statistics from the network and to display captured data.
- A *display password* allows the user to open only previously saved capture (.cap) files.

If you installed both Network Monitor and the Network Monitor Agent, the capture and display passwords apply both to Network Monitor and to the installation of the Network Monitor Agent on that computer.

Caution If the Network Monitor Agent is installed on your computer, if the service is running, and if no password is set, anyone using Network Monitor from an Systems Management Server computer can connect to your computer and use it to capture from your network.

Detecting Other Installations of Network Monitor

To protect your network from unauthorized monitoring, Network Monitor can detect other installations of Network Monitor on the local segment of your network. Network Monitor also detects all instances of the Network Monitor Agent being used remotely (by either Network Monitor from SMS or Windows NT Performance Monitor) to capture data on your network.

When Network Monitor detects other Network Monitor installations on the network, it displays the following information about them:

- Name of the computer
- Name of the user logged on at the computer
- State of Network Monitor on the remote computer (Driver Installed, Running, Capturing, or Transmitting)
- Adapter address of the remote computer
- Version number of Network Monitor on the remote computer

Note In some instances, your network architecture might prevent one installation of Network Monitor from detecting another. For example, if an installation is separated from yours by a router that does not forward multicasts, your installation cannot detect that installation.

Network Monitor Help

Network Monitor Help contains procedures to guide you through the tasks relating to the information covered in this chapter. In addition, two types of additional Help are available: Property and Protocol.

Property Help is available from the Detail window when you view a capture. Property Help gives you a quick way to view a protocol command reference when focused on a specific command. Currently, Property Help is available only for the Server Message Block (SMB) protocol.

Protocol Help includes an introduction to and the contents of the SMB protocol specification.

For more information about the Detail window and viewing captures, see "Displaying Captured Data" later in this chapter.

Configuring Network Monitor and the Network Monitor Agent

Use the Network Monitoring Agent option in Control Panel to describe each network card in your computer and to reset the Network Monitor defaults. Resetting Network Monitor defaults resets all Network Monitor settings.

Describing each network card is particularly useful if your computer has multiple network cards or when other people using SMS Network Monitor are using the Network Monitor Agent from your computer. Describing each network card in your computer makes it easier to identify which card you are using to capture or if someone is using the SMS Network Monitor to capture frames from your computer which computer they are using to capture.

For more information, open the Control Panel folder, double-click Monitoring Agent, and click **Help**.

Supported Protocol Parsers

A protocol parser is a dynamic-link library (.DLL) that identifies the protocols used to send a frame onto the network. Information about these protocols appears when you display captured frames in the Frame Viewer window. For each protocol that Network Monitor supports, there is a corresponding parser.

The following is a list of the protocols that Network Monitor supports. The SMS Network Monitor supports additional parsers.

AARP
ADSP
AFP
FINGER
FRAME
FTP
NBT
NCP
NDR
RPC
RPL
RTMP

ARP_RARP
ASP
ATP
BONE
BPDU
BROWSER
CBCP
CCP
DDP
DHCP
DNS
ETHERNET
FDDI
ICMP
IGMP
IP
IPCP
IPX
IPXCP
LAP
LCP
LLC
MSRPC
NBFCP
NBIPX
NBP
NetBIOS
NETLOGON
NFS
NMPI
NSP
NWDP
OSPF
PAP
PPP
PPPCHAP
PPPPAP
RIP
RIPX
SAP
SMB
SMT
SNAP
SPX
TCP
TMAC
TOKENRING
UDP
XNS
ZIP

If you want to capture data sent in a protocol that Network Monitor does not support, use the SMS Network Monitor or add your own parser.

Capturing Network Frames

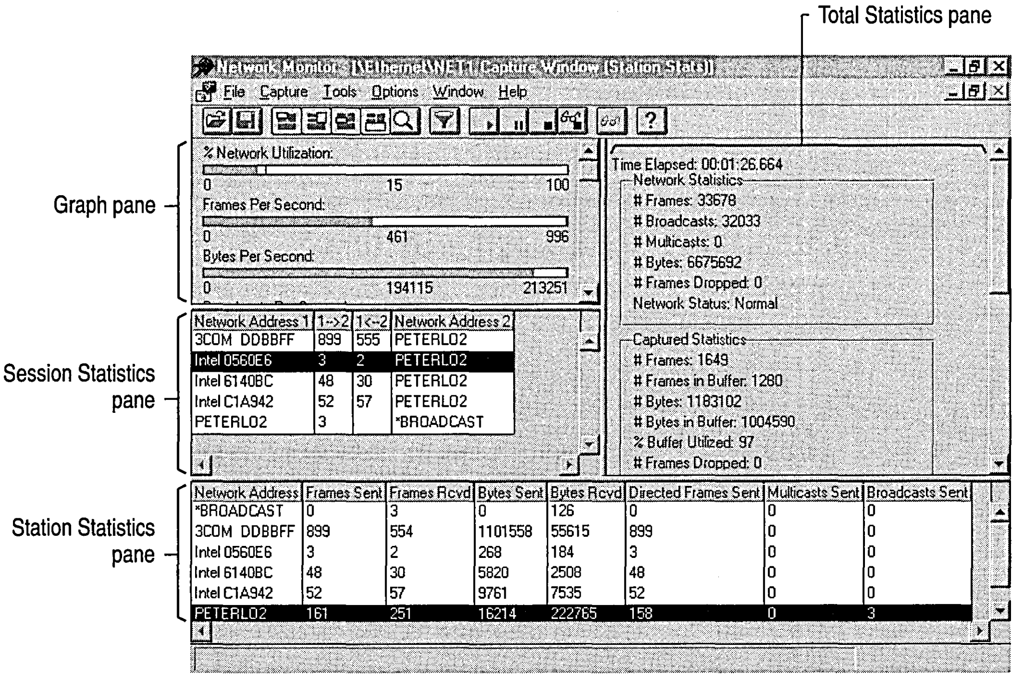
As mentioned earlier, capturing occurs when a network card passes on a subset of the frames that pass over the network to Network Monitor. Network Monitor stores these frames in the *capture buffer*, a sizable region of memory. If the capture buffer overflows, the newest frame added to the buffer, replaces the oldest frame. To prevent the capture buffer from overflowing and to make frame analysis easier use a *capture filter* to capture only those frames that meet criteria you define. To have a running capture respond to events on your network as soon as they are detected, design a *capture trigger*.

This section describes how to:

- Use the Network Monitor Capture window.
- Capture data from the network.
- Design a capture filter.
- Design a capture trigger.

Network Monitor Capture Window

As frames are captured from the network, statistics about the frames are displayed in the Network Monitor Capture window.



Total Statistics pane

Graph pane

Session Statistics pane

Station Statistics pane

Network Address 1	1-->2	1<--2	Network Address 2
3COM DDBBFF	899	555	PETERLO2
Intel 0560E6	3	2	PETERLO2
Intel 6140BC	48	30	PETERLO2
Intel C1A942	52	57	PETERLO2
PETERLO2	3		*BROADCAST

Time Elapsed: 00:01:26.664

Network Statistics
Frames: 33678
Broadcasts: 32033
Multicasts: 0
Bytes: 6675692
Frames Dropped: 0
Network Status: Normal

Captured Statistics
Frames: 1649
Frames in Buffer: 1280
Bytes: 1183102
Bytes in Buffer: 1004590
% Buffer Utilized: 97
Frames Dropped: 0

Network Address	Frames Sent	Frames Rcvd	Bytes Sent	Bytes Rcvd	Directed Frames Sent	Multicasts Sent	Broadcasts Sent
*BROADCAST	0	3	0	126	0	0	0
3COM DDBBFF	899	554	1101558	55615	899	0	0
Intel 0560E6	3	2	268	184	3	0	0
Intel 6140BC	48	30	5820	2508	48	0	0
Intel C1A942	52	57	9761	7535	52	0	0
PETERLO2	161	251	16214	222765	158	0	3

The Network Monitor Capture window includes the following panes.

Pane	Displays
Graph	A graphical representation of the activity currently taking place on the network
Session Stats	Statistics about individual sessions currently taking place on the network
Station Stats	Statistics about the sessions participated in by the computer running Network Monitor
Total Stats	Summary statistics about the network activity detected since the capture process began

Capturing and Displaying Frames

Frames captured from the network are copied to the *capture buffer*, a reserved storage area in memory. Information about these frames appears as they are captured in the Network Monitor Capture window. To control capture status, choose **Start**, **Stop**, **Stop and View**, **Pause**, or **Continue** from the **Capture** menu.

Note Network Monitor displays session statistics from the first 100 unique network sessions that it detects. To reset statistics and see information on the next 100 network sessions detected, click **Clear Statistics** on the **Capture** menu.

Customizing Capture Buffer Settings

Captured frames are stored in the *capture buffer*. When the capture buffer overflows, each new frame replaces the oldest frame in the buffer.

Four elements effect how quickly the capture buffer will be filled:

- Capture buffer size
- Frame size
- Capture filter
- Volume of network traffic

The first three of these elements can be customized.

Capture Buffer Size

The capture buffer is stored in memory, not on disk. Although Network Monitor can use virtual memory to store a capture buffer, it is better to use a buffer large enough to ensure that critical frames are not dropped. However, it should be small enough to prevent Windows NT from swapping part of the capture buffer to disk. (The default maximum capture buffer size is 8 MB less than the amount of RAM installed on your computer.)

Frame Size

Although you cannot adjust the frame size, you can store only *part* of the frame, thus reducing the amount of wasted capture buffer space. For example, if you are interested in only the data in the frame header, set the **Frame Size** (in bytes) to the size of the header frame. Network Monitor discards the frame data as it stores frames in the capture buffer, thereby using less capture buffer space.

Capture Filter

For more information on creating a capture filter, see "Capture Filters" later in this chapter.

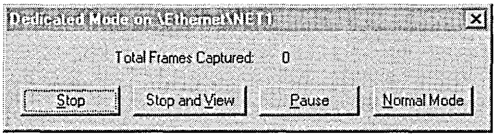
Building an Address Database

Sometimes you'll need to capture only those frames that originate with specific computers. To do this, you must know the addresses of the computers on your network.

Network Monitor can associate a computer's hexadecimal address with its more familiar name. After these associations are made, you can save the names to an address database (.adr) file that can be used to design capture filters and display filters. For more information on how to do this, see "Capture Filters" and "Designing a Display Filter" later in this chapter.

Avoiding Dropped Frames

In addition to setting a sufficient buffer size and capture filter, you can put Network Monitor into dedicated Capture mode, in which the Network Monitor Capture window statistics are replaced by the following dialog box:


Dedicated Mode on \Ethernet\NET1

Total Frames Captured: 0

By not displaying and updating Capture window statistics, Network Monitor reduces the load on the CPU, thereby reducing the chance that packets will be dropped. Use this option if you are running Network Monitor on a busy computer.

For more information on creating a Capture Filter, see "Capture Filters" later in this chapter.

Working With Multiple Network Adapters

If your computer uses multiple network adapters, use Network Monitor to collect data from both of them by either switching between the two adapters or by running multiple instances of Network Monitor.

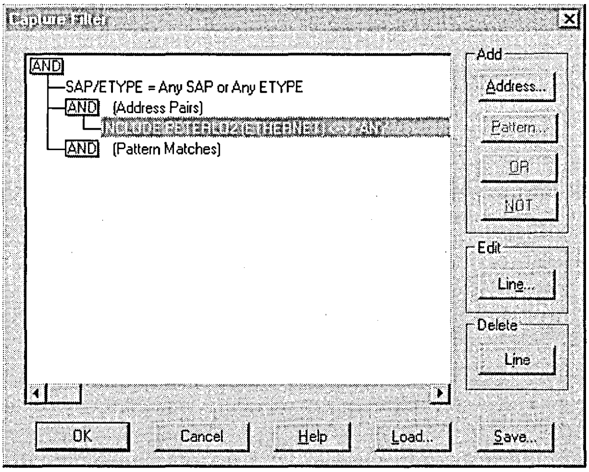
To switch between adapters, click **Networks** on the **Capture** menu and then select a different adapter.

Capture Filters

A *capture filter* functions like a database query. Use it to specify the types of network information you want to monitor. For example, to see only a specific subset of computers or protocols, you can create an address database, use the database to add addresses to your filter, and then save the filter to a file. By filtering frames, you save both buffer resources and time. Later, if necessary, you can load the capture filter file and use the filter again.

Designing a Capture Filter

To design a capture filter, specify decision statements in the **Capture Filter** dialog box. The **Capture Filter** dialog box displays the filter's *decision tree*, which is a graphical representation of a filter's logic. When you include or exclude information from your capture specifications, the decision tree reflects these specifications.



```
AND
├─SAP/ETYPE = Any SAP or Any ETYPE
├─AND  (Address Pairs)
│  └─INCLUDE PETERLO2 (ETHERNET) <--> ANY
└─AND  (Pattern Matches)
```

Filtering by Protocol

To capture frames sent using a specific protocol, specify the protocol on the capture filter SAP/ETYPE= line. For example, to capture only IP frames, disable all protocols and then enable IP ETYPE 0x800 and IP SAP 0x6. By default, all of the protocols that Network Monitor supports are enabled.

Filtering by Address

To capture frames from specific computers on your network, specify one or more *address pairs* in a capture filter. You can monitor up to four specific address pairs simultaneously.

An address pair consists of:

- The addresses of the two computers between which you want to monitor traffic. (An *address* is a hexadecimal number that identifies a computer uniquely on the network.)
- Arrows that specify the traffic direction you want to monitor.
- The INCLUDE or EXCLUDE keyword, indicating how Network Monitor should respond to a frame that meets a filter's specifications.

Note Regardless of the sequence in which statements appear in the **Capture Filter** dialog box, EXCLUDE statements are evaluated first. Therefore, if a frame meets the criteria specified in an EXCLUDE statement in a filter containing both and EXCLUDE and INCLUDE STATEMENT, that frame is discarded. Network Monitor does not test that frame by INCLUDE statements to see if it meets that criteria also.

For example, to capture all the traffic from Joe's computer—*except* the traffic from Joe to Anne—use the following capture filter address section:

```
Addresses
include   Joe <—> Any
exclude   Joe <—> Anne
```

Note If there are no include lines, <your computer> <—> Any is used by default.

Filtering by Data Pattern

By specifying a pattern match in a capture filter, you can:

- Limit a capture to only those frames containing a specific pattern of ASCII or hexadecimal data.
- Specify how many bytes into the frame the pattern must occur. This number of bytes is known as an *offset.*

When you filter based on a pattern match, you must specify where the pattern occurs in the frame (how many bytes from the beginning or end). If your network media has a variable size in the media access control (MAC) protocol, such as Ethernet or Token Ring, specify to count from the end of the topology header.

Capture Triggers

A *trigger* is set of conditions that, when met, initiate an action. For example, before using Network Monitor to capture data from the network, you can set a trigger to stop the capture or to execute a program or command file. You can also specify the conditions under which these actions will occur.

Use one of the following trigger types to specify the condition that starts the trigger:

Nothing
Click this option to specify that no trigger is initiated. This is the default.

Pattern Match
Click this option to initiate the trigger when the specified pattern occurs in a captured frame.

Buffer Space
Click this option to initiate the trigger when a specified amount of the capture buffer is filled.

Pattern Match Then Buffer Space
Click this option to initiate the trigger when the pattern occurs and is followed by a specified percentage of the capture buffer being filled.

Buffer Space Then Pattern Match
Click this option to initiate the trigger when the specified percentage of the capture buffer fills and is followed by the occurrence of the pattern in a captured frame.

You can specify to have one of the following actions occur when a trigger condition is met:

No Action
Click this option to specify that no action is taken when a trigger condition is met. This is the default.

Note Even though you select No Action, the computer beeps when the trigger condition is met.

Stop Capture
Click this option to stop the capture process when the trigger condition is met.

Execute Command Line
Select this check box to run a program or batch file when a trigger condition is met. If you select this option, provide a command or the path to a program or batch file.

Saving Captured Data

When you save captured data, the data in the capture buffer is written to a capture (.cap) file. Be sure to save captured data:

- Before starting another capture (to prevent loss of the captured data).
- If you might need to analyze the data later.
- If you need to document network use or problems.

Capture files can be opened and viewed in Frame Viewer windows.

For more information about saving captured data, see "To save the captured frames to a capture file or text file" in Network Monitor Help.

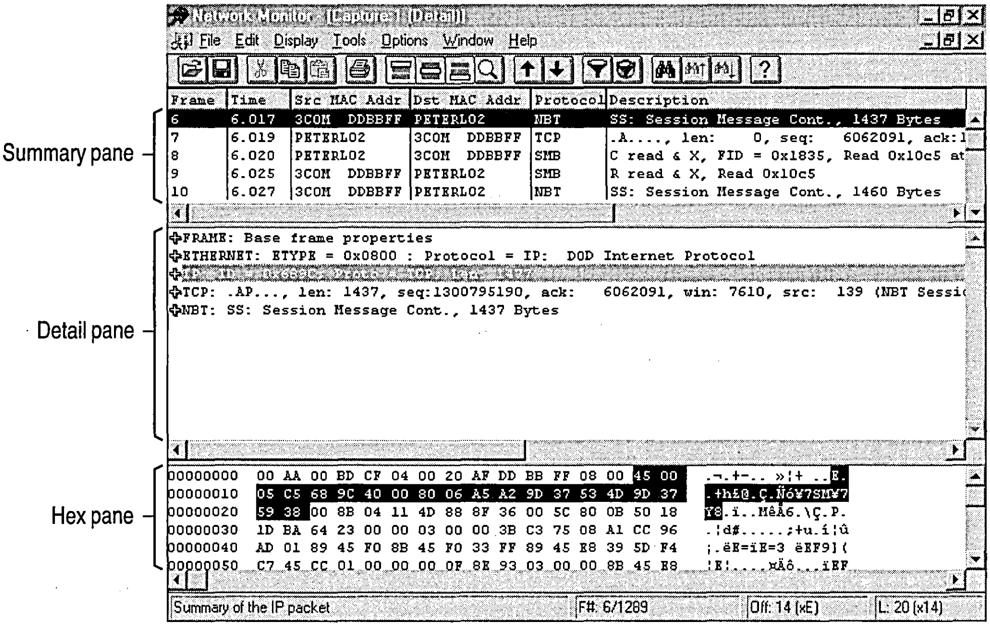
Displaying Captured Data

Network Monitor simplifies data analysis by interpreting raw data collected during the capture and displaying it in the Frame Viewer window.

To display captured information in the Frame Viewer window, choose **Stop and View** from the **Capture** menu while the capture is running or by opening a capture file (.cap).

Note To display data captured with Network General's Sniffer, open the noncompressed Sniffer files. To view a compressed Sniffer file, open the file in Sniffer and then save the file in uncompressed format, or obtain a Sniffer file decompression tool from Network General.

The following illustration shows the key elements in the Frame Viewer window:



```
Frame  Time   Src MAC Addr  Dst MAC Addr  Protocol Description
6      6.017  3COM  DDBBFF  PETERL02      NBT      SS: Session Message Cont., 1437 Bytes
7      6.019  PETERL02      3COM  DDBBFF  TCP      .A...., len:     0, seq:   6062091, ack:1
8      6.020  PETERL02      3COM  DDBBFF  SMB      C read & X, FID = 0x1835, Read 0x10c5 at
9      6.025  3COM  DDBBFF  PETERL02      SMB      R read & X, Read 0x10c5
10     6.027  3COM  DDBBFF  PETERL02      NBT      SS: Session Message Cont., 1460 Bytes
```

```
FRAME: Base frame properties
ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
[illegible]
TCP: .AP..., len: 1437, seq:1300795190, ack:   6062091, win: 7610, src:  139 (NBT Sessi
NBT: SS: Session Message Cont., 1437 Bytes
```

```
00000000  00 AA 00 BD CF 04 00 20 AF DD BB FF 08 00 45 00   .¬.+-.. »¦+ ..E.
00000010  05 C5 68 9C 40 00 80 06 A5 A2 9D 37 53 4D 9D 37   .+h£@.Ç.Ñó¥7SM¥7
00000020  59 38 00 8B 04 11 4D 88 8F 36 00 5C 80 0B 50 18   Y8.ï..MêÅ6.\Ç.P.
00000030  1D BA 64 23 00 00 03 00 00 3B C3 75 08 A1 CC 96   .¦d#.....;+u.í¦û
00000040  AD 01 89 45 F0 8B 45 F0 33 FF 89 45 E8 39 5D F4   ;.ëE=ïE=3 ëEF9](
00000050  C7 45 CC 01 00 00 00 0F 8E 93 03 00 00 8B 45 E8   ¦E¦....ÄÄô...ïEF
```

Summary of the IP packet | F#: 6/1289 | Off: 14 (xE) | L: 20 (x14)

The Frame Viewer window includes the following panes:

Pane	Displays
Detail	The frame's contents, including the protocols used to send it
Hex	A hexadecimal and ASCII representation of the captured data
Summary	General information about captured frames in the order in which they were captured

Using a Display Filter

Like a capture filter, a *display filter* functions like a database query, allowing you to single out specific types of information. But because a display filter operates on data that has already been captured, it does not affect the contents of the Network Monitor capture buffer.

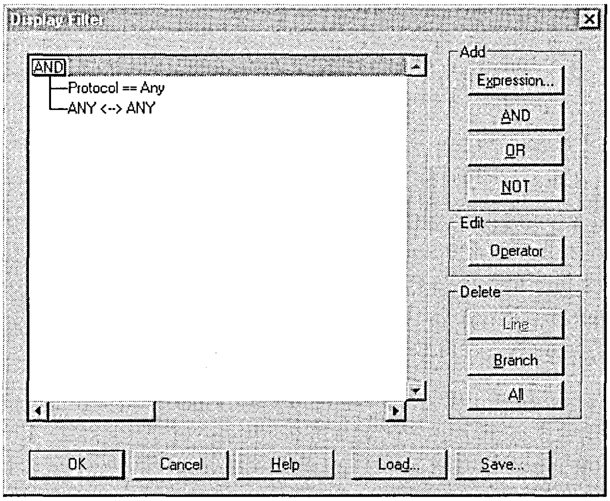
Use a display filter to determine which frames to display. You can filter a frame by:

- Its source or destination address.
- The protocols used to send it.
- The properties and values it contains. (A *property* is a data field within a protocol header. A protocol's properties, collectively, indicate the purpose of the protocol.)

For more information about showing and hiding panes, see "To show and hide panes in a window" in Network Monitor Help.

Designing a Display Filter

To design a display filter, you specify decision statements in the **Display Filter** dialog box. Information in the **Display Filter** dialog box is in the form of a *decision tree*, which is a graphical representation of a filter's logic. When you modify display filter specifications, the decision tree reflects these modifications.


AND
Protocol == Any
ANY <--> ANY

Protocol

Use protocol lines to specify the desired protocols or protocol properties.

For more information on filtering protocols, see the next section. For information on specifying particular protocol properties, see "Filtering by Protocol Property" later in this chapter.

Address Filter (default is ANY <--> ANY)

Use address filter lines to specify the computer addresses on which you want to capture data. For information on how to filter on an address pair, see "Filtering by Computer Address" later in this chapter.

Property

Use this to specify property instances that match your display criterion.

You can add only one decision statement at a time to your filter. If you specify a decision statement and then select another category, the decision statement is lost. You must click **OK** to save the specified decision statement and add it to the decision tree before adding another decision statement.

Note Although capture filters are limited to four address filter expressions, display filters are not. With display filters, you can also use AND, OR, and NOT logic.

Filtering by Protocol

When you display captured data, all available information on the captured frames appears in the Frame Viewer window. To display only those frames sent in a specific protocol, edit the Protocol line in the **Display Filter** dialog box.

Filtering by Protocol Property

Protocol properties are the elements of information that define a protocol's purpose. Because the purpose of protocols vary, properties differ from one protocol to another. To filter by protocol property, click **Expression** under Add in the **Display Filter** dialog box, click the **Property** tab, and then specify the protocol property, relation, and value to filter.

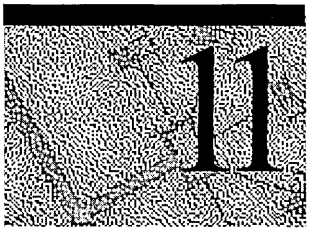
Suppose, for example, that you have captured a large number of frames using the SMB protocol but want to examine only those frames in which the SMB protocol was used to create a directory on your computer. In this instance, you can single out frames where the SMB command property is equal to "make directory."

Filtering by Computer Addresses

When you display captured data, all addresses from which information was captured appear in the Frame Viewer window. To display only those frames originating from a specific computer, edit the ANY <--> ANY line in the **Display Filter** dialog box.

CHAPTER 11

Managing Client Administration



This chapter introduces Network Client Administrator, Client-based Network Administration Tools, Microsoft Network Client version 3.0 for MS-DOS, and the Windows NT Server Remoteboot service. For a complete description of Microsoft Network Client version 3.0 for MS-DOS and the Windows NT Server Remoteboot service, see the *Windows NT Server Resource Kit* version 4.0.

Network Client Administrator

Use the Network Client Administrator to:

- Create a network installation startup disk. With this single disk, you start a client computer, connect to a server that stores installation files, and install the full network software from that server.
- Create a network installation disk set. The disk set contains all the files needed to install network client software.
- Copy Client-based Network Administration Tools to any computer running Windows NT Workstation or Windows NT Server for which you have administrative permissions. Clients can then install the tools by connecting to the server.

▷ **To start Network Client Administrator**

- Click **Start**, **Programs**, **Network Administrative Tools**, and then **Network Client Administrator**.

For more information on Client-based Network Administration Tools, see "Copying Client-based Network Administration Tools," later in this chapter.

Creating Network Installation Startup Disks

You can create network installation startup disks for the following network operating systems and clients:

- Microsoft Windows NT Server versions 3.5, 3.51, and 4.0
- Microsoft Windows NT Workstation versions 3.5, 3.51, and 4.0
- Microsoft Windows 95
- Microsoft Windows for Workgroups version 3.11
- Microsoft Network Client for MS-DOS version 3.0

By default, Network Client Administrator gives you the option to create network installation startup disks for Windows 95 and Microsoft Network Client for MS-DOS. Before you can create network installation startup disks for Windows NT Workstation, Windows NT Server, or Windows for Workgroups, you must first create a folder on the installation server in the shared clients folder (c:\clients by default) and then copy to it the appropriate source files. Windows NT Workstation and Windows NT Server files can be copied from their respective compact discs. Windows for Workgroups files can be copied from Windows for Workgroups disks or from the Windows NT Server version 3.5 or 3.51 compact disc.

Windows NT Workstation and Windows NT Server network installation startup disks can be created only for *x*86 computers and not for Alpha, MIPS, or Power PC computers.

Note Your Windows NT Server software license does not enable you to install additional copies of Windows NT Server, nor does it allow you to install Windows 95 clients free of charge, even though the files are provided on the compact disc. You must purchase a valid software license prior to installing Windows 95, Windows for Workgroups, Windows NT Workstation, or additional copies of Windows NT Sever on a computer. You can, however, freely install Microsoft Network Client for MS-DOS.

When creating network installation startup disks, you must choose from the network interface cards (NICs) supported by Network Client version 3.0 for MS-DOS. Regardless of the client software you are installing, the startup disk begins by starting Network Client so that it can connect to the server. The network card and its settings are not automatically detected. You must select the correct NIC driver and configure it appropriately.

For more information on creating folders and copying source files for Windows NT Workstation, Windows NT Server, or Windows for Workgroups prior to creating a network installation startup disk, see the Readme.txt file in the \Clients\support folder on the Windows NT Server compact disc. For more information on using Network Client Administrator to create network installation startup disks, see Network Client Administrator Help.

Creating Installation Disk Sets

You can create an installation disk set containing the actual installation files for:

- Microsoft Network Client version 3.0 for MS-DOS
- Microsoft LAN Manager version 2.2c for MS-DOS clients
- Microsoft LAN Manager version 2.2c for MS OS/2 clients
- Microsoft Remote Access Service client version 1.1 for MS-DOS
- Microsoft TCP/IP-32 for Windows for Workgroups version 3.11

Using the installation disk set, you can install the software manually on each computer. These files are all included on the Windows NT Server compact disc in the Clients folder. You can freely install this software on any client computer. For more information on using Network Client Administrator to create network installation disk sets, see Network Client Administrator Help.

Copying Client-based Network Administration Tools

Windows NT Server includes Client-based Network Administration Tools to use on Windows NT Workstation and Windows 95 clients. These tools enable you to administer computers running Windows NT Server, LAN Manager for MS OS/2, or LAN Manager for UNIX from a Windows-based computer. You have greater control when using a Windows NT Workstation client because more of these tools are available for Windows NT Workstation clients than for Windows 95 clients.

To use any of the Client-based Network Administration Tools, you must be a member of the Administrators local group at the computer you administer.

In Network Client Administrator, use the Copy Client-based Network Administration Tools option to:

- Share a folder that contains the Client-based Network Administration Tools.

  The folder can either be on the hard drive of a computer running Windows NT Workstation or Windows NT Server or on the Windows NT Server compact disc.
- Copy the Client-based Network Administration Tools to a new folder, and then share the files.

After you copy and share the Client-based Network Administration Tools, clients can install them by connecting to the share.

You can install the following Client-based Network Administration Tools on a computer running Windows NT Workstation:

- DHCP Manager
- Remote Access Administrator
- Remoteboot Manager
- Server Manager
- Services for Macintosh Manager
- User Manager for Domains
- WINS Manager
- User Profile Editor

You can install the following Client-based Network Administration Tools on a computer running Windows 95:

- Event Viewer
- Server Manager
- User Manager for Domains

In addition, when you install these tools, extensions are added to Explorer and My Computer to allow you to change security on Windows NT File System (NTFS) drives, manage Windows NT printers, and manage Windows NT Servers running File and Print Services for NetWare (FPNW).

If you have the Windows NT Server version 3.51 compact disc, you can install Client-based Network Administration Tools on computers running MS-DOS 5.0 or later with Windows version 3.1*x* (with LAN Manager for MS-DOS) or with Windows for Workgroups version 3.1*x*. Functionality of Client-based Network Administration Tools is the same with Windows 3.1 or Windows for Workgroups as with Windows 95.

For information on	See
Installing Client-based Network Administration Tools on a computer running Windows NT Workstation	"To install Client-based Network Administration Tools on a computer running Windows NT Workstation" in Network Client Administrator Help
Installing Client-based Network Administration Tools on a computer running Windows 95	"To install Client-based Network Administration Tools on a computer running Windows 95" in Network Client Administrator Help

Microsoft Network Client Version 3.0 for MS-DOS

Network Client runs on computers running the MS-DOS operating system. It enables the computer to use network resources. For example, a computer running Network Client can use printers, programs, and data stored on a Windows NT Server computer.

With Network Client, a computer can use resources on a Microsoft network from either domains or workgroups, as well as resources on other networks (such as Microsoft LAN Manager networks).

To issue Network Client commands, use the pop-up interface or type commands at the MS-DOS command prompt.

The pop-up interface eliminates the need for remembering Network Client commands at the MS-DOS command prompt. You can use it to view your current connections, browse for shared resources, and make new connections. It is a character-based utility: You must use the keyboard rather than a mouse.

Experienced MS-DOS users familiar with Network Client commands might prefer to type commands at the MS-DOS command prompt rather than using the pop-up interface.

For more information on using Network Client, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

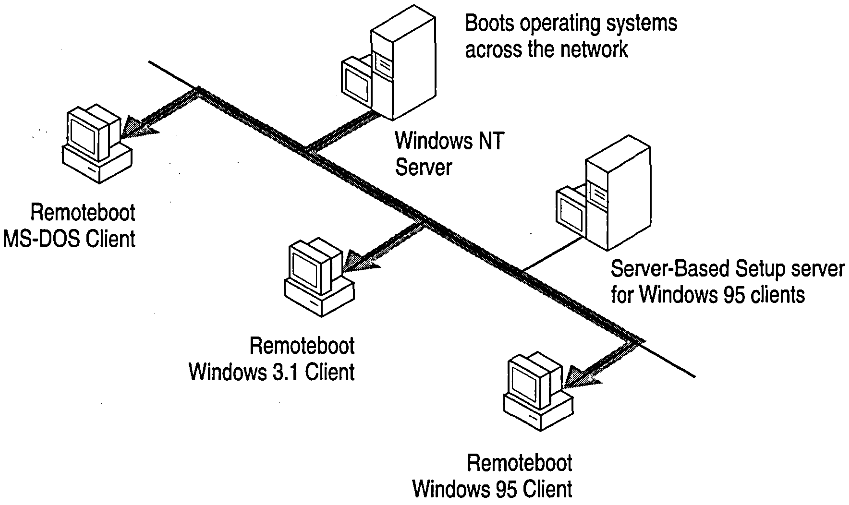
Remoteboot

The Remoteboot service is a Windows NT Server feature that starts MS-DOS and Microsoft Windows workstations (including Windows 95 clients) over the network. You install and configure the Remoteboot service on a server, and then customize it to be more effective for your particular network and for your users.

For more information on using the Remoteboot service, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

Understanding the Remoteboot Service

The Windows NT Remoteboot service enables computers running MS-DOS, Windows 3.1, and Windows 95 (also called *clients* or *workstations*) to start (*boot*) using software from the server's—rather than the client's—hard disk. Each client must have a network adapter with a Remote Initial Program Load (RPL) read-only memory (ROM) chip. This chip retrieves startup and configuration software from the server when the client boots. This process is known as *booting remotely* or the *remoteboot process*.


Boots operating systems across the network
Windows NT Server
Remoteboot MS-DOS Client
Server-Based Setup server for Windows 95 clients
Remoteboot Windows 3.1 Client
Remoteboot Windows 95 Client

The Advantages of Using Remoteboot

By eliminating the need for a hard disk on each client, the Remoteboot service promotes the use of diskless clients. The advantages include:

- Increased network security. (Diskless clients cannot be used to copy data and introduce viruses.)
- Greater control over the distribution of information and software resources.
- Ease of updating software centrally.
- Reduced cost in buying and maintaining client computers.

Clients with hard disks also benefit from the Remoteboot service:

- Easy upgrading of software and operating systems on many clients
- Greater flexibility in standardizing clients while allowing custom configurations

In general, remoteboot offers greater control to the network administrator.

Managing Remoteboot Clients

After you have installed the Remoteboot service and the MS-DOS operating system files, you can use Remoteboot Manager to manage remoteboot clients. To support Windows 95 or Windows 3.1 clients, you copy the client software to the server and make other preparations, including installing a Server-Based Setup (SBS) server for Windows 95 clients.

Note You must boot at least one client on MS-DOS before you can install Windows 3.1 or Windows 95 remoteboot clients.

Remoteboot Requirements

Use the following guidelines to meet the Windows NT Server Remoteboot service requirements:

- Install a network adapter containing an RPL ROM chip on each client computer you plan to boot remotely. (These adapters are available directly from network adapter manufacturers or from independent vendors.) Windows 95 remoteboot clients require 8 MB of RAM and must be 386-based or higher.
- Ensure that the server has enough disk space for the files needed by remote clients. These files can occupy as much as 30.4 MB of server disk space, depending on the type of client software you plan to support. If you plan to use Windows 95 remoteboot clients, either the remoteboot server or the SBS server needs an additional 90 MB of disk space to store the Windows 95 files.
- Reserve room for personal copies of remoteboot profiles (if needed) and for folders for each client (where users store data). The amount of space to allot for each client is up to you.
- If desired, define a separate server (or servers) to contain folders for Windows 95 clients. By doing so, you reduce the possibility of performance problems for remoteboot clients. Each Windows 95 client needs its own folder with a minimum of 8 MB of disk space—more if users install additional software.

Note Some computers must have at least a disk controller to boot remotely. Such computers (many IBM PC AT-compatibles) cannot be truly diskless workstations, even if their disk controller is removed: Their basic input/output system (BIOS) assumes that at least one disk or disk controller is present. Many new computers (even diskless ones) have disk controller circuitry on the motherboard and, therefore, are not truly diskless.

For a list of supported network adapters and complete details on remoteboot server disk space requirements, see the *Windows NT Networking Guide* in the *Windows NT Server Resource Kit* version 4.0.

CHAPTER 12

Licensing and License Manager

Network solutions generally have the following two components:

- Servers that contain information and provide services
- Clients that access information and services

With the Microsoft BackOffice licensing model, these components are licensed separately, so you purchase only what you need to build a network solution for your company's particular requirements. Each server requires a license and each client computer accessing a server also requires a license (called a Client Access License).

The license agreements for certain Microsoft BackOffice server products (such as Windows NT Server, Microsoft Exchange Server, SQL Server, and SNA Server) also provide the flexibility of two client licensing modes: Per Server and Per Seat. With Per Server licensing, each Client Access License is assigned to a particular server and allows one connection to that server for the use of that product. With Per Seat licensing, a Client Access License is assigned to each specific computer that accesses the server. Once a computer is licensed in the Per Seat mode, it can access any network server running that BackOffice server product at no additional charge.

Note Microsoft Systems Management Server (SMS) supports only the Per Seat licensing mode.

Client Access Licenses are separate from the desktop operating system software you use to connect to Microsoft server products. Purchasing Microsoft Windows 95, Windows NT Workstation, or any other desktop operating system (such as Macintosh) that connects to Microsoft server products does not constitute a legal license to connect to those Microsoft server products. In addition to the desktop operating system, Client Access Licenses must also be purchased.

Tracking licenses manually on local computers or within a small domain is time consuming but possible. Tracking licenses without the assistance of automated tools across an entire organization with multiple domains can be very difficult, extremely costly, and overly time consuming. A tool that manages and tracks licenses and usage throughout an organization can help contain these costs.

Windows NT Server 4.0 includes two administrative tools that help to reduce these costs and the administrative overhead of license tracking:

- Licensing option in Control Panel
- License Manager program

These tools enable you to automatically replicate licensing data from all the primary domain controllers (PDCs) in the organization to a centralized database on a specified master server, making it easier for you to comply with legal requirements.

Note Licensing replication does not depend on nor does it use the Replication service or the directory replication process.

Choosing Between the Two Licensing Modes

Licensing for the Microsoft BackOffice family of server products requires a Server License for each server and a Client Access License for each client computer to access the server. These licenses are acquired separately prior to using the product. For Windows NT Server, Microsoft Exchange Server, SQL Server, and SNA Server, the Client Access License can be used in one of two licensing modes (Per Server and Per Seat) offering customers the flexibility to choose the option that best meets their needs.

The licensing mode you select depends on which applications you will be using. For example, if you use Windows NT Server mainly for file and print sharing and on multiple servers, you may be better off with the Per Seat option. However, if you use it as a dedicated Remote Access Server computer, you can select the Per Server concurrent connections option.

Use the following guidelines for selecting a licensing mode:

- If you have only one server, select the Per Server option because you can change once later to the Per Seat mode.
- If you have multiple servers and the total number of Client Access Licenses across all servers to support the Per Server mode is equal to or greater than the number of computers or workstations, select or convert to the Per Seat option.

Use the following worksheet to decide between the two licensing modes:

Per Server

Number of servers A________________________

Number of simultaneous workstation connections to each server B________________________

In line C, enter (A*B) C________________________

Per Seat

Number of seats (computers) that will access any server D________________________

If C is less than D, you should use Per Server licensing. Line C shows the number of Client Access Licenses you need.

If D is less than C, you should use Per Seat licensing. Line D shows the number of Client Access Licenses you need.

In either case, line A shows the number of Server Licenses you need.

Notice that within a single organization, you can also mix the Per Server and Per Seat modes because your choice depends on how much the different server products are used in each department. You can also mix the Per Server and Per Seat modes on a single server if you are running multiple server products. However, a given server product, such as SQL Server, *cannot* be simultaneously run in two modes on the same server.

If you are ever unsure about which licensing mode to choose, select the Per Server option. If your network traffic later increases and more clients need to connect at the same time, you are legally permitted to convert from Per Server mode to Per Seat mode at no additional cost. This is a one-time, one-way conversion option and is available only for Windows NT Server, Microsoft Exchange Server, SQL Server, and SNA Server.

It is not necessary for you to notify Microsoft if you elect to make this change. However, you will need to reenter the licensing data in License Manager using the **New Client Access License** dialog box. You are *not* legally permitted to change the licensing mode from Per Seat to Per Server.

Per Server Licensing

The Per Server licensing mode is available for Microsoft Windows NT Server 3.51 or later, Microsoft SQL Server 4.21a or later, Microsoft SNA Server 2.11 or later and Microsoft Exchange Server 4.0 or later. It is not available for Microsoft Systems Management Server or the Microsoft BackOffice Client Access License.

With Per Server licensing, each Client Access License is assigned to a particular service (product) on a particular server and allows one connection to that service, such as basic network services. For Windows NT Server, the basic network services include the following:

- File services—sharing and managing files and/or disk storage
- Printing services—sharing and managing printers
- Macintosh connectivity—file sharing and printing services
- File and Print Services for NetWare connectivity—file sharing and printing services for NetWare clients
- Remote access services—accessing the server from a remote location through a communications link

Notice that a connection, in this case, is to a server and not just to an individual share point or printer on that server. If you connect to \\Airedale\Apps and \\Airedale\Public, that is considered as only one connection for licensing purposes. However, if you connect in Per Server mode to a server from two different computers using the same username, that is considered two connections.

You must have at least as many Client Access Licenses dedicated to a service on that server as the maximum number of client computers that will connect to that server at any point in time. If you select the **Per Server** option, you must specify during Setup or upon purchasing new Client Access Licenses, the number of Client Access Licenses (which corresponds to the number of concurrent connections) that you have purchased for that server.

With Per Server licensing, once the specified limit for concurrent connections is reached, the server returns an error to the client's computer and does not allow more computer connections to that server. Connections made by administrators are also considered as part of the total number of concurrent connections. When the limit is reached, though, administrators are still allowed to connect to manage the lockout situation. New users, however, cannot connect again until enough users (including administrators) have disconnected to get below the specified limit.

Note You can also check the application log in Event Viewer on the master server to view any license violation alerts, which appear every six hours as Error 71 and Event ID 201.

The Per Server option is often the most economical one for networks in which clients tend to connect to only one server or occasional-use or special-purpose servers, and they do not all need to connect at the same time. If a network environment has multiple servers, each server licensed in Per Server mode must have at least as many Client Access Licenses dedicated to it as the maximum number of clients that will connect to it at any one time.

Per Seat Licensing

The Per Seat licensing mode requires a Client Access License for each computer that will access a particular BackOffice product on any server. Once a computer is licensed for a particular product, it can be used to access that product at any computer running Windows NT Server. Multiple users can also log on to that single computer.

However, having a valid Per Seat mode Client Access License does *not* guarantee you access to a server that is licensed in the Per Server mode and has reached its specified limit. Such a connection also consumes one of the licenses assigned to the pool of available Per Server licenses. Therefore, you can connect only if there are Per Server licenses available.

For example, if a server in Per Server mode has 50 Client Access Licenses dedicated to that server and has fewer than 50 simultaneously connected clients, additional clients can connect. If, however, that server has reached its specified limit, additional clients *cannot* connect, even if they have a valid Per Seat mode license for that service.

If you select the Per Seat licensing mode, any number of licensed computers can be used to connect at any time to any Windows NT Server. However, remember that you must purchase a separate Client Access License for each computer even if you use client operating-system software from Microsoft (including Microsoft Windows for Workgroups, Microsoft Windows 95, or Microsoft Windows NT Workstation) or from a third-party vendor or use any of the other client software supported by Windows NT Server. The Per Seat option is often the most economical one for networks in which clients tend to connect to more than one server.

Note A Client Access License is *not* included when you acquire Windows 95, Windows NT Workstation, or Windows for Workgroups. The license must be purchased separately in addition to the operating-system software.

License Groups

To obtain correct licensing information when working with Per Seat licenses, you might need to group certain users and make them members of a license group.

License groups show a relationship (also known as a mapping) between users and computers and should be used only when one of the following configurations is true:

- Multiple people using one computer, such as when people share jobs or there are multiple shifts using the same computers.
- Many users are using many computers but there are still a different number of users than computers, such as in a university computer lab or in a retail store.
- One user to many computers, such as happens in many software developers' offices where they need to develop on one computer and test their applications on several different computer-hardware platforms.

A license group is composed of:

- A single descriptive name for the group
- A specified number of Per Seat licenses assigned to the group
- A specific list of users who are members of the group.

The number of licenses assigned should correspond to the number of computers in the licensing group. This number does not have to match the number of users in the group.

In the first example with multiple users but only one computer, you need only one Client Access License. You are licensing the number of computers, not the number of users.

The same logic also applies to the second configuration. For example, if you have 100 users accessing 10 computers, you need to purchase only 10 Client Access Licenses to cover those 10 computers. However, you might want to keep track of all 100 users and how often they use each computer to access various servers. The license group you create is assigned 10 Client Access Licenses and includes 100 users.

In the last case, the one user needs multiple Client Access Licenses to be in compliance with legal licensing requirements even though License Manager shows only one user. In this case, the license group includes only one user with multiple Client Access Licenses assigned.

Keeping an Enterprise Licensing Database

License tracking can be local, by domain, or across an entire organization. For organization-level tracking, an administrator can ensure the company's legal compliance with software license agreements by maintaining a centralized historical database of all purchases and deletions. Windows NT Server provides a means to keep a centralized database on a designated master server to which each server replicates its licensing information.

The master server is a server in an organization or domain that has been designated as the centralized repository of all licensing data for that organization or domain. It can be either the PDC for that individual domain or a specified *enterprise server*. An enterprise server is the server to which multiple PDCs in a large organization will replicate.

In a smaller, single-domain company, the domain's PDC is the master server for the domain (and thus the entire organization). In a larger multiple domain organization, each PDC is the master server for its domain, and the organization also has a single enterprise server which receives information from the various master servers.

The primary domain controller is the master server for all the backup domain controllers and other servers in that domain. The backup domain controllers and other servers always replicate to the PDC.

You should set a server to replicate to an enterprise server only in the following cases:

- The server is a standalone server, not participating in a domain.
- The server is a PDC that you want to replicate its information to an enterprise server

The following table shows the availability of each option and under what circumstances you would select each one.

If the server is a	Select domain controller	Select enterprise server
Server in a domain	Default option	Not available
Standalone server in its own domain	If you don't want to replicate	If you want to replicate to a higher server
Backup domain controller	Default option	Not available
Primary domain controller	If you don't want to replicate	If you want to replicate to a higher server
Enterprise server	Default option	Not available

Choosing an Enterprise Server

You can have one or more enterprise servers in your organization. However, it is easier to have a single enterprise server so that you collect all the organization's licensing information into one complete database.

If you have multiple enterprise servers, none of them can replicate to another enterprise server. In this case, each enterprise server would compile only a subset of your organization's licensing information.

For your enterprise server, you should choose only a primary domain controller or a standalone server that is not participating in a domain.

Balancing the License Replication Load

License Manager provides two ways for you to balance the network load of the replication of licensing information.

- You can select how often the server is to replicate its information. License Manager automatically staggers the replication of licensing data from each server, ensuring that the load is balanced. You can set the frequency to any amount between 1 and 72 hours between replications.
- For each server, you can specify what time each day that server is to replicate its information. This allows you to balance the load manually. In this case, the server replicates its information every 24 hours.

Each of these options is available both for backup domain controllers and servers replicating to their domain PDCs and for PDCs replicating to an organization's enterprise server.

The time for licensing changes on an individual server to make their way up to the enterprise server in a domain can be as much as twice the frequency you set. For example, at a frequency of 24 hours, information can take as much as 24 hours to replicate to the PDC and 24 more hours to replicate to the enterprise server.

For detailed instructions on how to perform these activities, see Help.

Administering Licenses and Licensing Information

Windows NT Server provides two tools—License Manager and the Licensing option in Control Panel—to assist administrators in managing licensing.

These tools provide a way for administrators to track Client Access Licenses across an organization and ensure compliance with the requirements of the Microsoft BackOffice family license agreements.

Administrators can use the License Manager program to obtain a centralized view of Per Seat and Per Server licenses across the organization, manage the purchasing or deleting of licenses for products on network servers over which they have administrative rights, view usage statistics per user, and balance the licensing replication load across the network.

Licensing Option in Control Panel

Licensing

After the initial Setup process, you can use the Licensing option in Control Panel if you need to change the licensing mode on that computer from Per Server to Per Seat (a one-time only option). You can also use it to configure licensing replication for that computer and to add or delete Per Server licenses for each BackOffice family product installed on the server (Per Seat licenses can be administered only through License Manager).

License Manager

With License Manager, administrators can (locally or remotely) change the licensing mode of BackOffice™ family products from Per Server to Per Seat, add or delete Client Access Licenses for BackOffice products, create license groups, and view licensing information at several levels.

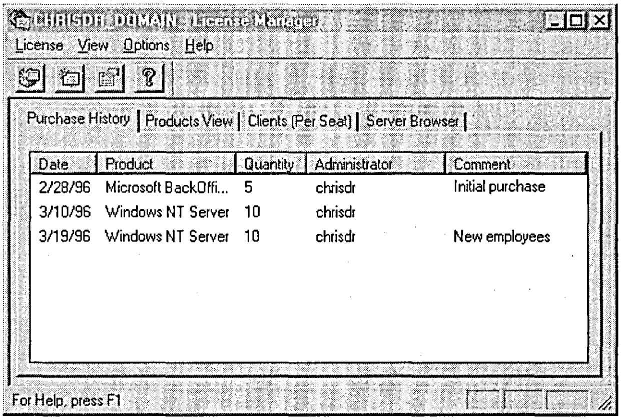
▷ **To start License Manager**

1. On the **Start** menu, click **Programs**, and then click **Network Administration**.
2. Click **License Manager**.

Upon starting License Manager, you see an opening screen with the following tabs that provide overall information and paths to the tool's principal management functions:

- Purchase History
- Products View
- Clients (Per Seat)
- Server Browser

Each tab provides a different view of the information (products, product licenses, clients, and servers) tracked by License Manager and access to various Properties screens with additional tabs for information that is specific to that item.



Date	Product	Quantity	Administrator	Comment
2/28/96	Microsoft BackOffi...	5	chrisdr	Initial purchase
3/10/96	Windows NT Server	10	chrisdr	
3/19/96	Windows NT Server	10	chrisdr	New employees

Purchase History Tab

The **Purchase History** screen provides a historical overview of the licenses purchased for products installed in the selected domain or organization. It also shows the quantity of licenses purchased and deleted, the date of installation or deletion, and the identity of the administrator (the one who certifies that the company purchased the license) who either installed or deleted the product license. It also shows comments that were entered during installation or deletion of licenses.

Products View Tab

The second main tab is for the **Products View** screen, which contains information on the products in the selected domain or the entire organization. What this screen shows depends on the licensing mode of each product:

- For Per Seat mode, it shows how many licenses have been purchased for the product and how many licenses have been allocated to users' computers for all the products.
- For Per Server mode, it shows the total number of licenses that have been purchased for each product on all the servers in the domain or organization that have that product installed. It also shows the maximum number of concurrent connections reached up to that date on all the servers in the domain or organization with that product on them.

You can use both the numerical and graphical information in this screen to determine the following:

- The products in compliance with legal licensing requirements
- The products not in compliance with legal licensing requirements
- The products that have reached the legal limit and for which you might want to purchase additional licenses

While in this screen, you can also do the following:

- Add new Client Access Licenses.
- Delete existing Client Access Licenses for a product.
- Open the selected product's Properties screen.

For detailed instructions on how to perform these activities see Help.

Double-clicking any product name opens the Properties screen for that product and enables you to access three additional tabs with information that is specific to that product.

Clients (Per Seat) Tab

The third tab is for the **Clients (Per Seat)** view, which provides information on a list of clients (or users) that have used the products in that domain or organization. It also shows how many of the listed products (licensed in Per Seat mode) they are licensed to use and how many they are *not* licensed to use.

These users can be either single users or members of license groups. (To see which users are members of particular license group, click **Advanced** on the **Options** menu, and then click **Edit License Groups**.)

You can use both the numerical and graphical information in this screen to determine the following:

- The users who in compliance with legal licensing requirements
- The users who are not in compliance with legal licensing requirements

While in this screen, you can also do the following activities:

- Add new Client Access Licenses.
- Delete a user.
- Create, view, and edit license groups.

For detailed instructions on how to perform these activities see Help.

Double-clicking the user's name opens the **Properties** screen for that user and enables you to access a **Products View** tab, which shows which products in the domain or organization are being used by that user, the last date the user used them, and how many times the user has used them.

Server Browser Tab

The final tab is for the **Server Browser** view, which lists all the domains and servers in the organization. This tab enables you to view and edit server and server product licensing information in any domain in which you have administrative authority.

While in this screen, you can access these three levels and do the following:

- At all levels, add new Client Access Licenses.
- At the server and product levels, open the selected item's **Properties** screen.

For detailed instructions on how to perform these activities see Help.

Double-clicking a domain name displays a list of all the servers located in that domain. Double-clicking a server name displays a list of all the products installed on that server. Double-clicking a product name displays the **Choose Licensing Mode** dialog box for changing the licensing mode.

Troubleshooting Licensing Problems

The following section provides a list of licensing-related events you might see in the Application Log of Event Viewer and the steps to take (if any) with each. The events are listed by event ID number, with the lowest first.

201 No license was available for user *user_name* using product *product name*.
202 The product *product_name* is out of licenses.

Each of these messages indicate licensing violations of the products named in the message.

203 The user data could not be saved.
204 The license group data could not be saved.
205 The purchased license data could not be saved.

Each of these messages indicated that an error occurred, preventing licensing data from being saved. The license service may be able to succeed later in writing the file. If not, the data is lost for now. Data that is received from other computers will be regained during the next round of replication, but local data must be reentered.

208 The saved user data could not be restored.

209 The saved license group data could not be restored.

210 The saved purchased license data could not be restored.

Each of these messages indicated that an error occurred, preventing licensing data from being read from a saved file. The license service will overwrite the file the next time it saves information. Data that is received from other computers will be regained during the next round of replication, but local data must be reentered.

213 Replication of license information failed because the License Logging Service on server *server_name* could not be contacted.

The indicated PDC or enterprise server is either not available on the network or the license service on that computer is not running. Verify that the computer is on the network and is running, and use Server Manager to make sure the license service is running on that computer.

214 The License Logging Service encountered an error while initiating replication to server *server_name*.

The license service on the named server was contacted, but an error occurred before replication could begin. This is probably due to communications problems on the network. The license service will retry replication in 15 minutes and every 15 minutes thereafter until it succeeds.

215 License database replication to server *server_name* was unsuccessful.

Replication to the named server began successfully but failed to complete. This is probably due to communications problems on the network. The license service will retry replication in 15 minutes and every 15 minutes thereafter until it succeeds.

216 The license certificate for product *product_name* with serial number *serial_number* is in violation. There are currently *installed_number* licenses installed from this certificate, while only *licensed_number* are allowed by the license agreement. The servers with this certificate installed are as follows: *server_names* Use License Manager to remove licenses in order to comply with the license agreement.

The license service has detected that the certificate with the listed serial number has had more licenses installed from it than it allows. The servers for which this certificate has licenses installed are listed. You should use License Manager to reduce the number of licenses installed from this certificate.

217 The certificate database could not be saved.

Check whether the server has enough disk space.

218 The certificate database could not be restored.

The database file may be corrupt. No action is necessary. The database will be automatically regenerated.

219 License database replication cannot be performed to server *server_name* because the version of Windows NT installed there does not support the License Logging Service.

The named server is available on the network but has no license service installed because it is running a version of Windows NT prior to 3.51.

Reestablishing Lost Connections

A lost connection with a domain server results in the error message "The RPC server is unavailable." To reestablish a lost connection with a server, reselect the domain.

Situations That Use Up Licenses

The following is a list of many common situations that use up one or more licenses from the pool of available licenses in either Per Seat or Per Server mode or both modes. These are situations under which License Manager assigns licenses. They do not always coincide with when you legally use a license, such as what happens with license groups.

- Disconnecting from a connection to basic network services on a computer running Windows NT Server using the IPX protocol results in a license being held upon disconnection for up to the time value of the ConnectionlessAutoDisc function, which is a minimum of 15 minutes. In other words, this is the amount of time that it will take to free up that license for use by others, and you cannot shorten it. However, if you reconnect within that 15-minute period, you use the same license and do not consume another one. (Per Server only)
- Connecting to a server from two different computers using the same username legally counts as two connections. (Per Server only)
- In Windows NT Workstation and Windows NT Server, using the **net use** command with the **/u** option could result in another license being assigned. This depends on the name you specify with the **/u** option and happens only when a name other than the user's domain name is used. For an example, see "Counting Connections Twice for Licensing" later in this chapter. (Per Seat only)
- The following list provides several examples of services whose connections use up from one to many Client Access Licenses:
    - Windows NT Backup, when used to back up to a remote server. Local backups do not use up a license. (Both modes)
    - A Remote Access Server (RAS) connection to Windows NT Server using PPP or SLIP (Both modes)
    - Macintosh connections using Services for Macintosh (Both modes)

- NetWare client connections using FPNW (Both modes)
- File and print sharing connections to Windows NT Server using Server Message Block (SMB) (Both modes)
- UNIX connections using the Windows NT Server UNIX-LPD service for print sharing (Both modes)
- Microsoft logon scripts that exist on a Windows NT Server to be run on a workstation (Windows NT Workstation, Windows for Workgroups, or Windows 95) (Both modes)
- Configuring Windows 95 to authenticate to a Windows NT Server domain, due to the policy profile feature (Both modes)
- Systems Management Server (SMS), when workstations are inventoried (Per Seat only)
- SNA Server, when a client connects to a server running SNA Server (Both modes)
- Microsoft Exchange Server, when a Microsoft Exchange Client connects to a server running Microsoft Exchange Server (Both modes)
- SQL Server, when a client connects to a server running SQL Server (Both modes)

The following list shows several (but not all) situations that do *not* use a license:

- Connecting to a remote server's registry
- Remote administration of another computer using Performance Monitor, Server Manager, or User Manager for Domains
- Local logons to a server
- Using the File Transfer Protocol (FTP), Telnet, and Windows Sockets Internet utilities, unless they are connecting to a computer (or an application) that does use up a license
- Using Windows Internet Name Service (WINS) and Dynamic Host Configuration Protocol (DHCP)
- Using simple network management protocol (SNMP)
- Using network dynamic data exchange (NetDDE)
- Using remote procedure call (RPC), unless it connects to an application that does use up a license, such as SMB Server
- Using named pipes, unless they connect to a service that does use up a license
- Connections to non-Microsoft server products, such as ORACLE, unless they connect to an application that does use up a license

Counting Connections Twice for Licensing

Consider the following scenario in which two licenses are assigned to the same user. (This can happen only on Windows NT Workstation or Windows NT Server; not on Windows 95 or Windows for Workgroups.) A primary domain controller (PDC) has its Guest account disabled. It has a share named LLS and a user named DomUser, whose password is also DomUser.

From DomainA, the user connects in Per Seat mode to the PDC using the following command:

```
net use * \\pdc\lls /u:DomUser DomUser
```

This is counted as DomainA\DomUser, and one license is assigned.

From DomainB, the user connects through RAS to the PDC using the same command as before. This is counted as DomainB\DomUser, and another license is assigned.

The reason is that the user did not specify the domain of the account. Therefore, the local account on the PDC is providing access, but the connection is still from the remote domain. To avoid this situation, the user must specify a domain name along with theusername. For example, if you specify the same name from both domains, that is /u:DomainA\DomUser, the PDC counts it as a single connection and assigns a single license.

If you are using a notebook or laptop computer that is disconnected from the network, another solution is to log on as the domain user account rather than as the local user. Then, if you connect through RAS to the network, you are assigned only one license and not two.

License Purchasing Requirements

Before purchasing a product, it also helps to know if you need to purchase licenses, how many, and what kind. The following examples provide detailed information on several Microsoft server products.

Microsoft Exchange Server

The Microsoft Exchange Server license enables you to install and use the Microsoft Exchange Server software on a single server computer. A few components of the server software can be installed and used on any number of computers without purchasing additional licenses. The Microsoft Exchange Administrator program, the MS Mail Connector, and the Source Extractors contain such components.

You can install client software on any number of computers. However, a Client Access License is required for every computer that accesses the services of Microsoft Exchange Server. This is required regardless of the client operating system software used, or whether the client operating system includes a Micrososft Exchange Client Inbox.

Connector software is licensed to be installed and used on a single computer running Microsoft Exchange Server. If you install connector software on one server, you must purchase licenses to use the connector software on every other server in the same organization. This is because once a connector is installed on one server, users of any server in the same organization can access the connector to send and receive mail.

Microsoft SQL Server

With SQL Server, you can have a server running a SQL gateway application (that is, an application that maintains a single connection to the SQL Server database). Multiple clients can access the gateway, which manages the database queries on behalf of the clients. However, clients do not connect directly to the SQL Server database, so License Manager cannot track the usage accurately. License Manager detects only one licensed connection.

The product license specifically addresses this type of multiplexing or pooling application. The license states that using software or hardware that reduces the number of users directly accessing or using SQL Server, which is sometimes called multiplexing or pooling software or hardware, does *not* reduce the number of Client Access Licenses required. The required number of Client Access Licenses equals the number of distinct connections to the multiplexing or pooling software or hardware front end.

Microsoft Systems Management Server

In a Systems Management Server (SMS) hierarchy, at least one Server License for a SQL Server is required and must be purchased separately. A Server License for Windows NT Server is also required for each server using server code (such as primary, secondary, and helper servers) for a Systems Management Server. Therefore, if you need to purchase Server Licenses to run three server products (Systems Management Server, SQL Server, and Windows NT Server) on the same computer, it is cheaper to purchase the BackOffice Server License.

Microsoft SNA Server

Microsoft SNA Server requires a Server License for the server and Client Access Licenses for all computers that access the SNA Server. You can access SNA Server in many ways. The most common form of access is through an application, such as Attachmate Extra or an application developed with Visual Basic, that is accessing SNA services. Although you are not directly connected to SNA Server, the application that you are using is connected, so an SNA Server Client Access License is required.

Microsoft BackOffice 2.0

Microsoft BackOffice 2.0 is an integrated family of server products, consisting of Windows NT Server 3.51, Microsoft SQL Server 6.5, Microsoft SNA Server 2.11a, Microsoft Systems Management Server 1.1, Microsoft Exchange Server 4.0, and Microsoft Internet Information Server 1.0. Like the other server products, Microsoft BackOffice is available in both a Server License and a Client Access License.

Customers can purchase Microsoft BackOffice Client Access Licenses to access standalone servers. In other words, a BackOffice Client Access License gives that client the capability to access the services of all the server products mentioned previously, regardless of whether the Server Licenses for those products were acquired through a BackOffice Server License or through individual product Server Licenses. A BackOffice Client Access License can be used only in the Per Seat licensing mode.

Microsoft Internet Information Server

To use Microsoft Internet Information Server, you need only a Server License. You do not need to ensure that every person using its services over the Internet has a Client Access License.

You may copy and distribute the client software accompanying Microsoft Internet Information Server for use within your organization.

Microsoft FPNW and Microsoft DSMN

If you are using FPNW with Windows NT Server, you must purchase Windows NT Server Client Access Licenses for the NetWare or compatible clients that connect to the server. These licenses can be used in either the Per Seat or Per Server mode.

With Directory Service Manager for NetWare (DSMN), you purchase Windows NT Server Client Access Licenses only if you are also using Windows NT Server basic network services.

Microsoft Services for Macintosh

For the Services for Macintosh feature of Windows NT Server, you must purchase Windows NT Server Client Access Licenses for the Macintosh clients that connect to the server. These licenses can be used in either the Per Seat or Per Server mode.

FTP, Gopher, WWW, or RAS Server

To set up an FTP, Gopher, or World Wide Web (WWW) site, you purchase only a Server License. You do not need to make sure that every user has a Client Access License from Microsoft.

If you also want to use the Microsoft Remote Access Service for PPP or SLIP dial-in support, you also need one Client Access License per connection. In other words, if the site supports 10 concurrent connections, you need to purchase a Server License and 10 Client Access Licenses for basic network services in the Per Server mode. If the site supports workstations in the Per Seat mode, purchase a Server License and Client Access Licenses for basic network services for each workstation. If you increase the number of concurrent connections allowed, you must purchase additional Client Access Licenses in the Per Server mode up to the maximum number of concurrent users of the Remote Access Service.

APPENDIX A

Windows NT Registry

In Windows NT, configuration information is centrally stored in a single database called the *registry*. The registry replaces the .ini, .sys, and .com configuration files used in Windows for MS-DOS and Microsoft LAN Manager.

This appendix provides an overview of registry structure, describes how Windows NT components use the registry, provides an overview of the Registry Editor and Windows NT Diagnostics, and describes how .ini files are mapped to the registry.

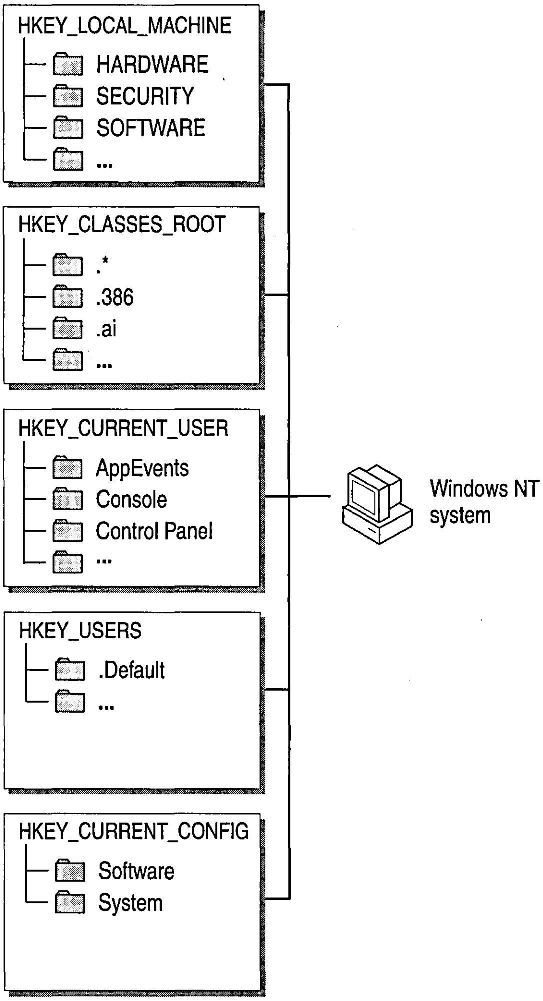
For more detailed information about the registry and specific registry keys, see the *Windows NT Workstation Resource Kit* version 4.0.

Registry Structure

The registry is a database organized in an hierarchical structure. The registry is comprised of subtrees and their keys, hives, and value entries. A key can also contain additional *subkeys.*

Registry Hierarchy

The registry subtrees are divided into per-computer and per-user databases. The per-computer information includes information about hardware and software installed on the specific computer. The per-user information includes the information in user profiles, such as desktop settings, individual preferences for certain software, and personal printer and network settings.



The subtrees in the Windows NT registry

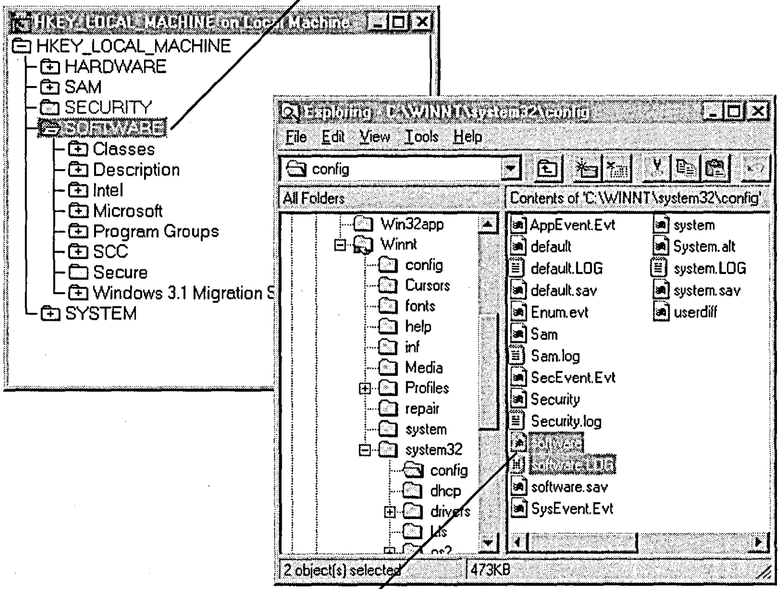
The following table identifies and defines the registry subtrees.

Root key name	Description
HKEY_LOCAL_MACHINE	Contains information about the local computer system, including hardware and operating system data such as bus type, system memory, device drivers, and startup control data.
HKEY_CLASSES_ROOT	Contains object linking and embedding (OLE) and file-class association data (equivalent to the registry in Windows for MS-DOS).
HKEY_CURRENT_USER	Contains the user profile for the user who is currently logged on, including environment variables, desktop settings, network connections, printers, and application preferences.
HKEY_USERS	Contains all actively loaded user profiles, including HKEY_CURRENT_USER, which always refers to a child of HKEY_USERS, and the default profile. Users who are accessing a server remotely do not have profiles under this key on the server; their profiles are loaded into the registry on their own computers.
HKEY_CURRENT_CONFIG	Contains information about the hardware profile used by the local computer system at startup. This information is used to configure settings such as the device drivers to load and the display resolution to use.

Each root key name begins with HKEY_ to indicate to software developers that this is a *handle* that can be used by a program. A handle is a value used to uniquely identify a resource so that a program can access it.

Hives and Files

The registry subtree is divided into parts called *hives* (after their resemblance to the cellular structure of a beehive). A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. A hive is backed by a single file and a .log file which are in the *%SystemRoot%*\system32\config or the *%SystemRoot%*\profiles*username* folders. By default, most hive files (Default, Sam, Security, Software, and System) are stored in the *%SystemRoot%*\system32\config folder. The Ntuser.dat and Ntuser.dat.log files are stored in the *%SystemRoot%*\profiles*username* folder. The *%SystemRoot%*\profiles folder contains the user profile for each user of the computer.



The SOFTWARE hive in the registry

The SOFTWARE hive files as seen in Windows NT Explorer

Tip By default, when viewing files using Windows NT Explorer, file extensions are hidden.

The following table shows the standard hives for a computer running Windows NT.

Registry hive	File names
HKEY_LOCAL_MACHINE\SAM	Sam and Sam.log
HKEY_LOCAL_MACHINE\SECURITY	Security and Security.log
HKEY_LOCAL_MACHINE\SOFTWARE	Software and Software.log
HKEY_LOCAL_MACHINE\SYSTEM	System and System.log
HKEY_CURRENT_USER	Ntuser.dat and Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default and Default.log

Registry Size Limits

The total amount of space that can be consumed by Registry data (hives) is restricted by the r*egistry size limit*, which is a kind of universal maximum for registry space that prevents an application from filling the paged pool with registry data. Registry size affects both the amount of paged pool the registry can use and the amount of disk space used by the registry.

To view or set the value for **RegistrySizeLimit**, first create the key using the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RegistrySizeLi
mit
```

The registry size can also be viewed and set using the System option in Control Panel. See the Virtual Memory box in the **Performance** tab. For information about how to set the registry size using Control Panel, see "Virtual Memory" or "Changing the Virtual-Memory Paging File" in Help.

The registry size should be changed only if the computer is either a primary or backup domain controller for a large network because all user accounts are stored in the registry.

RegistrySizeLimit must have a type of REG_DWORD and a data length of 4 bytes, or it will be ignored. By default, the registry size limit is 25 percent of the size of the paged pool.

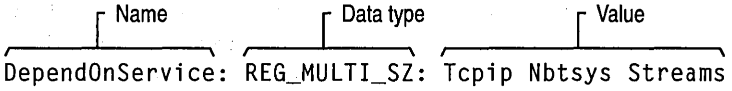
Setting a large value for **RegistrySizeLimit** does not cause the system to use that much space unless it is actually needed by the registry. A large value also does not guarantee that the maximum space will actually be available for use by the registry.

For more details about **RegistrySizeLimit**, see the *Windows NT Workstation Resource Kit* version 4.0.

Value Entries in the Registry Keys

Each registry key can also contain data items called *value entries.* Keys are analogous to directories, and value entries are analogous to files.

A value entry has three parts: the name of the value, the data type of the value, and the value itself, which can be data of any length. The three parts of value entries always appear in the following order.



```
DependOnService: REG_MULTI_SZ: Tcpip Nbtsys Streams
```

Data types, such as REG_SZ or REG_EXPAND_SZ, describe the format of the data which can be up to 1 MB. Data types from 0 to 0x7fffffff are reserved for definition by the system, and applications are encouraged to use these types. Data types from 0x80000000 to 0xffffffff are reserved for use by applications.

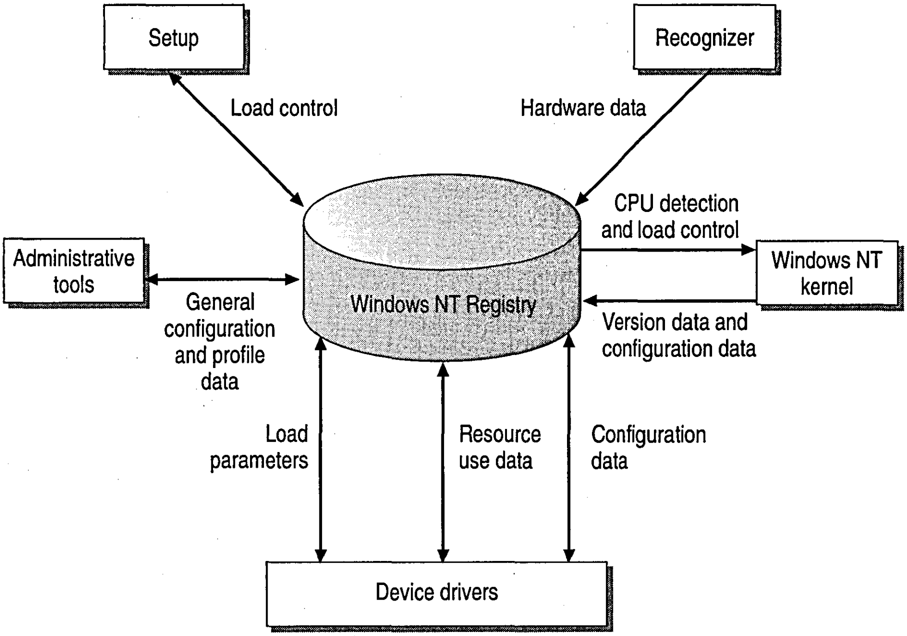
The following table lists the data types currently defined and used by the system.

Data type	Description
REG_BINARY	Binary data. Most hardware component information is stored as binary data and can be displayed in Registry Editor in hexadecimal format or displayed via the Windows NT Diagnostics program (WINMSD.EXE)[1] in an easy-to-read format. For example: `Component Information : REG_BINARY : 00 00 00...`
REG_DWORD	Data represented by a number that is 4 bytes long. Many parameters for device driver and services are this type and can be displayed in Registry Editor in binary, hexadecimal, or decimal format. For example, entries for service error controls are this type: `ErrorControl : REG_DWORD : 0x1`
REG_EXPAND_SZ	An expandable data string, which is text that contains a variable to be replaced when called by an application. For example, for the following value, the string *%SystemRoot%* will be replaced by the actual location of the directory containing the Windows NT system files: `File : REG_EXPAND_SZ :` *%SystemRoot%*`\file.exe`
REG_MULTI_SZ	A multiple string. Values that contain lists or multiple values in human readable text are usually this type. Entries are separated by NULL characters. For example, the following value entry specifies the binding rules for a network transport: `bindable : REG_MULTI_SZ : dlcDriver dlcDriver non non 50`
REG_SZ	A sequence of characters representing human readable text. For example, a component's description is usually this type: `DisplayName : REG_SZ : Messenger`

[1] For more information about Registry Editor and Windows NT Diagnostics, see "Using Registry Editor" and "Using Windows NT Diagnostics to View System Configuration Data" later in this appendix.

How Windows NT Components Use the Registry

The following figure shows how various Windows NT components and applications use the registry.



How components and applications use the registry

- *Setup.* Both the Windows NT Setup program and other setup programs (for applications or hardware) add configuration data to the registry. For example, new information is added when you install a new small computer system interface (SCSI) adapter or change the settings for your display. Setup also read information from the Registry to determine if the prerequisite components have been installed.
- *Recognizer.* Each time you start a computer running Windows NT, the Hardware Recognizer places hardware configuration data in the registry. This data includes a list of hardware detected in your system. On *x*86-based computers, hardware detection is done by the Hardware Recognizer (Ntdetect.com) and the Windows NT Kernel (Ntoskrnl.exe) programs. On RISC-based computers, this information is extracted from the ARC firmware.
- *Windows NT Kernel.* During system startup, the Windows NT Kernel extracts information from the registry, such as which device drivers to load and their load order. The Ntoskrnl.exe program also passes information about itself (such as its version number) to the registry.

- *Device drivers.* Device drivers send and receive load parameters and configuration data from the registry. This data is similar to what you might find on the DEVICE= lines in the Config.sys file in the MS-DOS operating system. A device driver must report system resources that it uses (such as hardware interrupts and direct memory access (DMA) channels) so that the system can add this information to the registry. Applications and device drivers can access this registry information to provide users with smart installation and configuration programs.
- *Administrative tools.* The options and administrative tools in Windows NT (such as those provided in Control Panel and in the Administrative Tools (Common) folder) enable you to modify configuration data indirectly.

Registry contents can be directly viewed, modified, or both using one of the following tools:

- The Registry Editor is helpful for viewing and occasionally making detailed changes to the system configuration. For more information about Registry Editor, see “Using Registry Editor” later in this appendix.
- The System Policy Editor enables you to view and modify certain registry keys. The System Policy Editor also displays the data in a much more user-friendly manner. For more information about the System Policy Editor, see “System Policy” in Chapter 3, “Managing User Environments.”
- The Windows NT Diagnostics program (Winmsd.exe) also provides a view of configuration information stored in the registry. Windows NT Diagnostics can read and display registry data about the system resources used by drivers. For more information about using the Windows NT Diagnostics program, see “Using Windows NT Diagnostics to View System Configuration Data” later in this appendix or see the *Windows NT Workstation Resource Kit* version 4.0.

Caution Although it is possible to modify the contents of the registry directly, it is recommended that the tools (especially Registry Editor) be used by system administrators only.

Using Registry Editor

Registry Editor

You can use the Registry Editor to view registry entries for the various components in Windows NT. You can also use Registry Editor to modify or add registry entries.

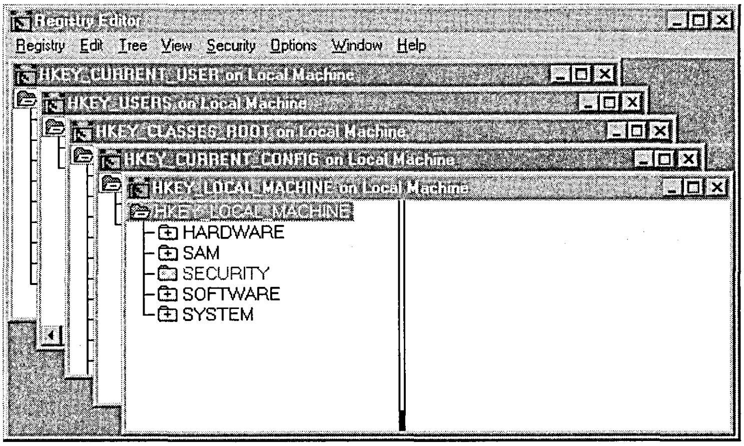
Caution When making changes to the system configuration, it is best to use Control Panel or the applications in the Administrative Tools (Common) folder. Otherwise you can impair or disable Windows NT.

The Registry Editor application, Regedt32.exe, does not appear in any default folders It is installed automatically in your *%SystemRoot%*\system32 folder. Click **Run** on the **Start** menu or switch to a command prompt and type **regedt32.**

For information about how to start Registry Editor, see "Understanding Registry Editor" in Registry Editor Help.

Viewing the Registry

Registry Editor displays the subtrees of the registry. The hierarchical structure that appears in Registry Editor is similar to the hierarchical directory structures of Windows NT Explorer.

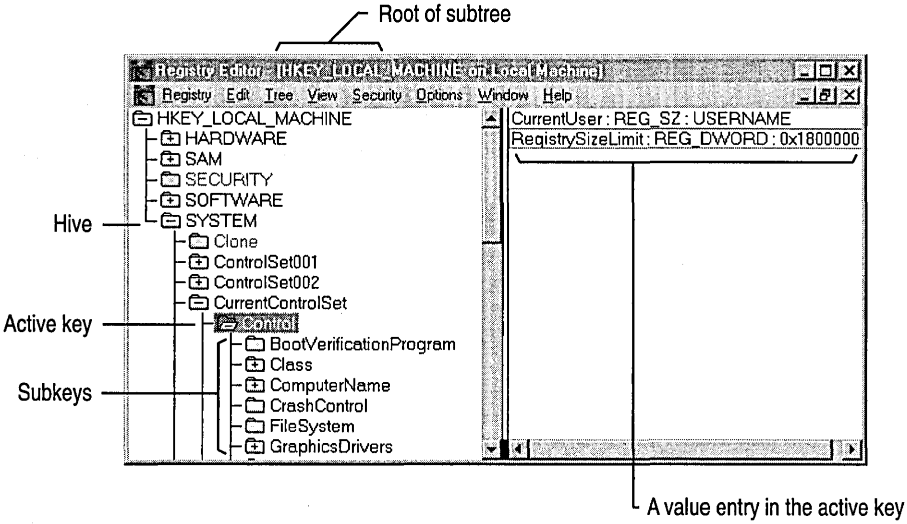

Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_CURRENT_USER on Local Machine
HKEY_USERS on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_LOCAL_MACHINE on Local Machine
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM

Your ability to make changes to the registry using Registry Editor depends on your access permissions. In general, you can make the same kinds of changes in Registry Editor as your permissions allow for Control Panel or other administrative tools.

For information about security and backup measures to take with the registry and other issues, see the *Windows NT Workstation Resource Kit* version 4.0.

Registry Editor Commands

As shown in the following figure, Registry Editor displays data in two panes. The value entries in the right pane are associated with the selected key in the left pane.


Root of subtree
Registry Editor - [HKEY_LOCAL_MACHINE on Local Machine]
Registry Edit Tree View Security Options Window Help
Hive
Active key
Subkeys
A value entry in the active key

HKEY_LOCAL_MACHINE
- HARDWARE
- SAM
- SECURITY
- SOFTWARE
- SYSTEM
  - Clone
  - ControlSet001
  - ControlSet002
  - CurrentControlSet
    - Control
      - BootVerificationProgram
      - Class
      - ComputerName
      - CrashControl
      - FileSystem
      - GraphicsDrivers

CurrentUser : REG_SZ : USERNAME
RegistrySizeLimit : REG_DWORD : 0x1800000

You can use the mouse or commands to manipulate the windows and panes in the Registry Editor in the same way as in the Windows NT Explorer. For example:

- Double-click a key name to expand or collapse an entry. Or click commands from the View and Tree menus to control the display of a selected key and its data.
- Use the mouse or arrow keys to move the vertical split bar in each window to control the size of the left and right panes.
- Click **Tile** or **Cascade** from the **Window** menu to arrange the Registry Editor windows.
- Click Auto Refresh from the Options menu to update the display continuously. You can also click one of the Refresh commands from the View menu to update the display of registry information when Auto Refresh is turned off.

Tip Turning off Auto Refresh improves the performance of Registry Editor.

The following table shows some keyboard methods for managing the display of data in each Registry Editor window.

Procedure	Keyboard action
Expand one level of a selected registry key.	Press ENTER.
Expand all of the levels of the predefined handle in the active Registry window.	Press CTRL + *.
Expand a branch of a selected registry key.	Press the asterisk (*) key on the numeric keypad.
Collapse a branch of a selected registry key.	Press ENTER or the minus (-) sign on the numeric keypad.

Registry Editors

The Windows NT Setup program installs two versions of Registry Editor: the Windows NT Registry Editor (Regedt32.exe) and, either the Windows version 3.*x* version of Registry Editor or the Windows 95 version, which are both named Regedit.exe.

The Windows NT Registry Editor is installed in the *%SystemRoot%*\system32 directory. The Windows 3.*x* version (16-bit), or the Windows 95 version (32-bit) of Registry Editor is installed in the *%SystemRoot%* directory.

Setup installs the Windows 3.*x* version of Registry Editor if one of the following occurs:

- If Setup detects that it is installing Windows NT version 4.0 in a directory that contains Windows version 3.*x*.
- If Setup detects that it is upgrading Windows NT version 3.*x* that was originally installed in a directory that contained Windows version 3.*x*.

In all other cases, Setup installs the Windows 95 version of Registry Editor in the *%SystemRoot%* directory.

Systems installed with the Windows 3.*x* version of Registry Editor can still use the Windows 95 Registry Editor. To use the Windows 95 Registry Editor, copy the following files from the Windows NT Server version 4.0 compact disc: Regedit.exe, Regedit.hlp, and Regedit.cnt.

Caution Do not copy Windows 95 Registry Editor files to the *%SystemRoot%* directory because they can overwrite the Windows version 3.*x* Registry Editor files and prevent users from installing applications when running Windows version 3.*x*. The Windows 95 registry files can be copied to any other directory.

Using Windows NT Diagnostics to View System Configuration Data

You can also use Windows NT Diagnostics to view configuration information stored in the registry. This is the recommended tool to browse for system information. It is located in the Administrative Tools (Common) folder.

Tip You cannot edit value entries using Windows NT Diagnostics, so the registry contents are protected while you browse for information. However, you can create reports and save and print them to use the values in the registry.

Initialization Files and the Registry

The registry is analogous to the initialization (.ini) files used under Windows for MS-DOS, with each key in the registry similar to a bracketed heading in an .ini file and entries under the heading similar to values in the registry. However, registry keys can contain subkeys, whereas .ini files do not support nested headings. Registry values can also consist of executable code rather than the simple strings representing values in .ini files. And unlike .ini files, individual preferences for multiple users of the same computer can be stored in the registry.

Although the registry replaces the .ini files used in versions of Microsoft Windows created for MS-DOS, some .ini files still appear in the Windows NT system directory. Also, applications created for 16-bit Microsoft Windows must still be able to read and write .ini values that were previously stored in the Win.ini or System.ini file.

This section describes how .ini files and other configuration files are used under Windows NT and how these values are stored in the registry.

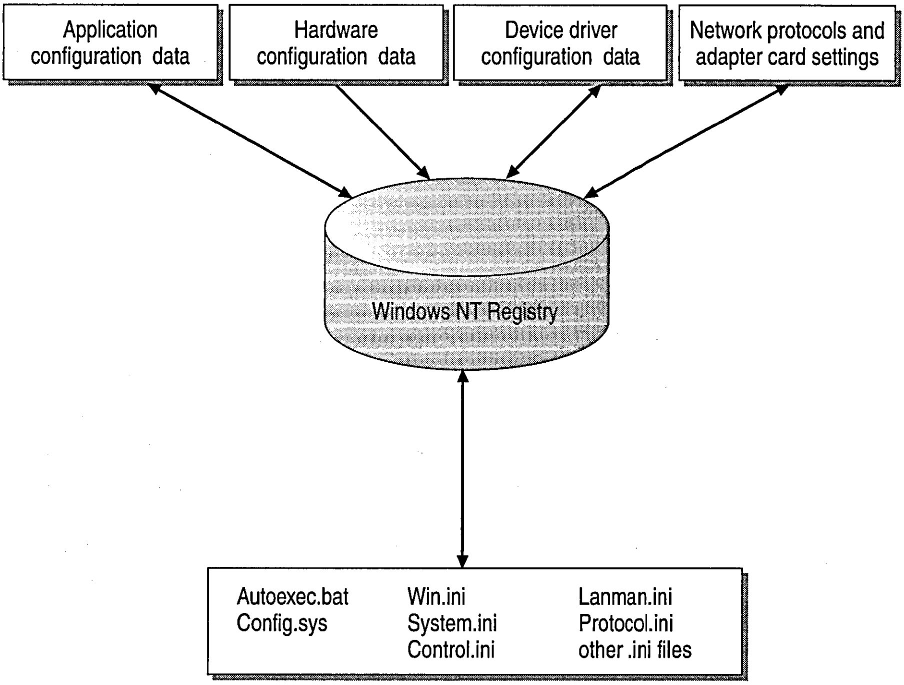
- How Windows NT uses MS-DOS configuration files
- How .ini files are mapped to the registry
- Microsoft OS/2 version 1.*x* entries in the registry
- POSIX entries in the registry

Note Although Microsoft encourages using registry entries instead of .ini files, some applications (particularly 16-bit Windows-based applications) continue to use .ini files. Windows NT supports .ini files solely for compatibility with 16-bit Windows-based applications and with related tools (such as Setup programs). Some form of the Autoexec.bat and Config.sys files also still exist to provide compatibility with applications created for MS-DOS and Windows 3.1.

For details about how Windows NT uses .ini files in conjunction with the Registry, see the *Windows NT Workstation Resource Kit* version 4.0.

How Windows NT Uses MS-DOS Configuration Files

Windows NT stores and checks the configuration information in the registry. Windows for MS-DOS involves synchronization between multiple configuration files which start the system, connect to the network, and run applications.


Application configuration data
Hardware configuration data
Device driver configuration data
Network protocols and adapter card settings
Windows NT Registry
Autoexec.bat
Config.sys
Win.ini
System.ini
Control.ini
Lanman.ini
Protocol.ini
other .ini files

Data in the Windows NT Registry

During system startup, Windows NT adds **Path**, **Prompt**, and **Set** commands from the C:\Autoexec.bat file to the Windows NT environment variables and then ignores the remainder of C:\Autoexec.bat and C:\Config.sys. (If these files are not present when you install Windows NT, the Setup program creates them.)

For a RISC-based computer, default Autoexec.nt and Config.nt files are created.

The path and other Windows NT environment information are stored under the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment
```

When an MS-DOS–based application is started, Windows NT runs the files specified in the application's PIF or the Autoexec.nt and Config.nt files in the *%SystemRoot%*\system32 directory. Changes made to these files take effect as soon as the file is saved and as soon as a new MS-DOS–based application that uses the file is started. You do not need to restart your system after changing the *.nt files.

File	Use in Windows NT
C:\Autoexec.bat	Path and environment variables are added to the Windows NT environment at system startup.
C:\Config.sys	Not used by Windows NT.
Autoexec.nt and Config.nt in *%SystemRoot%*\system32	Used every time an MS-DOS-based application is run with the _Default.pif. (Custom *.nt files can be created and used when starting an application from another PIF.)

Use the Windows NT Diagnostics program to view the contents of the Autoexec.nt files and the Config.nt files by clicking **Run** on the Windows NT Diagnostics **File** menu. Select **View autoexec.nt** or **View config.nt**. You can edit the contents of these files using Notepad.

Windows NT ignores the Autoexec.bat and Config.sys files for starting applications and initializing drivers. To have an application run automatically when you start Windows NT, drag an icon for the application to the Startup folder, as described in *Windows NT Server Start Here.* For a service or driver, use the Services option in Control Panel to define the startup type. The Services option settings are saved as the **Start** value in the service's subkey under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services in the registry.

VDM Sessions

Each MS-DOS–based and 16-bit Windows-based application runs in a Windows NT virtual MS-DOS machine (VDM). Windows NT includes the necessary virtual device drivers (VDDs) for the mouse, keyboard, printer, COM ports, and network support. The VDDs are loaded into every VDM based on values stored in the registry. Information about VDDs is found in the following registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\VirtualDeviceDrivers
```

Changes to the VDD entries are managed automatically by the system when you add a device driver using the options in Control Panel.

Windows for MS-DOS on Windows NT

Windows NT is a 32-bit environment, and Windows 3.*x* for MS-DOS is a 16-bit environment. For a 16-bit Windows-based application, Windows NT runs the application using a VDM and VDDs. This process is called WOW (for Win16 on Win32). Using a Win16 VDM, Windows NT translates Windows 3.1-based application calls in standard mode for RISC-based computers and in 386 enhanced mode for *x*86 based-computers.

Control parameters for WOW startup and for the WOW application environment are found under the following registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW
```

The settings in this key are maintained automatically by the system and should not require manual changes.

The environment settings equivalent to the System.ini file for Windows 3.*x* are found in the following registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WOW
```

The WOW subkeys have the same names as headings in the System.ini file, and the values are the same items contained in the old System.ini file. For details about these entries, see the Regentry.hlp file on the *Windows NT Workstation Resource Guide* compact disc.

How .ini Files are Mapped to the Registry

If you install Windows NT as an upgrade over Windows 3.1, all settings from the various initialization files (including Control.ini, Progman.ini, System.ini, Win.ini, Winfile.ini) are copied into the registry. To see where the Windows initialization files are mapped in the registry, view the subkeys and value entries under the following path:

```
HKEY_Local_Machine\SOFTWARE\Microsoft
    \Windows NT\CurrentVersion\IniFileMapping
```

When you install an application created for 16-bit Microsoft Windows, the application's Setup program creates its own .ini file or creates entries for the Win.ini or System.ini file in the same way that it does for any versions of Windows for MS-DOS. These entries are not updated in the registry because these applications do not know how to access the Windows NT registry. For this reason, basic System.ini, Win.ini, and Winfile.ini files appear in the *%SystemRoot%* directory in Windows NT.

If a Windows-based application tries to write to Win.ini, System.ini, or any other section listed in the **IniFileMapping** key, and if the application uses the Windows NT registry APIs, the information is stored in the registry. If the application writes to other sections of the .ini file or tries to open the .ini file directly without using the Windows NT registry APIs, the information is saved in an .ini file.

To find mapping information in the HKEY_LOCAL_MACHINE\Software key, the system looks up the *filename.ext* of the initialization file. If a match is found, the system looks under the mapped key for the specific application name and a variable name. If necessary, the system continues to look for keys whose value entries are the variable names. If no mapping for the application name or file name is found in the registry, the system looks for an .ini file. The system then reads and writes the file contents to the key.

Tables in the following section show where system settings are saved in the registry in comparison to initialization files used with Windows 3.1 for MS-DOS.

In the tables, and in the entries in the **IniFileMapping** key, the following symbols are used.

Symbol	**Description**
!	Forces all writes to go to both the registry and to the .ini file on disk.
#	Causes the registry value to be set to the value in the Windows 3.1 .ini file whenever a new user logs in for the first time after Setup, if Windows NT was installed on a computer that had Windows 3.1 already installed.
@	Prevents any reads from going to the .ini file on disk if the requested data is not found in the registry.
USR	Stands for HKEY_CURRENT_USER, and the text after the prefix is relative to that key.
SYS	Stands for HKEY_LOCAL_MACHINE\Software, and the text after the prefix is relative to that key.

Win.ini Settings in the Registry

The following table describes where you can view or edit registry entries equivalent to a Win.ini file.

WIN.INI section	**Registry path**	**Description**
[colors]	#USR\Control Panel\Colors[1]	Defines colors for the Windows display as set using the Display icon in Control Panel.
[compatibility]	#SYS...\Compatibility[3]	—

(continued)

WIN.INI section	Registry path	Description
[desktop]	#USR\Control Panel\Desktop[1]	Specifies appearance of the desktop as set using the Display icon in Control Panel.
[embedding]	#SYS...\Embedding[3]	Lists the server objects used in object linking and embedding (OLE); created during software Setup.
[extensions]	#USR...\Extensions[2]	Associates types of files with applications as set by double-clicking the program in the Windows NT Explorer.
[fonts] and**[fontSubstitutes]**	#SYS...\Fonts and \FontSubstitutes[3]	Describes the screen font files loaded by Windows as set using the Display icon in Control Panel.
[intl]	#USR\Control Panel\International[1]	Describes items for languages and locales as set using the Regional Settings icon in Control Panel.
[mci extensions]	SYS...\MCI Extensions[3]	Associates file types with Media Control Interface devices as set by double-clicking the file in the Windows NT Explorer.
[network]	USR...\Network\Persistent Connections[2]; network printers in HKEY_LOCAL_MACHINE\SYSTEM\Control\Print	Describes network printer port settings as set using the Printers folder and the persistent network connections as set using Map Network Drive.
[ports]	SYS...\Ports[3]	Lists all available printer and communications ports as set using the Ports icon in Control Panel.
[printerPorts] and **[devices]**	SYS...\PrinterPorts and \Devices[3]	Lists active and inactive output devices to be accessed by Windows as set using the Printers folder.
[sounds]	#USR\Control Panel\Sounds[1]	Lists the sound files assigned to each system event as set using the Sounds icon in Control Panel.
[TrueType]	#USR...\TrueType[2]	Describes options for using TrueType fonts as set using the Fonts icon in Control Panel.
[Windows Help]	USR\Software\Microsoft\Windows Help[1]	Lists settings for the Help window as set using the mouse or menus in any Help window.
[Windows]	#SYS...\Winlogon[3]	Specifies the Windows environment and user startup options as set using the Display, Keyboard, and Mouse icons in Control Panel.

[1] Full path = HKEY_CURRENT_USER

[2] Full path = HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion

[3] Full path = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

System.ini Settings in the Registry

When you install Windows NT, entries from a Windows for MS-DOS System.ini file are preserved under the following path:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WOW
```

The following table describes where you can view or edit entries for similar purposes in Windows NT. These entries are used by applications that look for values in the System.ini file.

System.ini section	Registry path	Description
[boot] and **[boot.description]**	#SYS...\WOW\Boot and \Boot.description[3]; replaced by...CurrentControlSet\Control	Lists drivers and Windows modules as set using the System icon in Control Panel.
[drivers]	Replaced by #SYS...\Drivers32[3]	Contains a list of aliases (or names) assigned to installable driver files as set using the Multimedia and Devices icons in Control Panel.
[keyboard]	#SYS...\WOW\Keyboard[3];#USR\Keyboard Layout[1]	Contains information about the keyboard as set using the Regional Settings icon in Control Panel or identified by the Hardware Detector.
[mci] and **[mci32]**	Replaced by #SYS...\MCI and \MCI32[3] and #SYS...\Drivers.desc[3]	Lists Media Control Interface (MCI) drivers as set using the Multimedia icon in Control Panel.
[NonWindows App]	#SYS...\WOW\NonWindowsApp[3]	Contains information used by non-Windows-based applications as defined in PIFs for specific applications or in Config.nt.
[standard]	Standard in #SYS...\WOW[3]	Contains information used by Windows for MS-DOS in standard and 386 enhanced mode. All memory management is handled automatically by Windows NT.

[1] Full path = HKEY_CURRENT_USER

[2] Full path = HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion

[3] Full path = HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows NT\CurrentVersion

Other Initialization File Settings in the Registry

The following table describes where you can view or edit registry entries equivalent to Control.ini, Progman.ini, and Winfile.ini entries.

.ini file section	Registry path	Description
CONTROL.ini**[Current]**, **[Color Schemes]**, **[Custom Colors]**	Color Schemes, Current, and Custom Colors subkeys in #USR \Control Panel[1]	Describes color schemes and custom colors as set using the Display icon in Control Panel.
CONTROL.ini**[Patterns]** and **[Screen Saver*]**	Patterns and Screen Saver.*x* subkeys in #USR\Control Panel[1]	Describes elements of desktop appearance and performance as set using the Display icon in Control Panel.
CONTROL.ini **[MMCPL]**, **[Drivers.Desc]**,**[Userinstallable.drivers]**	#USR\Control Panel\MMCPL[1];#SYS...\Drivers.Desc and \Userinstallable.drivers[3]	Contains values for installable drivers and devices used for multimedia as set using the Multimedia icon in Control Panel.
PROGMAN.ini**[groups]**,**[restrictions]**,**[settings]**	Groups, Restrictions, and Settings subkeys in #USR...\Program Manager[2]	Describes window appearance, folders and the icons in the folders, and restrictions on Task Bar operations; restrictions are set in User Manager for Domains (Server only).
WINFILE.ini **[settings]**	#USR...\File Manager[2]	Describes the appearance and behavior of items in the Windows NT Explorer.

[1] Full path = HKEY_CURRENT_USER

[2] Full path = HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion

[3] Full path = HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows NT\CurrentVersion

Microsoft OS/2 Version 1.x Entries in the Registry

The Microsoft OS/2 version 1.*x* subsystem starts whenever a user starts an OS/2 character-based application on an *x*86-based computer. The registry entries for the OS/2 subsystem are found under this path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems
```

The Os2 entry in this subkey describes the path to the executable file used to start the OS/2 subsystem. The directory path for the OS/2 library is the Os2LibPath value defined under the Session Manager\Environment subkey.

If Setup finds a copy of Config.sys for OS/2 when Windows NT is installed, a copy is placed in the *%SystemRoot%*\system32 directory. This information is used to configure the OS/2 subsystem whenever an OS/2 application is started. If a Config.sys file is not found, a substitute with the following values is created in the Registry:

```
PROTSHELL=C:\os2\pmshell.exe c:\os2\os2.ini c:\os2\os2sys.ini
    %SystemRoot%\system32\cmd.exeSET
COMSPEC=%SystemRoot%\system32\cmd.exe
```

The OS/2 Config.sys information is stored in the following registry entry, which appears only after an OS/2 application has been run on the system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT\config.sys
```

The other subkeys under the OS/2 Subsystem key do not contain entries.

If you subsequently edit the C:\Config.sys file using a text editor, LIBPTH=, SET PATH=, and Set WINDIR= entries are appended to the end of the file from the Windows NT environment. Any changes made to the path or environment variables take effect after the system is shut down and restarted.

For details about managing this environment under Windows NT, see Appendix B "Other Application Environments."

You can disable an OS/2 subsystem in Windows NT and still run a bound application under a VDM. Many bound applications run better under a VDM than under the OS/2 subsystem.

▶ **To disable the OS/2 subsystem in Windows NT**

- In Registry Editor, change the value of GlobalFlag to 20100000 in the following registry path:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SessionManager
  ```

You can also use Forcedos.exe, a tool supplied in the *%SystemRoot%*\system32 subdirectory. This tool enables you to run a bound application under a VDM. For information about how to use the ForceDOS tool, type **forcedos /?** at the command prompt.

POSIX Entries in the Registry

The POSIX subsystem starts whenever a user starts a POSIX application. The registry entries for the POSIX subsystem are found under this path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems
```

The **Posix** entry in this subkey describes the path to the executable file used to start the POSIX subsystem. The POSIX subsystem does not have any parameters or environmental variables that the user can set.

POSIX utilities and their source code are available on the *Windows NT Workstation Resource Kit* compact disc.

APPENDIX B

Other Application Environments

In addition to 32-bit applications designed for Windows NT, Windows NT supports applications designed for the following environments: Windows 3.*x*, MS-DOS, 16-bit OS/2, and POSIX.

This chapter provides information on these environments, including the following topics:

- How Windows NT runs applications
- The Windows 3.*x* environment
- The MS-DOS environment
- The OS/2 environment
- Setting up and starting applications

How Windows NT Runs Applications

Windows NT is a modular operating system that uses operating subsystems to run applications. Each subsystem provides a different operating environment for applications. Windows NT runs Windows 3.*x*, MS-DOS, 16-bit OS/2, and POSIX based applications in addition to 32-bit applications designed for Windows NT and most 32-bit applications developed for Windows 95.

The following table shows the Windows NT subsystems and the applications each subsystem supports.

Subsystem	**Supports**
Windows (16-bit)	MS-DOS, and Windows 3.*x* based applications
OS/2	16-bit character-based OS/2 applications (on *x*86-based computers only)
POSIX	POSIX applications compliant with IEEE Std 1003.1 and compiled using Windows NT

The Windows NT Executive is the portion of the operating system at the center of Windows NT that manages processes and memory. You can think of a process as a discrete set of computing tasks. When you run Windows 3.*x*-based applications, applications run by default as tasks within a single process.

Each process is protected. That is, the Executive makes sure that each process runs in its own area of the computer's memory so that processes cannot interfere with one another. If an application fails, that failure will not affect the rest of the system.

You can start any application from the **Start** menu, Windows NT Explorer, or from the command prompt without concern for the operating environment the application requires. This functionality enables full interaction among applications.

Supported Applications

Windows NT can run most Windows 95, Windows 3.*x*, MS-DOS, and 16-bit character-based OS/2 applications. Applications not designed for Windows NT or Windows 95 sometimes use device drivers that attempt to communicate with computer hardware directly. To protect the integrity of the operating environment, such drivers are prevented from being installed with the application. A device driver designed to run with Windows NT is required.

If you have an application that requires but does not supply a Windows NT-compatible device driver, contact the application's manufacturer for the availability of a Windows NT-compatible driver. In some cases, the manufacturer may have developed a version of the application that is fully compatible with Windows NT.

The following types of existing applications require either Windows NT-compatible device drivers or an application upgrade:

- Applications that directly communicate with hardware; for example, FAX cards, scanner cards, or terminal emulation cards
- Applications that rely on their own disk device drivers; for example, applications that increase hard disk capacity
- Applications that communicate directly with disk drives; for example, disk maintenance applications
- Applications that rely on their own graphics device drivers to communicate with the hardware; for example, applications that use private printer drivers

Windows 3.*x* Environment

Windows NT provides a complete operating environment for Windows 3.*x*-based applications. The environment is comparable to the enhanced mode environment in Windows 3.*x*.

On RISC-based computers, Windows NT provides a 486 emulator that runs applications designed for 286, 386, or higher processors.

Configuring the Windows 3.*x* Environment

When you install Windows NT, the Setup program checks to see whether a previous version of Windows NT or Windows 3.*x* is installed on the computer. If it is, you should install Windows NT in the same directory as Windows 3.*x*. Windows NT then configures its environment based on the existing environment, enabling Windows NT to support all the features of currently installed Windows 3.*x*-based applications.

Windows 3.*x* stores configuration information in the Win.ini and System.ini files. Windows NT stores configuration information in the registry. However, the Win.ini and System.ini files are retained in Windows NT for use by Windows 3.*x*-based applications. For more information about how Windows NT uses configuration files, see Appendix A, "Windows NT Registry."

If you installed Windows NT in the same directory as Windows 3.*x*, the first time you log on to Windows NT, Windows NT migrates any program groups that are not predefined for Windows NT and the settings that configure your desktop. The Windows 3.*x* program groups appear as folders on the **Start** menu.

If you later install a new application while running Windows 3.*x*, Windows NT does not automatically gather file association and object linking and embedding (OLE) information for the new application when you start Windows NT.

Running a Windows 3.*x*-Based Application in Separate Memory

When you start a Windows 3.*x*-based application, by default it runs in the same memory space as the first Windows 3.*x*-based application you started. If several Windows 3.*x*-based applications are running in the same memory space when one of the applications crash, all the applications become unavailable. You can, however, run each application in its own memory space.

Running a Windows 3.*x*-based application in a separate memory space prevents the application from affecting other Windows 3.*x*-based applications if the application crashes or hangs. However, the performance of Windows NT could be slower if several Windows 3.*x*-based applications are each run in their own memory spaces. Running Windows 3.*x*-based applications in separate memory spaces uses more memory.

Running a Windows 3.*x*-based application in a separate memory space also prevents the application from sharing memory with other Windows 3.*x*-based applications. Some applications rely on the shared memory space to work with other applications. However, cross-application communication using OLE or dynamic data exchange (DDE) still works if you run one application in a separate memory space.

For information about how to run a Windows 3.*x*-based application in its own memory space, or create a shortcut for a Windows 3.*x*-based application to run in its own memory space, see “Running a Windows 3.1 application under Windows NT in Help.

MS-DOS Environment

Windows NT provides a complete operating environment for MS-DOS applications.

- Expanded memory is emulated for applications that require it.
- On *x*86-based computers, character-based applications run either in a window or the full-screen mode. Applications that use graphics run in the full-screen mode.
- On RISC-based computers, character-based and graphics-based applications run in a window only. You can change the size of the window using the **Properties** command on the **Control** menu. Click the **Layout** tab.

Configuring the MS-DOS Environment

During system startup, Windows NT adds **Path**, **Prompt**, and **Set** commands from the C:\Autoexec.bat file to the Windows NT environment variables and then ignores the remainder of C:\Autoexec.bat and C:\Config.sys. (If these files are not present when you install Windows NT, the Setup program creates them.)

For a RISC-based computer, default Autoexec.nt and Config.nt files are created.

File	Use in Windows NT
C:\Autoexec.bat	Path and environment variables are added to the Windows NT environment at system startup.
C:\Config.sys	Not used by Windows NT.
Autoexec.nt and Config.nt in *%SystemRoot%*\system32	Used every time an MS-DOS-based application is run with the _Default.pif. (Custom *.nt files can be created and used when starting an application from another PIF.)

When you log on to Windows NT, the path and environment variables stored in the Autoexec.bat file are appended to the Windows NT path and environment settings. Because this portion of the operating environment is established when you log onto Windows NT, the values set for the path and environment variables are available to each application you use. If you change values in Autoexec.bat, Autoexec.nt, or Config.nt, you must log off and log on to Windows NT again so that the changes take effect.

Environment variables can also be changed using the System option in Control Panel. Click the **Environment** tab. For more information about environment variables, see "Using Environment Variables to Manage Workstations" in Chapter 3, "Managing User Work Environments."

When you start an application in a new command window, Windows NT reads the Config.nt and Autoexec.nt files to configure the environment for the application. If, for example, you change an application's driver in the Config.nt file, restarting the application puts the change into effect. You can edit the Config.nt and Autoexec.nt files just as you would CONFIG.SYS and Autoexec.bat. Config.nt and Autoexec.nt are located in the *%SystemRoot%*\system32 directory.

As with Windows 3.*x*, Windows NT enables you to customize the environment for each MS-DOS-based application with program information files (PIFs). However in Windows NT version 4.0, PIFs are only created when you create a shortcut for the application. For information about how to create PIFs, see "New PIF handling in Windows NT" in Help.

Commands Available in Config.nt

Windows NT supports the configuration commands shown in the following table. If you include commands in your Config.nt file that are not supported, Windows NT ignores them. For more information about Windows NT commands, see the online Command Reference.

Command	Function
country	Sets the language conventions for a specific country.
device	Loads an installable device driver. If necessary, you can load drivers that control memory, such as Himem.sys, or that control character-based display, such as Ansi.sys.
dos	Specifies how the upper memory area will be used.
dosonly	Prevents starting applications other than MS-DOS–based applications from the Command.com prompt.
echoconfig	Switches on the display of Config.nt and Autoexec.nt messages when you start an application.

(continued)

Command	Function
fcbs	Sets the number of file control blocks (FCBs) that can be opened concurrently.
files	Sets the number of files that can be open at one time.
install	Loads a memory-resident program into memory.
loadhigh	Loads device drivers into the upper memory area.
ntcmdprompt	Runs the Windows NT command interpreter, Cmd.exe, rather than Command.com after running a terminate-and-stay-resident (TSR) application or after starting the command prompt from within an MS-DOS–based application.
rem	Marks lines in the Config.nt file as comments (remarks).
shell	Specifies the command interpreter. Only the Windows NT command interpreter is supported.
stacks	Sets the amount of RAM reserved for processing hardware interrupts.

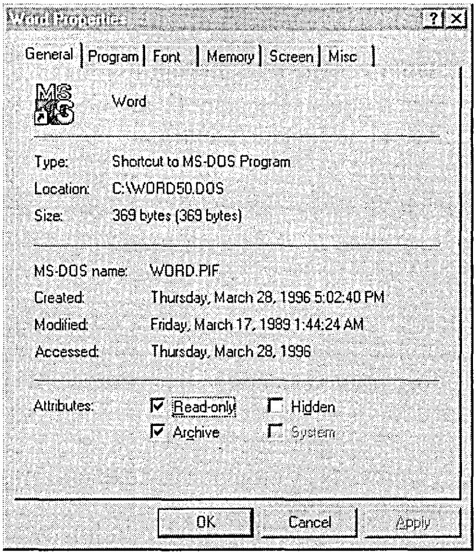
Commands Available in Autoexec.nt

Windows NT supports a similar range of commands as MS-DOS for use in the Autoexec.nt file. For more information about Windows NT commands, see the Command Reference in Help.

Using Program Information Files

A program information file (PIF) provides information to Windows NT about how best to run MS-DOS applications. Windows 3.*x*, OS/2, and POSIX based applications do not use or require PIFs. When you start an MS-DOS application, Windows NT looks for a PIF to use with the application. If you have been using a PIF to run an application in Windows 3.*x*, you can continue to use it with Windows NT. For information about how to use PIFs, see "New PIF Handling in Windows NT" in Help.

To create, modify, and save PIFs, right-click the application file name in Windows NT Explorer. If you click **OK** after changing any of the settings in the **Properties** dialog box, you create a PIF (a shortcut) for the application. Typically, a PIF has the same file name as the associated application's main program file, except that a PIF has the .pif extension. You can change the PIF file name, but do not change the extension.



Word

Type: Shortcut to MS-DOS Program
Location: C:\WORD50.DOS
Size: 369 bytes (369 bytes)

MS-DOS name: WORD.PIF
Created: Thursday, March 28, 1996 5:02:40 PM
Modified: Friday, March 17, 1989 1:44:24 AM
Accessed: Thursday, March 28, 1996

Attributes: ☑ Read-only ☐ Hidden
☑ Archive ☐ System

Some software manufacturers provide a PIF for an application. To determine whether a PIF has been supplied, contact the software manufacturer or search the disks for a file that has a .pif extension. For information about how to implement a manufacturer-supplied PIF file, see "Using a manufacturer-supplied PIF file" in Help.

Windows NT includes a PIF named _Default.pif, located in the *%SystemRoot%* folder. The _Default.pif file contains settings that work with most MS-DOS–based applications. Windows NT uses this PIF when it is the only one available for MS-DOS–based applications. You should not change the settings in the _Default.pif file because Windows NT uses this file for every MS-DOS–based application.

For information about how to create or edit a PIF and other PIF options, see "New PIF handling in Windows NT" in Help.

Using Multiple PIFs for an Application

You can create more than one PIF for an application. You can create several PIFs if you run an application differently under different circumstances.

For example, you can specify in a PIF how much EMS (expanded) memory an application has access to. By using two PIFs, you can give an application access to a large amount of EMS memory when you're using large data files but limit its use of memory when you are working with smaller files.

For information about how to set up two PIFs for an application, see "Creating two PIFs for an application" in Help.

Custom Startup Files

Windows NT enables you to create custom startup files that you can specify in an application's PIF. When you start the application, Windows NT reads the custom files you specify rather than the Config.nt and Autoexec.nt files. Specifying custom startup files enables you to create a custom MS-DOS environment for each application you use. For example, if one of your applications requires a memory-resident program when it runs, you can include the name of that program in a custom startup file. When you start the application using its PIF, Windows NT automatically starts the memory-resident program.

When you create startup files, base them on the Autoexec.nt and Config.nt files. That way, the basic information needed to configure the MS-DOS environment will already be included in your files. In configuration files, Windows NT uses the variable *%SystemRoot%* to represent the Windows NT directory. When processing the files, Windows NT automatically expands this variable.

For information about how to create custom startup files, see "Creating custom startup files for an MS-DOS program" in Help.

Running Memory-Resident Programs

Windows NT supports MS-DOS memory-resident programs, also called pop-up and terminate-and-stay-resident (TSR) programs. Like any MS-DOS–based application you run in Windows NT, memory-resident programs run in the window in which they are started and can be used only within that window. MS-DOS–based TSR programs can function reliably only when running alone or with other MS-DOS–based applications.

In general, you should not start memory-resident programs from your Autoexec.nt or Config.nt files. If you do, each time you start an application that reads the Autoexec.nt or Config.nt files, you will also start another copy of the memory-resident program, thereby wasting memory. Start the TSR-based application just as you would any other application in Windows NT.

If one of your applications requires a memory-resident program to work properly, start the memory-resident program and then start the application in the same command window. You can also create a custom startup file that starts the memory resident program, and then specify that startup file in the application's PIF. For more information about custom startup files, see "Custom Startup Files" earlier in this appendix.

When you quit an MS-DOS–based application, Windows NT returns to the Windows NT command interpreter, Cmd.exe. However, by default, when you run a TSR or temporarily suspend an MS-DOS–based application to return to the command prompt, Windows NT runs Command.com, the command interpreter for the MS-DOS environment. This preserves the MS-DOS environment, allowing you to use the TSR immediately. Because starting and running other types of applications from the Command.com prompt can disrupt a TSR or suspended MS-DOS–based application, Windows NT provides the **dosonly** command. The **dosonly** command enables only MS-DOS–based applications to be started from the Command.com prompt. You can include the **dosonly** command in your Config.nt file or the equivalent custom startup file in an application's PIF.

When Command.com is running, some features of the Windows NT command prompt, such as the Doskey display of command history, are not available. If you would prefer to run the Windows NT command interpreter after you have started a TSR or started the command prompt from within an MS-DOS–based application, you can use the **ntcmdprompt** command. However, keep in mind that the TSR may not be available for use when you are running Cmd.exe. You can include the **ntcmdprompt** command in your Config.nt file or the equivalent custom startup file in an application's PIF.

OS/2 Environment

Windows NT supports 16-bit character-based OS/2 applications on *x*86-based computers only. OS/2 bound applications (applications that can run under both OS/2 and MS-DOS) run on RISC-based computers using the MS-DOS subsystem.

Configuring the OS/2 Environment

When Windows NT starts for the first time, it checks the registry for OS/2 subsystem configuration information. If none is found, it looks for information in the original Config.sys file and adds the information to the registry. If the original Config.sys file does not exist or is not an OS/2 configuration file, the subsystem adds the following default information to the registry:

```
PROTSHELL=c:\os2\pmshell.exe c:\os2\os2.ini c:\os2\os2sys.ini
   %SystemRoot%\system32\cmd.exe
SET COMSPEC=%SystemRoot%\system32\cmd.exe
```

The subsystem updates the environment variable Os2LibPath with LIBPATH information found in the original Config.sys file. The updated Os2LibPath is *%SystemRoot%*\system32\os2\dll concatenated with the list of directories specified in the LIBPATH line of the original Config.sys file.

Windows NT supports the OS/2 configuration commands shown in the following table. If you use commands that are not supported, Windows NT ignores them.

Command	Function
protshell	Specifies the command interpreter. Only the Windows NT command interpreter is supported.
devicename	Specifies a user-defined Windows NT device driver used by OS/2 applications.
libpath	Specifies the location of OS/2 16-bit dynamic-link libraries.
set	Sets environment variables.
country	Sets a country code that defines country-dependent information such as time, date, and currency conventions.
codepage	Specifies which code pages your system is prepared to use.
devinfo=KBD	Specifies the information the keyboard needs in order to use a particular code page.

The **libpath**, **set**, and **devicename** commands are processed as follows:

- In Config.sys, **libpath** appends path information to the OS/2 library path in the Windows NT environment. At the command prompt, you can change the library path for OS/2 applications only for the current Command Prompt window by using the **set os2libpath** command.
- To change the OS/2 library path permanently, you must change the Os2LibPath system environment variable using the System option in Control Panel. For more information about environment variables, see "Using Environment Variables to Manage Workstations" in Chapter 3, "Managing User Work Environments."
- The following **set** commands are ignored in Config.sys:

  set vio_ibmvga **set vio_vga** **set prompt**

  set compspec **set video_devices**

- **devicename** specifies a device driver compatible with Windows NT for use with an OS/2 application. The syntax of the command is:

  ```
  DEVICENAME=OS/2devicename [[path][NTdevicename]]
  ```

  Devicename is the logical name OS/2 applications use to address the device. *Path* and *NTdevicename* specify the Windows NT device driver to which the OS/2 device name is mapped. If these are not specified, the device is mapped to \DEVICE\os/2devicename.

Changing OS/2 Configuration Information

Although the OS/2 configuration information is stored in the registry, you can edit that information just as you would edit an OS/2 Config.sys file. To edit the information, you must use an OS/2 text editor.

To change configuration information, you must be logged on as a member of the Administrators group. For additional information about how to change configuration information, see "Changing configuration information" in Help.

Setting Up and Starting Applications

Follow the manufacturer's instruction to install Windows 3.*x*, MS-DOS, OS/2, or POSIX based applications.

When you use the manufacturer's instructions to install an MS-DOS–based application, Windows NT either creates a PIF, uses the PIF that accompanies the application, or uses the _Default.pif file supplied with Windows NT. Windows 3.*x*, OS/2, and POSIX based applications do not use PIFs.

When you use the **Run** command on the **Start** menu to start an MS-DOS–based application, Windows NT searches for a PIF to use with the MS-DOS–based application:

- If it finds one, Windows NT starts the application using the PIF.
- If no PIF is available, Windows NT uses _Default.pif.

For more information about _Default.pif, see "Using Program Information Files" earlier in this chapter.

Using an Application's Own Mouse Cursor

Some MS-DOS–based applications use a mouse cursor that cannot be synchronized with the system mouse pointer used by Windows NT. If the system mouse pointer does not work as you expect with an MS-DOS–based application, you can hide the system pointer which returns control of the mouse cursor to the application.

For information about how to hide and display the system mouse pointer, see "Hiding the system mouse pointer" in Help.

Starting an Application

You can start applications for all supported application environments using the **Run** command on the **Start** menu, Windows NT Explorer, or the command prompt.

When you start an MS-DOS–based application at the command prompt, Windows NT uses _Default.pif to establish the MS-DOS environment. The following PIF settings in _Default.pif are used to establish the environment:

Expanded (EMS) memory

Extended (XMS) memory

Miscellaneous Multitasking Options (such as Windows shortcut keys)

Application shortcut key

Custom MS-DOS initialization files

Compatible Timer Hardware Emulation

To start an MS-DOS–based application at the command prompt using its PIF, use the **start** command. For example, to start Myapp.exe using Myapp.pif, type **start myapp**. The first MS-DOS–based application started at the command prompt establishes the MS-DOS environment for all MS-DOS–based applications run in that window.

In a few cases, Windows NT may not recognize that a program is MS-DOS based. If an MS-DOS–based application fails to start, try starting it using the **forcedos** command. For example, to start a program called MYPROG in the \Oldapps directory, type **forcedos \oldapps\myprog** at the command prompt.

If a Subsystem Does Not Start

If services or subsystems do not start properly, use the Services or Devices options in Control Panel to check their status. You can try to start services using the Services option and start a device with the Devices option. Also, check the system log in Event Viewer for entries relating to the problem. Event Viewer is in the Administrative Tools (Common) folder.

Interoperability with Windows for Workgroups

When setting up your network, check the issues to ensure smooth interoperability between Windows NT and Windows for Workgroups.

- Browsing is not available if you log on to a Windows for Workgroups computer whose workgroup name is the same as the name of a Windows NT Server domain or if the user name and password are not valid for the domain. If you want to browse the domain, log on with another user name and password that are valid in the domain.

- Guest accounts should remain enabled on domain controllers. Instead of removing guest accounts to restrict access to certain services, just remove any unwanted guest account rights in User Manager for Domains.
- Avoid duplicate user names on different domains. If a user name is duplicated across different domains, logging on produces different results on the Windows NT network and the Windows for Workgroups computer.
- If you seem to have password problems logging on to Windows for Workgroups, delete your passwords list (the .pwl file with your username in the Windows directory). The next time you log on, you will be asked for your password, and a new list will be created.

Running Windows 3.*x*-based Mainframe Connectivity Software

Some Windows 3.*x*-based software for connecting to mainframe computers requires a memory-resident program to operate correctly. Such software includes Access for Windows 3270 from Eicon Technology, Extra! for Windows from Attachmate, and Rumba from Wall Data.

When these programs run under 16-bit Windows 3.*x*, they add a command to Autoexec.bat to start the memory-resident program, or they require the user to start the memory-resident program through a batch file that must be run manually before starting Windows.

To run any of these memory-resident programs with Windows NT Server, add the command for starting the program to the Autoexec.nt file. To find the command used to start the memory-resident program, check Autoexec.bat or the batch file used to start the program under MS-DOS.

Autoexec.nt is stored with other Windows NT Server program files, usually in the *%SsystemRoot%*\system32 directory. Add the line with the command for starting the memory-resident program after the line containing Redir.exe in Autoexec.nt. Then restart your computer before starting the connectivity application.

Index

* 6 9 9 4 0 *

Recyclable Paper

Microsoft®