MICROSOFT®
WINDOWS NT™

Microsoft® SUPPORTING WINDOWS NT™ SERVER

Study Guide for the Microsoft Windows NT Server Version 3.5 Certified Professional Exam

Microsoft Press

Microsoft® SUPPORTING WINDOWS NT™ SERVER

Study Guide for the Microsoft Windows NT Server Version 3.5 Certified Professional Exam

Microsoft® Press

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Printed and bound in the United States of America.

4 5 6 7 8 9 MLML 0 9 8 7 6 5

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office. Or contact Microsoft Press International directly at fax (206) 936-7329.

Project Lead: Cindy Tompkins
Instructional Designers: Jeff Madden, Susan Greenberg, and Marilyn McGill
Subject Matter Experts: Wally Mead, Beth Nelson, and Keith Cotton
Manufacturing Support: Bo Galford
Graphics: Julie Stone
Production Support: Barnett Communications
Editing: Fjord Press
Indexing: Veronica Maier and Jane Dow

Contents

Figures

FOREWORD

Supporting Microsoft® Windows NT™ Server 3.5: Self-Paced Training

When I first came to Microsoft in 1990, the company was about to launch LAN Manager 2.0, a system that was designed to be as good a file server as NetWare, but which could also run server applications. The problem was that this early version of LAN Manager wasn't quite as fast as NetWare as a file server, and there weren't really any server applications.

By 1991, we had fixed the file server performance problem with LAN Manager when we released LAN Manager 2.1. Although the 16-bit OS/2 environment was adequate for small workgroup application servers, it did not really meet the needs of large business-critical loads. Customers needed a minicomputer substitute, but LAN Manager on OS/2 could not deliver.

In 1993, Microsoft shipped Windows NT Advanced Server 3.1. Combined with a new generation of hardware that could deliver the performance of minicomputers costing ten or twenty times as much, the first version of Windows NT was an excellent application server. Because the industry had delivered a full complement of development tools, independent software vendors began porting their applications to Windows NT.

Although the early reviews of Windows NT Advanced Server 3.1 were positive in terms of its application server performance, it did not deliver the file server performance necessary to compete with NetWare. Windows NT 3.1 did support IPX, the same network protocol that customers used with NetWare, so many NetWare customers began using Windows NT as an application server right alongside the NetWare file servers.

As work began on Windows NT Server 3.5, Microsoft focused on three primary goals:

- Improve Windows NT Server's file server performance
- Make it easier to set up and manage Windows NT Servers
- Improve the networking capabilities of the product

When we shipped Windows NT Server 3.5 in September of 1994, we solved a problem that Microsoft and the industry had been focusing on for over eight years. Windows NT Server 3.5 is a network operating system that is the foundation for a new generation of applications. It delivered the application server performance of UNIX, and most reviewers agree that it now boasts file server performance that is competitive with any other server operating system, even NetWare.

Dave Cutler and his team built Windows NT Server to meet customer demand for a server operating system that could harness the new generation of hardware, and they delivered a multipurpose system which can be the minicomputer substitute that customers have been waiting for.

As you begin learning more about Windows NT Server, the first thing that you will notice is how easy it is to install. Installing Windows NT Server from CD-ROM takes a beginner about 45 minutes. Once you get running, you will also find that the designers spent a lot of time making it easier to do the things that you do most often.

When you begin installing Windows NT Server in existing networks, you will find it is the most network-agnostic network operating system available. In general, Windows NT Server doesn't care whether you are using NetBEUI, IPX, or TCP/IP—so we included them all.

Windows NT Server 3.5 is a complete network server. It has directory service, which provides: a single network logon, security and centralized management. With Windows NT Server 3.5 you get simplified, dynamic management of TCP/IP addresses using automatic network name management. Windows NT Server 3.5 includes remote networking that provides complete, secure dial-in access for remote users to connect to any network, including SNA networks and the Internet. Windows NT Server is also the best server platform for Macintosh clients.

Delivering on the vision of distributed computing, Windows NT Server is the single foundation for the future. Windows NT Server is the right decision today that will not need to be changed in the future.

More and more companies are deploying Windows NT Server–based solutions to achieve mission-critical business functions. Company decision-makers have cited robustness, flexibility, ease of use, and business value as reasons why they chose to adopt Windows NT Server.

The demand for implementation of Windows NT–based systems within corporations is leading to a surge in training requests. Training enrollment is driving revenue growth for companies certified as trainers for Windows NT–based development and implementation.

As you read this book, you will find that managing the setup and support of networks doesn't have to be complicated. As you begin working with the product, I think you will also find that there has never been a server operating system that gives you the opportunity to look so good.

Mike Nash
Windows NT Server Product Manager
January 20, 1995

About This Book

Welcome to *Supporting Microsoft® Windows NT™ Server 3.5: Self-Paced Training*. This book provides the knowledge and skills to plan, install, configure, customize, optimize, and integrate networks with Windows NT Server 3.5, and it prepares you to meet the certification requirements to become a Microsoft Windows NT Server 3.5 Certified Professional.

Each chapter in this book is divided into lessons. Most lessons include hands-on procedures to practice or demonstrate the concept or skill presented in the lesson, or a set of review questions to test your knowledge. At the end of each lesson is a short summary. If appropriate, there are references to further information on the lesson material or related topics.

The lesson disks contain supplemental files required to perform the hands-on procedures.

Video

The "Microsoft Windows NT 3.5 Server" video provided in this kit supplements the key Windows NT Server concepts covered in this book. We recommend that you begin by watching this video and then use it as a review tool while you work through the material.

Reference Materials

You need the Windows NT Server 3.5 documentation to complete the lessons in this book. In addition, you will find the following reference material useful.

- Windows NT Workstation 3.5 documentation
- Windows NT 3.5 Resource Kit

Intended Audience

This book is designed for network support professionals who install, configure, and support Windows NT Server 3.5.

Prerequisites

Before taking this self-paced training, you should have completed the *Support Fundamentals for Windows NT Workstation 3.5: Self-Paced Training* book or have equivalent knowledge.

Finding the Best Starting Point for You

This book is designed for you to complete at your own pace, and so you can skip some lessons and revisit them later. Use the following table to find the best starting point for you.

If you	Follow this learning path
Are preparing to take the Certified Professional Examination	Read the following section, "Getting Started," Next, work through Chapters 1–5. Work through the other chapters in any order.
Need to install and configure a small network	Read the following section, "Getting Started." Next, work through Chapters 1–4. Work through the other chapters in any order. If a chapter requires Trust Relationships, complete Chapter 5.
Need to install and configure multiple departments, groups, or computers	Read the following section, "Getting Started." Next, work through Chapters 1–5. Work through the other chapters in any order.
Need to install and configure TCP/IP	Read the following section, "Getting Started." Next, work through Chapter 1. Then complete Chapters 7 and 8.
Need information on a specific topic related to Windows NT Server	Refer to the Table of Contents or Index.

Chapter and Appendix Overview

This self-paced training combines notes, hands-on procedures, and review questions to teach you how to support Windows NT Server 3.5. It is designed to be completed from beginning to end, but you can choose a customized track and complete only the sections that interest you. If you choose the customized track option, see the "Before You Begin" section in each chapter. Any hands-on procedures that require preliminary work from previous chapters will refer to the appropriate chapters.

The self-paced training is divided into 11 chapters and six appendix:

- The "About This Book" section contains a self-paced training overview and introduces the components of this training. Read this section thoroughly to get the greatest educational value from this self-paced training and to plan which lessons you will complete.
- The "Getting Started" section contains preliminary information necessary for completing this training. It explains concepts and defines terms that are used in Chapter 1 and throughout the book.
- Chapter 1, "Installing Windows NT Server," gives you the knowledge and skills to install, upgrade, and configure Windows NT Server. You have the opportunity to install and configure Windows NT Server to function as a primary domain controller (PDC).
- Chapter 2, "Using Groups to Manage Users," covers the different types of groups that are used to manage a user's access to resources, and how groups are implemented in a single domain. You have the opportunity to create both local and global groups, add a global group to a local group, and then use global and local groups to perform domain administration and to access domain resources.
- Chapter 3, "Configuring the User Environment," gives you the knowledge and skills to configure the user environment with user profiles and logon scripts. You will have the opportunity to create user profiles and logon scripts that configure the desktop environment.
- Chapter 4, "Configuring the Server Environment," gives you the knowledge and skills to configure and manage servers using Server Manager. You will have the opportunity to use Server Manager to add a computer to a domain; install a backup domain controller (BDC); synchronize domain controllers; promote a backup domain controller to the role of primary domain controller; and remotely administer a service on a different domain controller.
- Chapter 5, "Establishing Trust Relationships Between Domains," gives you the knowledge and skills to plan and implement trust relationships in a master domain, multiple master domain, and complete trust domain. You will have an opportunity to implement the master domain model and learn about group strategies.
- Chapter 6, "Protecting Server Data," covers how to implement fault tolerance functions, such as striping with parity and disk mirroring. You will have the opportunity to implement disk striping with parity and/or disk mirroring, depending on your hardware configuration. Information will also be provided on creating a fault-tolerant boot disk and recovering data.

Important The hands-on procedures in this chapter require additional hard disks. Refer to the "Hardware and Software Requirements" section for detailed information.

- Chapter 7, "Implementing TCP/IP," gives you the basic knowledge and skills to install and configure Microsoft TCP/IP. You will have the opportunity to manually configure an IP address, Subnet Mask, and default gateways, use the ping utility to test the configuration and diagnose a common configuration problem, and then install and configure DHCP to configure TCP/IP parameters automatically.
- Chapter 8, "Browsing Network Resources," gives an overview of the Windows NT Server Computer Browser service, types of browser servers, and multiple domain and wide-area network browsing issues. You will have the opportunity to design browsing for a wide-area network domain, based on a scenario.
- Chapter 9, "Installing Microsoft Network Client Software," describes the MS-DOS® client software that is included in the Windows NT Server package, how to use the Windows NT Network Client Administrator, and how to install and use the client-based network administration tools. You will have an opportunity to use the Network Client Administrator to create a startup disk, install Windows for Workgroups using a startup disk, and install and use the administration tools from a Windows for Workgroups client.
- Chapter 10, "Optimizing Windows NT Server for Performance," covers how to use Performance Monitor to identify common performance problems and isolate server bottlenecks. You will have the opportunity to use Performance Monitor as a tool to determine and resolve a bottleneck in a computer's performance.
- Chapter 11, "Integrating Novell® NetWare® with Windows NT Server," gives you the knowledge and skills required to install and configure the NWLink protocol and Gateway Service for NetWare (GSNW) and to integrate Novell NetWare into a Windows NT Server environment. You will have the opportunity to install and configure Windows NT Server as a NetWare gateway, and then use it to access files on a NetWare server.

Note Completion of this chapter requires a NetWare server.

- Appendix A, "Installation Files and Components," gives additional information on the installation process and upgrading.
- Appendix B, "File Systems," gives additional information on the advantages and disadvantages of the FAT, NTFS, and HPFS file systems.
- Appendix C, "The Server Service Configuration Parameter Values," is a table with the Server service parameter values.
- Appendix D, "Windows NT Security Data Structures," explains the Windows NT security model in more detail.

- Appendix E, "Windows NT Server and Novell NetWare File and Directory Permissions and Rights," is a set of tables presenting naming convention comparisons between Windows NT Server and Novell NetWare.
- Appendix F, "Microsoft Windows NT Server Dynamic Host Configuration Protocol and Windows Internet Naming Service," is an in depth look at DHCP and WINS.

Other Features of This Book

- Each chapter opens with a "Before You Begin" section, which describes other chapters that must be completed before continuing.
- Whenever possible, lessons contain procedures that give you an opportunity to use the skills being presented or explore the part of Windows NT Server being described. All procedures are identified through the following procedural convention: ▶
- The "Review Questions" sections at the end of some lessons allow you to test what you have learned in the lesson. They are designed to familiarize you with the Microsoft Certified Professional examination.
- The "For more information" table at the end of many lessons lists additional resource locations for information on the concepts and skills covered in the lesson. The information referred to covers product documentation, online locations, or both.
- The "Questions and Answers" section contains all of the book's questions and corresponding answers. Each question is referenced by page number.
- The "Glossary" presents a set of definitions for the technical terms that appear in this book.

Network Configurations in This Book

This section is intended to give you a visual picture of the network that you will be designing throughout this book. You will progress from a basic small network configuration to more complex network configurations.

Chapter 1

After Chapter 1, "Installing Windows NT Server," you should have the following configuration.

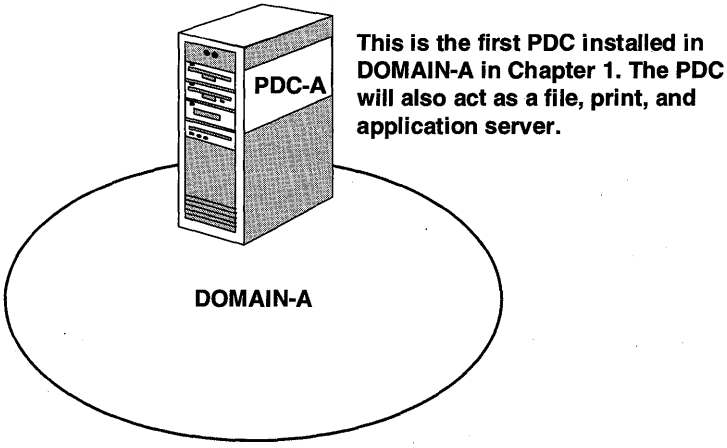


Figure 1: DOMAIN-A with a primary domain controller configured

Chapter 2

After Chapter 2, "Using Groups to Manage Users," you should have the following configuration.

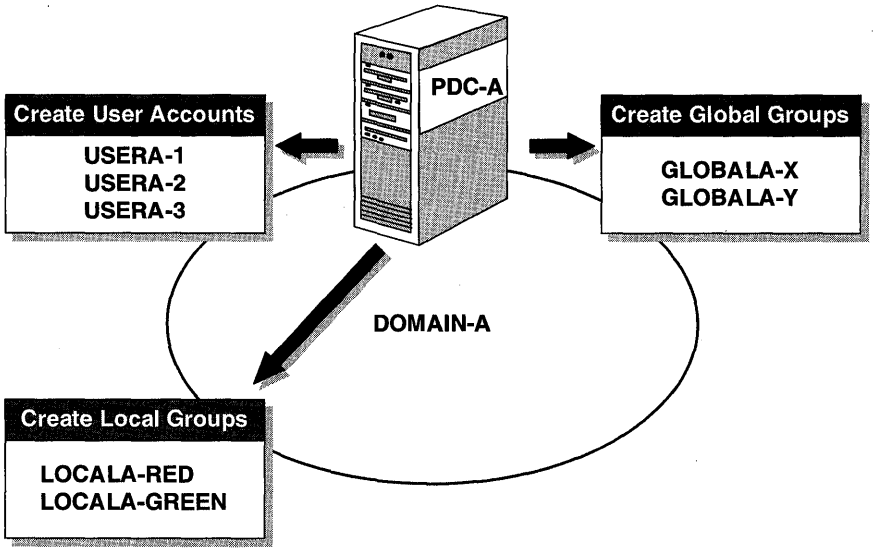


Figure 2: DOMAIN-A with users, local groups, and global groups

Chapter 4

In this chapter you will install Windows NT Server on a second computer as a backup domain controller (BDC) for DOMAIN-A. You will then perform directory replication to make a copy of the user accounts database.

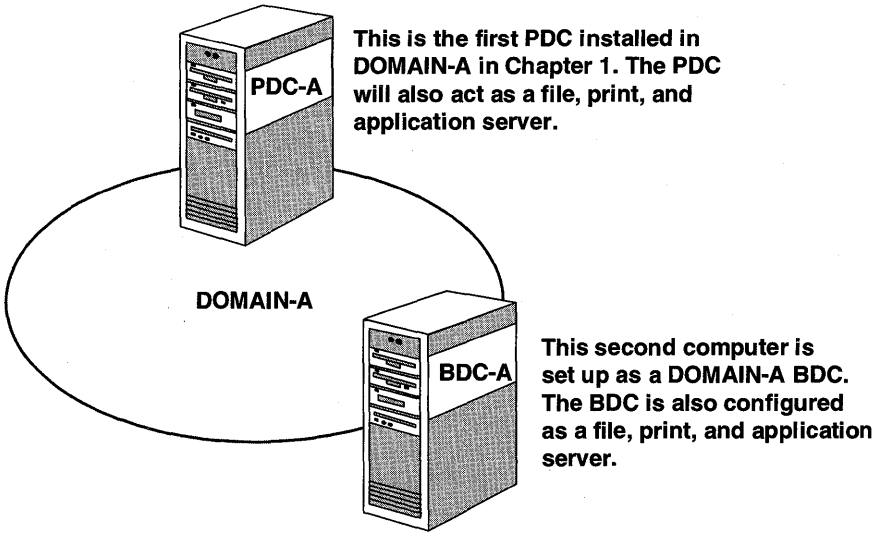


Figure 3: DOMAIN-A network configured with a PDC and BDC

Chapter 5

After you have two computers set up in DOMAIN-A, you will set up the second computer to dual-boot between the current BDC installation for DOMAIN-A and a new installation of Windows NT Server. This new installation will be configured as a primary domain controller for DOMAIN-B.

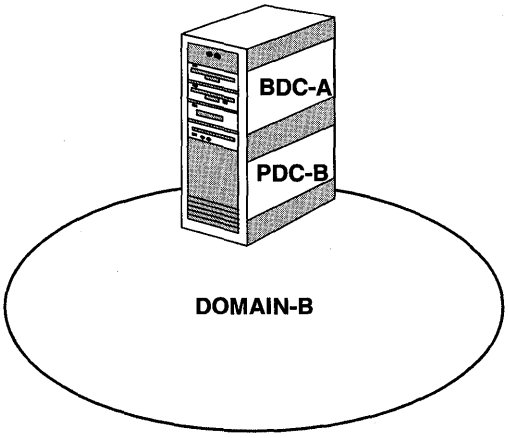


Figure 4: Second computer set up to dual-boot between the BDC for DOMAIN-A and the PDC for DOMAIN-B

When you complete Lesson 1 of Chapter 5, you should have the following configuration.

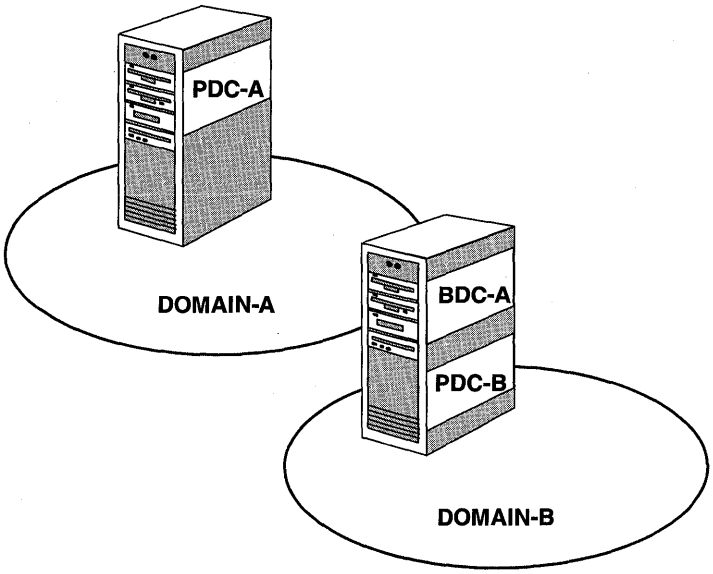


Figure 5: Two single domains

After you create two single domains, you will implement trust relationships. When Lesson 2 is complete, your network should have the following configuration.

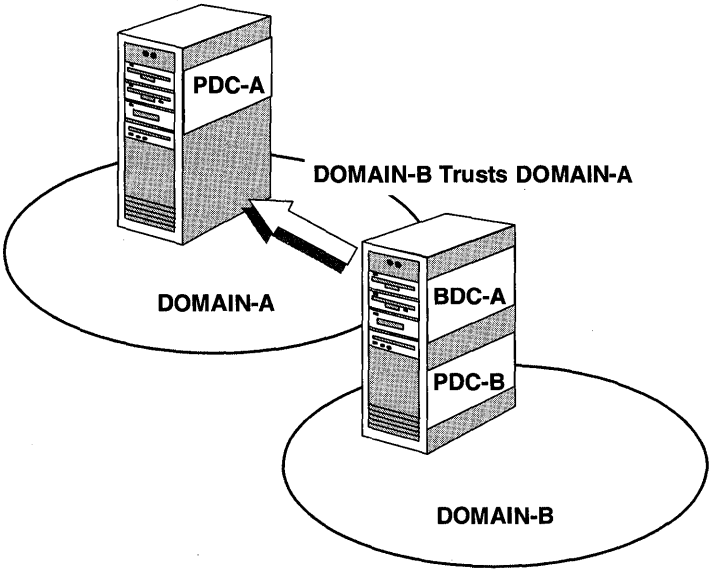


Figure 6: A one-way trust relationship, allowing DOMAIN-B to trust DOMAIN-A

By the time you complete Chapter 5, "Establishing Trust Relationships," your network should have the following configuration.

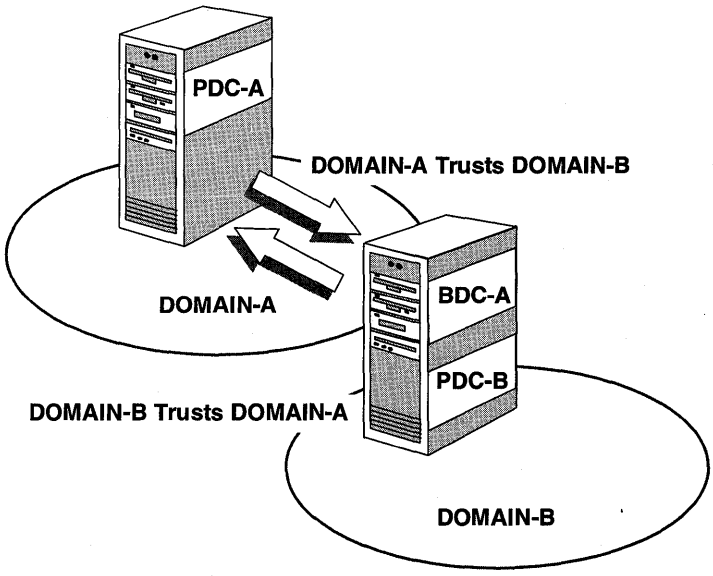


Figure 7: Both domains trust each other

When you have created this network configuration you can take advantage of the advanced features of Microsoft Windows NT Server 3.5.

Conventions Used in This Book

Before you start any of the lessons, it is important that you understand the terms and notational conventions used in this book.

Procedural Conventions

- Hands-on procedures that you are to follow are given in numbered lists of steps (1, 2, and so on). A triangular bullet (▶) indicates the beginning of a procedure.
- The word *select* is used for highlighting directories, filenames, text boxes, menu bars, and option buttons, and for selecting options in a dialog box.
- The word *choose* is used for carrying out a command from a menu or dialog box.

Notational Conventions

- Characters or commands that you type appear in **bold lowercase** type.
- *Italic* in syntax statements indicates placeholders for variable information. *Italic* is also used for important new terms, for book titles, and for emphasis in the text.
- Names of files, paths, or directories appear in ALL CAPITALS, except when you are to type them directly. Unless otherwise indicated, you can use lowercase letters when you type a directory name or filename in a dialog box or at the command prompt. Full capitals are also used for acronyms.
- Monospace type represents code samples, examples of screen text, or entries that you might type at the command line or in initialization files.
- Square brackets [ ] are used in syntax statements to enclose optional items. For example, [*filename*] in command syntax indicates that you can choose to type a filename with the command. Type only the information within the brackets, not the brackets themselves.
- Braces { } are used in syntax statements to enclose required items. Type only the information within the braces, not the braces themselves.

Keyboard Conventions

- Names of keys that you press appear in SMALL CAPITALS; for example, TAB and SHIFT.
- A plus sign (+) between two key names means that you must press those keys at the same time. For example, "Press ALT+TAB" means that you hold down ALT while you press TAB.
- A comma (,) between two or more key names means that you must press each of the keys consecutively, not together. For example, "Press ALT, F, X" means that you press and release each key in sequence. "Press ALT+W, L" means that you first press ALT and W together, and then release them and press L.
- You can choose menu commands with the keyboard. Press the ALT key to activate the menu bar, and then sequentially press the keys that correspond to the highlighted or underlined letter of the menu name and the command name. For some commands, you can also press a key combination listed in the menu.
- You can select or clear check boxes or option buttons in dialog boxes with the keyboard. Press the ALT key, and then press the key that corresponds to the underlined letter of the option name. Or you can press TAB until the option is highlighted, and then press SPACEBAR to select or clear the check box or option button.
- You can cancel the display of a dialog box by pressing the ESC key.

Notes

Notes appear throughout the lessons.

- Notes marked **Tip** contain explanations of possible results or alternative methods.
- Notes marked **Important** are items you should check before completing an action.
- Notes marked **Note** contain supplementary information.
- Notes marked **Caution** contain warnings about possible loss of data.
- Notes marked **Warning** alert you to possible hardware damage.

Hardware and Software Requirements

This self-paced training contains hands-on procedures to help you learn about Microsoft Windows NT Server 3.5. To complete these procedures, you must have at least two computers with the following configuration.

Hardware

All hardware must be on the Microsoft Windows NT Server version 3.5 Hardware Compatibility List.

- 33 MHz 80486 (or higher) processor
- Minimum of 16 MB RAM (32 MB or higher recommended)
- Minimum of 210 MB hard disk space (Additional disk space is required for paging memory if the computer has more than 32 MB RAM.)

Note To complete the hands-on portion of the disk mirroring lesson in Chapter 6, one additional hard disk is required with free space equivalent to the size of the partition that you want to mirror.

To complete the hands-on portion of the striping with parity lesson in Chapter 6, two additional hard disks are required. Each disk must have free space available.

- Network adapter card
- Pointing device
- VGA monitor
- 3.5-inch 1.44-MB floppy disk drive
- CD-ROM (recommended for installation)

Software

- Microsoft MS-DOS version 6.0 or later
- Microsoft Windows NT Server version 3.5 retail product
- Microsoft Windows for Workgroups version 3.11 retail product

Additional Computers

The following configuration is required to complete the hands-on portion of the lesson for integrating Novell NetWare into a Windows NT Server environment.

- One Novell NetWare server running NetWare version 2.*x*, 3.*x*, or 4.*x* with bindery emulation

---

Warning The computers used for the hands-on procedures in this training should be test computers and should not contain files that cannot be reproduced.

Getting Started

This section of the book prepares you to take your first steps into the Microsoft Windows NT Server environment. To best understand the advantages of Windows NT Server, you must first be able to differentiate between a workgroup model and a domain model. In this section, we will briefly compare the workgroup and domain model concepts.

After this section you will be able to:

- Identify situations in which a workgroup strategy should be used.
- Identify situations in which a domain strategy should be used.

Estimated Completion Time: 20 minutes

The Workgroup Model

The workgroup model is a networking scheme in which both resources and administration are distributed throughout the network. Every computer in the workgroup (network) can be used as both a server and a workstation, and each has its own accounts and administration.

Note For more information on workgroups see the *Support Fundamentals for Microsoft Windows NT 3.5: Self-paced Training* book included in this kit.

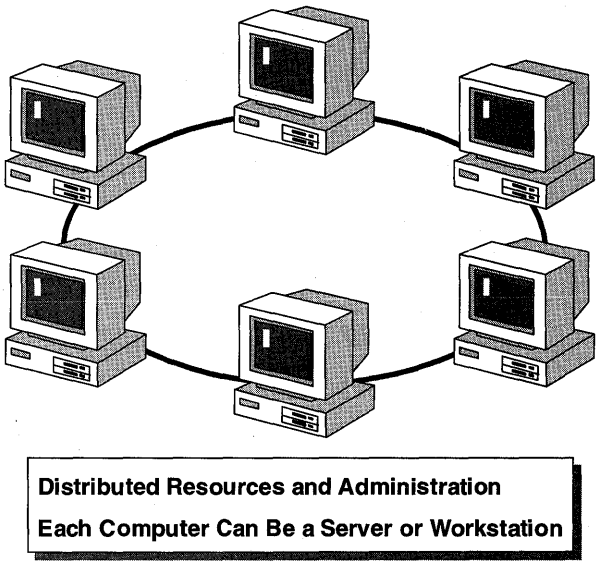


Figure 8: The workgroup model

The workgroup model has the following advantages and disadvantages.

Advantages	Disadvantages
Easy to share resources	No centralized administrative control
Distributed resources	No centralized account management
Low maintenance for administrators	No centralized management of access to resources
Simple design and implementation	No centralized management of workstation configuration and security
Convenient for a limited number of workstations (4–6) in close proximity	Inefficient for networks of many workstations
	Accounts must be monitored at each computer
	Numerous accounts on each computer and duplicate accounts throughout the network

The Domain Model

The domain model is a networking scheme in which administration and security are centralized. A domain consists of networked workstations and servers that:

- Share a Security Accounts Manager (SAM) database.
- Can be administered as a group.

Individual network administrators should determine when and if it makes sense to implement a domain environment. The many computers that make up a domain are organized on the basis of a logical or common purpose. In a large company, for example, each department can create its own domain. The practical user limit for each domain is currently 15,000 accounts.

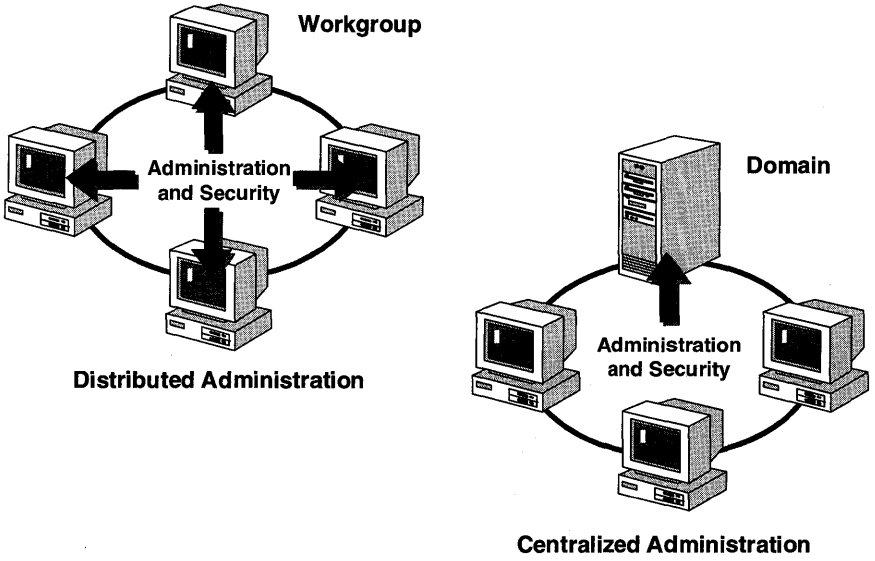


Figure 9: The domain model

The following table outlines the advantages of a domain.

Feature	Advantage
Centralized administration	All the accounts and account policies for the entire network can now be managed from a single point instead of computer-by-computer and user-by-user.
Resource sharing	Assigning permissions to resources becomes more structured. This is crucial where sensitive information is concerned, or where there are many resource share points on the network.
Defining a user's environment	Administrators can create user profiles to determine what each Windows NT Workstation user's logon environment will be like. This is helpful with users who are not computer literate.

In this book we will concentrate on the domain model.

Review Questions

1. What are the differences between the workgroup model and the domain model?

2. What are the advantages of using a domain model?

CHAPTER 1

Installing Windows NT Server

Before You Begin

This chapter assumes that you have an understanding of the workgroup and domain models and the differences between them as described in the "Getting Started" section of this book.

You need one computer to complete this chapter.

Lesson 1: Introduction to Domains

In a Windows NT Server environment, a domain is the basic unit of security and centralized administration. It consists of a group of domain controllers (a minimum of one, but usually multiple domain controllers) running Windows NT Server; in many ways, they function as a single computer. This lesson further explores domains and how to plan your domain.

After this lesson you will be able to:

- Explain the roles a server can play in a domain.
- Describe the four domain models.
- Describe when you would implement the single domain model.
- Plan a domain.

Estimated Completion Time: 25 minutes

Beyond the Workgroup Model

The primary reason for going beyond the workgroup model and implementing the domain model is the need for centralized administration. Grouping computers into domains offers three main benefits to network administrators and users.

- The domain controllers in a domain form a single administrative unit, sharing security and user account information. Each domain has one database containing user and group accounts and security policy settings. All domain controllers running Windows NT Server in the domain keep a copy of this database, so that administrators need to manage only one account for each user, and each user has to use only one account with one password.
- The second benefit of a domain is user account validation. When users log on to the domain, they are validated by one of the domain controllers. This validation ensures that the users have supplied the correct user account name and password to gain access to network resources.
- The third benefit of a domain 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.

The Role of Domain Servers

As the administrator you determine the server's role during installation. The servers in a Windows NT Server domain can be of three different types:

Server type	Role	Number required in a domain
Primary domain controller (PDC)	The PDC is the first computer named in the domain during installation, and it: • Contains a master copy of domain information. • Validates users. • Can act as a file, print, and application server.	One. Each domain can have only one PDC.
Backup domain controller (BDC)	The BDC maintains a copy of domain information, and it: • Validates users. • Provides a backup in the event the PDC becomes unavailable. • Can function as a file, print, and application server.	None. A domain does not require a BDC, but it is recommended that each domain have at least one in case the PDC is unavailable.
Server	The server functions as a file, print, and application server.	None. The server is optional.

The Primary Domain Controller (PDC)

Each domain requires a PDC, which contains the master account database and security policies for the domain. Any changes to account information take place on the primary domain controller. During installation, the PDC is the first Windows NT Server computer named to be part of the domain.

All changes to the accounts database are made at the PDC. When you want to make changes, the actual connection is to the domain's PDC. If the PDC is off-line, no changes can be made to the domain's accounts database or security policies.

The Backup Domain Controller (BDC)

The PDC periodically replicates (copies) the domain accounts database to other Windows NT Server computers in the domain, which are designated during installation as BDCs. A BDC can authenticate and log on domain users. It is common to have more than one BDC.

If the PDC fails, you can promote one of the domain's BDCs to a PDC. The only user account data that would be lost are recent changes that have not yet been replicated to the BDCs.

Any BDC can validate logons from the following clients:

- Microsoft Windows NT
- Microsoft Windows® for Workgroups
- Microsoft LAN Manager OS/2®
- MS-DOS–based computers running Microsoft Network Client 3.0

The Server

Other domain servers, known as servers, can be used as file, print, and application servers. They do not share the domain accounts database or participate in domain user logon validation, and they do not have the overhead of being a domain controller. Even though a server maintains its own database, domain accounts can be granted access to resources on the local server.

A server has all the features provided with Windows NT Server, including:

- RAS server support for up to 256 simultaneous connections.
- Fault tolerance.
- Macintosh® file and print services.
- Remote boot service that supports MS-DOS and Windows 3.*x* clients.

Note These servers cannot be promoted to either a BDC or PDC without reinstalling Windows NT Server.

The Four Domain Models

Every network has special requirements that must be considered before designing and installing Windows NT Server. Domains are created to be expanded and combined into a variety of configurations. Each Windows NT Server–based network originates from one of four basic models:

- The single domain model
- The master domain model
- The multiple master domain model
- The complete trust domain model

You can choose to follow one of these models exactly, to modify one, or to mix and match them.

In this chapter you implement only the single domain model. The master, multiple master, and complete trust models are covered in detail in Chapter 5, "Establishing Trust Relationships Between Domains."

Before determining which domain model to implement, consider the following:

- Location of user accounts—A user account should be defined only once on the network. If this rule is not followed, the same user account name will have multiple security identifiers (SIDs). Multiple SIDs can cause administrative inconsistencies when assigning permissions or user rights.
- Administration requirements—Different models can easily support either centralized or decentralized administration of user accounts and resources.
- Number of servers—There is a limit of 500 servers per domain.
- WAN connections—The quality and speed of WAN connections can influence the location of servers and domains.

The Single Domain Model

As the name implies, this model consists of only one domain, with one primary domain controller and one or more backup domain controllers. A single domain model would be most appropriate in the following situations:

- When there are a very few users.
- If the network does not have to be split for organizational reasons.

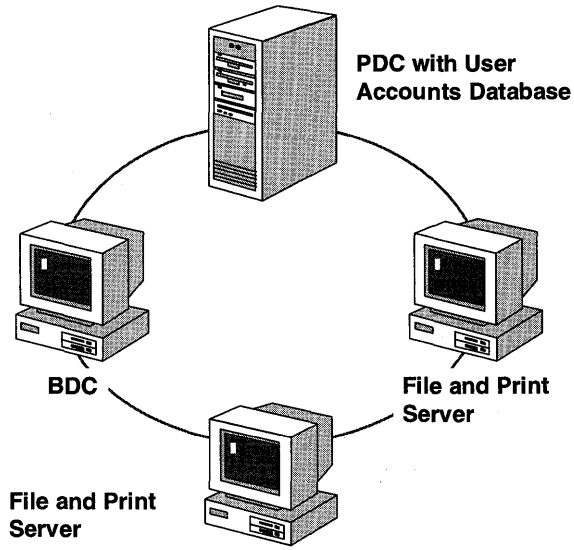


Figure 10: A single domain with one PDC, one BDC, and two file and print servers

A network can use the single domain model if it has a small number of users and groups to be included in the network. The exact number of users and groups depends on the number of servers in the domain and the server hardware.

Using a single domain has the following advantages and disadvantages:

Advantages	Disadvantages
It is the best model for companies with few users and resources.	Performance is poor if the domain has too many users and groups.
It provides centralized management of user accounts.	It does not allow users to be grouped by department.
No management of trust relationships is necessary.	If there are multiple domains functioning in individual single domain models, user accounts must be created in each domain to provide access to all network resources.
Local groups have to be defined only once.	Browsing is slow if a domain has a large number of servers.

Planning Your Domain

Before installing Windows NT Server 3.5, you have to plan your domain configuration. This is important, because once you install Windows NT Server as either a PDC or BDC, the only way to change to a different domain is to reinstall Windows NT Server.

Note You use this planning information in the lessons that follow.

There are many things to consider before installing Windows NT Server, including:

- Windows NT Server requirements.
- The role the server plays in the domain.
- Selection of a file system.
- How the server hard disks are partitioned.

System Requirements

Before installing Windows NT Server, make sure that your hardware is on the *Hardware Compatibility List* (HCL) included in your Windows NT Server documentation set. Microsoft can support only devices that are on the HCL. If one of your devices is not on the HCL, contact the device manufacturer to request a Windows NT Server driver.

Windows NT Server supports computers with up to four microprocessors. Support for additional microprocessors is available from an original equipment manufacturer (OEM). The following table describes the system requirements for Windows NT Server. Notice that the system requirements are different for Intel®- and RISC-based computers.

Category	Intel Requirement	RISC Requirement
Processor	32-bit *x86*-based (80386/25 or higher) Intel Pentium™	A supported RISC-based processor, such as the MIPS® R4000™ and R4400, and DEC™ Alpha AXP™
Display	VGA (or higher resolution) video display adapter	VGA (or higher resolution) video display adapter
Hard disk space	One or more hard disks, with approximately 90 MB minimum free disk space on the partition that will contain the Windows NT Server files	One or more hard disks, with approximately 110 MB minimum free disk space on the partition that will contain the Windows NT Server files
Other drives	High-density 3.5-inch floppy disk drive, or a high-density 5.25-inch floppy drive plus an SCSI® CD-ROM drive (for computers with only a 5.25-inch drive, you must install Windows NT Server over a network)	SCSI CD-ROM drive
Memory	16 MB minimum	16 MB minimum
Disk compression	Windows NT Server does not support disk compression and cannot be located on a partition that runs disk-compression products.	Not supported
Optional components	Mouse or other pointing device One or more SCSI CD-ROM drives For network installation, an MS-DOS–based network operating system that permits connection to a server containing the Windows NT Server files	Mouse or other pointing device
Other components	One or more network adapter cards (required for a domain controller)	One or more network adapter cards (required for a domain controller)

Note Windows NT cannot access all the space on 1-GB Integrated Drive Electronics (IDE) drives because they follow the EIDE (Extended IDE) standard and do not support translation that Windows NT Server understands. This is due to a BIOS limit of 1024 cylinders, not an operating system limit. To overcome this limit, either your system's BIOS must be able to work around it (by sector translation or by using relative cluster addressing as SCSI drives do) or Windows NT Server must be able to communicate directly with the controller. Windows NT Server is currently able to communicate with Western Digital™ WD 1003 compatible controllers.

PDCs and BDCs

Each domain is identified by the domain's SID. The domain SID is used for all accounts in the domain, and it is unique. The only way to change a domain controller's SID is to reinstall Windows NT Server. The best way to avoid this is to plan ahead, so that Windows NT Server PDCs and BDCs begin as part of the domain with which they will remain.

Servers

Because a server (not functioning as a domain controller) has its own user account database and SID, it can be moved without reinstalling Windows NT Server. Even though it is part of a domain, its SID will be different from that of the domain.

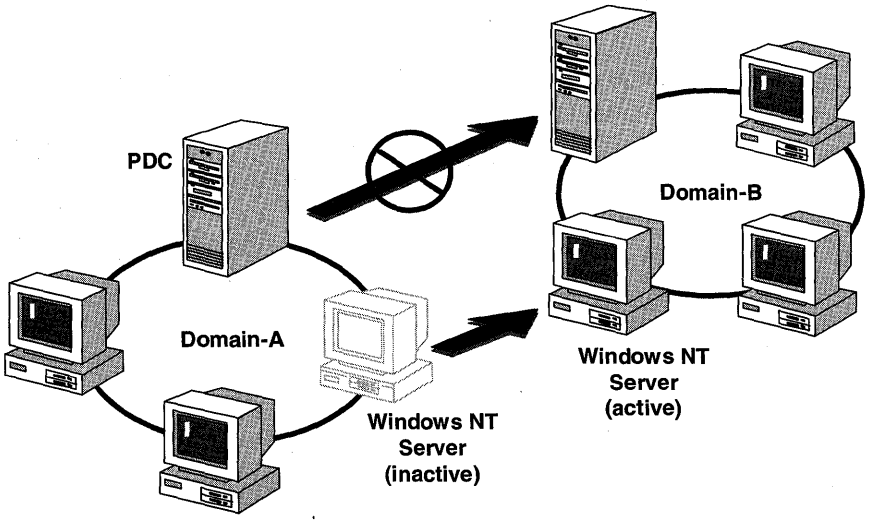


Figure 11: A file, print, and application server being moved from one domain to another

The previous figure illustrates two domains with PDCs and servers. The PDC from Domain-A cannot be moved to Domain-B; however, the Windows NT Server can be moved.

Naming Your Domain

Your domain name can be any combination of 15 characters except for a space, currency symbol, bullet symbol, pipe character, section symbol, or paragraph symbol.

You can change the name of your domain at any time. Because the domain's SID (rather than the domain's name) uniquely identifies the domain, you can change the domain's name if needed. The new name is associated with the existing SID.

After the domain name has been changed on the PDC, the domain name on all the other computers in the domain must be changed to reflect the new domain name.

Selecting a File System

Before you install Windows NT Server, you should know which file systems you need. Windows NT Server supports the following file systems:

- The Windows NT File System (NTFS)
- File Allocation Table (FAT)
- High Performance File System (HPFS)

NTFS

NTFS is a Windows NT disk partition format that offers advantages over FAT or HPFS file systems, including the ability to:

- Set file and directory access permissions.
- Implement transaction tracking and recovery.
- Create very large volume sizes.

It is not supported by other operating systems, such as MS-DOS or OS/2. However, other computers on the network running other operating systems are able to access the NTFS partition as file, print, and application servers.

Note For more information on NTFS, see the *Support Fundamentals for Microsoft Windows NT 3.5: Self-Paced Training* book or *Inside the Windows NT File System* by Helen Custer.

Other operating systems on the local computer cannot access NTFS partitions. For example, if your computer is configured with Windows for Workgroups and Windows NT Server, when you boot Windows for Workgroups you will not see any NTFS partitions. Access to NTFS partitions is available on the local computer only when you boot Windows NT Server.

If you will be running only Windows NT Server, choose NTFS. You should also use NTFS if:

- You will be using Services for Macintosh.
- Directory and file-level security is required.
- You will be migrating directories and files from a NetWare server and you want to preserve permissions.

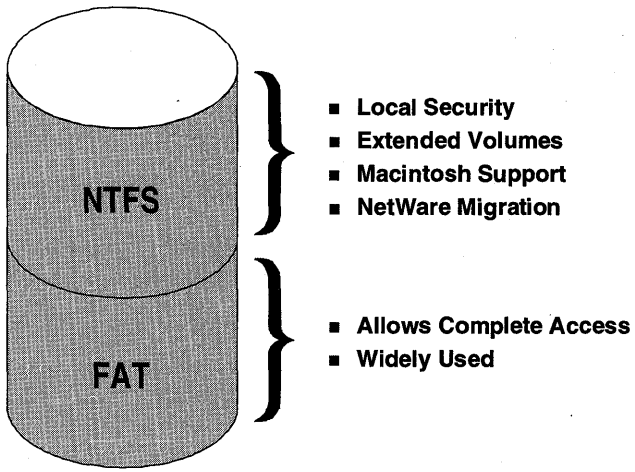


Figure 12: NTFS and FAT file systems

File Allocation Table (FAT)

The FAT file system is used by MS-DOS and OS/2 operating systems. Use the FAT file system if you need to boot between Windows NT Server and MS-DOS or OS/2.

High Performance File System (HPFS)

HPFS was first introduced with OS/2 version 1.2. It was designed to overcome some of the limitations of the FAT file system, and thus provides support for longer file names, extended file attributes, less file fragmentation, and so on. HPFS support is included with Windows NT primarily to ease the migration from LAN Manager to Windows NT.

Dual-Booting Operating Systems

To boot between Windows NT Server and MS-DOS, one partition on the computer must be formatted with the FAT file system for MS-DOS.

If you want to boot between OS/2 and Windows NT Server, at least one partition must be FAT or HPFS. HPFS partitions can be converted to NTFS, either as part of the installation process or after Windows NT is installed.

Additional File System Considerations

Other file system considerations to keep in mind include:

- RISC—The hardware specification requires drive C to be FAT.
- Local Security—NTFS is the only file system that provides local security.

Note The Setup program can format a partition for NTFS or FAT, but it cannot format a partition for HPFS (nor can Disk Administrator). You can format an HPFS partition only by typing **format d:/fs:hpfs** at a command prompt.

It is important to plan your file system installation carefully. Although you can change file systems on any partition after running Setup, you have to perform a backup and restore operation if you want to save your data. Converting an NTFS partition to any other file system requires that you:

1. Back up all the files.
2. Reformat the partition (deleting all the files).
3. Restore the files from the backup.

You can convert FAT or HPFS to NTFS without performing the previous steps.

► **To plan your domain configuration**

Before running Setup, it is recommended that you plan your computer and domain configuration. The following configuration table lists all the configuration information that the Setup program prompts you for during the installation and configuration process. It also lists the suggested configuration information used for the hands-on procedures. If your company has standards that you are required to adhere to, you can substitute the suggested configuration information with your own.

Tip Make a copy of this table and fill in your configuration information. You can then use the page with any procedure in this book. This Configuration Table is mentioned before each procedure it is needed.

Configuration Table

In procedures in this book, you are asked to refer back to this table. All items are named with regard to the domain they will be a part of. For example, "LOCALA-RED" is part of "DOMAIN-A" and "PDC-B" is part of "DOMAIN-B".

Important It is recommended that you use the suggested configuration names throughout this book. If more than one person in your organization is doing this training you must have unique computer names and domain names on your network.

Configuration option	Suggested configuration	Your configuration (if different from the suggested configuration)
Product ID (from Windows NT Server box)		
Location of distribution files	CD-ROM	
Your name and company		
Computer names		
First domain primary domain controller	PDC-A	
First domain backup domain controller	BDC-A	
Second domain primary domain controller	PDC-B	
Windows for Workgroups workstation	WFW-B	
Windows NT file locations		
First domain PDC drive/partition		
First domain PDC winnt_root	\WINNT35	
First domain BDC drive/partition		
First domain BDC winnt_root	\WINNTBDC	
Second domain PDC drive/partition		
Second domain PDC winnt_root	\WINNTPDC	
WFW workstation drive/partition		
WFW workstation win_root	\WINDOWS	
Language (locale)		
Time zone		
Network adapter		
Network adapter configuration settings (for example, IRQ or base I/O address)		
Other settings particular to your card		

(*continued*)

Configuration option	Suggested configuration	Your configuration (if different from the suggested configuration)
Network protocol(s)	NetBEUI and NWLINK (IPX)	
NWLINK (IPX) Parameters		
Frame Type		
Internal Network Number		
Computer Name of NetWare Server		
Gateway account	Administrator	
Password of gateway account	<blank>	
Name of text file on Netware Server \SYS\PUBLIC	NWGATE.TXT	
TCP/IP Parameters		
IP Address PDC-A	131.107.2.150	
IP Address PDC-B	131.107.2.155	
Subnet Mask	255.255.0.0	
Default Gateway		
Non-existent IP Address	131.107.2.255	
Scope for DHCP Server IP Address Pool Start Address	131.107.2.160	
Scope for DHCP Server IP Address Pool End Address	131.107.2.169	
Domain names for:		
First domain	DOMAIN-A	
Second domain	DOMAIN-B	
Additional Administrator names	ADMIN-A	
User names for:		
First domain, user #1	USERA-1	
First domain, user #2	USERA-2	
First domain, user #3	USERA-3	
First domain, user #4	Replicate	
Second domain, user #1	USERB-4	
Second domain, user #2	USERB-5	

(continued)

Configuration option	Suggested configuration	Your configuration (if different from the suggested configuration)
Local group names for:		
First domain, local #1	LOCALA-RED	
First domain, local #2	LOCALA-GREEN	
Global group names for:		
First domain, global #1	GLOBALA-X	
First domain, global #2	GLOBALA-Y	
Share Names for:		
First domain PDC, share #1	SHARE-A	
First domain PDC, share #2	USERS	
First domain PDC, share #3	NWDATA	
First domain PDC, share #4	NWPUBLIC	
Second domain PDC, share #1	SHARE-B	
Second domain PDC, share #2	CLIENTS	
Second domain PDC, share #3	SETUPADM	
Second domain PDC, share #4	UTILS	

Lesson Summary

Before installing Windows NT Server, it is important to understand all the installation issues and to plan your configuration. Planning is important to ensure that computer and domain names, the roles of computers within a domain, and the type of domain model are implemented properly.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Explain when you would use a domain instead of a workgroup.

2. What are the differences in a PDC, BDC, and server?

3. Which type of server is recommended to install first? How is this determined?

For more information on	See
Installation requirements	Chapter 1, "Installing Windows NT Server," in the *Windows NT Server Installation Guide.*

Lesson 2: Installing Windows NT Server

When you have a plan for naming and configuring your domain, you are ready to install Windows NT Server.

After this lesson you will be able to:

- Install Windows NT Server 3.5.
- Describe the Windows NT 3.1 files and directories that are preserved when upgrading to Windows NT Server 3.5.
- Identify common upgrade issues and how to solve them.
- Distinguish between the Express and Custom Setup options.
- List the default protocols and describe the configuration requirements so that they can communicate on the same network.

Estimated Completion Time: 50 minutes

Upgrade and Install Methods

Windows NT Server can be installed or upgraded from CD-ROM, from a sharepoint over the network, or from disk.

CD-ROM

Installing from CD-ROM requires the following:

- A supported CD-ROM (see the Microsoft Windows NT Hardware Compatibility List).
- The three Setup disks included with Windows NT Server 3.5.

Over the Network

Installing over the network requires a sharepoint to the Windows NT Server 3.5 distribution files. You can install over the network from a computer running any of the following operating systems:

- Microsoft Windows NT
- Microsoft LAN Manager
- Novell NetWare
- Banyan® VINES®
- Microsoft Windows for Workgroups

You can set up the distribution files in two ways:

- Create a sharepoint on the hard disk and then XCOPY the \I386, \MIPS, or \ALPHA directory from the CD-ROM.

- Create a sharepoint to the \I386, \MIPS, or \ALPHA directory on the Windows NT Server compact disk (CD-ROM).

Note For more information, see the section "Setting Up Master Files on a Server" in Chapter 1, "Installing Windows NT Server," in the *Windows NT Server Installation Guide*.

Disk

Installing from disk is recommended only if the CD-ROM and over the network methods are not available. This method uses many disks and is much slower, because it requires swapping many disks.

Supported Windows NT Upgrade Options

The Windows NT 3.5 Setup program includes the option to upgrade any Windows NT–based computer to a Windows NT Server 3.5 computer without having to delete and reinstall Windows NT Server. If it detects any existing version of the Windows NT operating system, it provides the upgrade option.

It is important to keep the various versions and names (as shown in the following table) of the Windows NT family of products separate so that you will be aware of the options available. You can upgrade to Windows NT Server 3.5 from the following operating systems.

Operating system	Function
Windows NT 3.1	As a server only, and not a domain controller
Windows NT Workstation 3.5	As a server only, and not a domain controller
Windows NT Advanced Server 3.1	As a domain controller or server

---

Note Because Windows NT Server domain controllers use a different structure for their user accounts databases, it is not possible to upgrade a Windows NT 3.1 computer to a Windows NT Server 3.5 domain controller. It can be upgraded only to a computer running Windows NT Server 3.5 as a file, print, or application server.

If you choose to upgrade a Windows NT 3.1 or Windows NT Workstation 3.5 computer, a screen appears with a message stating that the computer you are upgrading cannot be made a primary or backup domain controller. You can then continue and either:

- Upgrade over the existing version.
- Select another installation to upgrade over.
- Install a new copy of Windows NT Server in a new location.

If you are upgrading from Windows NT Advanced Server 3.1, you can make an existing domain controller a domain controller under Windows NT Server. You should first upgrade the PDC.

Note For more information, see Chapter 1, "Installing Windows NT Server," in the *Windows NT Server Installation Guide*.

Information Preserved During an Upgrade

Upgrading Windows NT Advanced Server 3.1 to Windows NT Server 3.5 preserves:

- Local security accounts.
- Network adapter settings, protocols, and services configurations (including settings for RAS and Services for Macintosh servers).
- Custom program groups, desktop settings, and other preferences that were set using Control Panel.
- Preferences that were set for administrative tools and accessories.
- Custom settings that were made using Registry Editor.

Upgrade Issues

Before you begin the process of upgrading, make sure that you understand the following problems that might arise.

Important These six areas have the potential to cause serious upgrade problems. They require extra attention.

- Upgrading a computer with additional components—When upgrading a Windows NT 3.1 computer that has additional network components installed, such as a third-party redirector, it is recommended that these be removed or disabled before upgrading.

  If they are not removed or disabled before upgrading, they could potentially lead to problems during the upgrade process. For example, if the Novell Personal NetWare Requestor for Windows NT is installed during the upgrade, the computer's attempt to reboot into the graphical portion of Setup will fail.

  Note Network components, such as a third-party redirector, will typically have to be upgraded to a Windows NT Server 3.5 version of the driver before they can be used with a Windows NT 3.5 computer. Contact the manufacturer for a new version of the driver.

- Undo or Rollback—After the upgrade process has started copying files to the computer, there is no way to undo or roll back the upgrade and return to the previous installation of Windows NT. However, if the upgrade process encounters a problem and does not complete, it can be restarted as many times as necessary to complete the upgrade.

  If the upgrade process cannot be completed, the current Windows NT Server installation must be removed, because it has been partially deleted and is in an unusable state. Windows NT Server must then be installed from the beginning.

- Old device drivers—If Windows NT Server does not have a device driver for a piece of third-party hardware that was used under Windows NT 3.1, it is tempting for users to try to use the third-party Windows NT 3.1 driver under Windows NT 3.5. However, doing so can lead to very unpredictable results, especially with network drivers.

  This can generate problems ranging from access violations to error messages stating that the appropriate DLLs cannot be found.

  One symptom that might appear when using Windows NT 3.1 device drivers under a Windows NT 3.5 system is that the Control Panel can take up to three minutes to load.

- Mandatory user profiles— A mandatory user profile created under a Windows NT 3.5 system cannot be used under Windows NT 3.1. However, a mandatory user profile created under Windows NT 3.1 can be used under a Windows NT 3.5 system. The reason for this is that user profiles are now being stored in Unicode™ under Windows NT 3.5.

  Therefore, if a user will be logging on to both Windows NT 3.1 and Windows NT 3.5 systems, the user's mandatory profile *must* be created on a Windows NT 3.1 computer.

- Missing DLLs—If a pop-up error occurs when starting a Win32® application that ran under Windows NT 3.1, it is an indication that a DLL could not be found. This is because the application requires one of the files, such as LMUICMN0.DLL, which the upgrade deleted. This problem could be encountered when trying to use some of the utilities included in the Windows NT 3.1 Resource Kit.

Note Expanding the LMUICMN0.DLL and LMUICMN1.DLL files off the Windows NT 3.1 CD-ROM will allow most utilities that require these DLLs to function properly. However, the Windows NT 3.5 Resource Kit will include updated versions of these utilities, which will run without these DLLs.

- Windows NT 3.1 and Windows NT Server 3.5 dual-boot systems— If a new installation of Windows NT Server will be performed on a system that also boots Windows NT 3.1, UPGRADE.EXE must be run before installing Windows NT Server. Because of changes in the NTFS file system and the addition of long filename support to the FAT file system, Windows NT 3.1 will not be able to access NTFS partitions and might damage FAT partitions if UPGRADE.EXE is not used.

  UPGRADE.EXE replaces the following Windows NT 3.1 files on the system:

  - AUTOCHK.EXE
  - FASTFAT.SYS
  - UFAT.DLL
  - NTFS.SYS
  - UNTFS.DLL

  The UPGRADE.EXE utility is located under \FS31UPD*processor_type* on the CD-ROM and under \FS31UPD\I386 on the i386™ Update Disk in the disk set.

Using the Setup Programs

There are two Setup executable files, WINNT.EXE and WINNT32.EXE.

- WINNT.EXE—This can be used only while the computer is booted under MS-DOS.
- WINNT32.EXE—This is a Win32 version of the WINNT.EXE network install utility. It is used for upgrading Windows NT operating systems.

When using WINNT32.EXE, the following steps must be performed:

1. Under Windows NT 3.1, connect to the server that has the Windows NT Server 3.5 files, or change to the directory on the CD-ROM with the appropriate files, such as \I386.
2. Start WINNT32.EXE.
3. When prompted, give the location of the Windows NT Server 3.5 files.

Note WINNT32.EXE, by default, prompts the user to upgrade the current Windows NT installation. However, it is possible to have WINNT32.EXE install Windows NT Server 3.5 in a different location and thus maintain the Windows NT 3.1 installation on the computer.

It is possible to use WINNT32.EXE to upgrade Windows NT 3.1 from an unsupported CD-ROM drive, just as it was possible to use WINNT.EXE to install Windows NT 3.1 from an unsupported CD-ROM drive. This is useful when there is a third-party driver available for a CD-ROM drive or SCSI adapter that does not yet have a driver for Windows NT 3.5.

The Setup Process

The Setup programs (WINNT.EXE and WINNT32.EXE) perform the following steps:

1. Setup first creates a set of boot disks for the computer's drive A for over-the-network or unsupported CD-ROM installations. This step requires three blank formatted disks.

   Note The disk and supported CD-ROM versions of Windows NT Server include the three Setup disks.

2. Setup creates a WIN_NT.~LS temporary directory on the local hard disk, and then copies Windows NT Server files from the network sharepoint to this directory.
3. Finally, Setup prompts you to restart your computer from the first Setup disk.

Modifying the Setup Process

The Setup program has switches that can save time or space when installing or upgrading. These switches can be used with WINNT.EXE.

The Setup process can be modified by using any of the following switches:

- /O and /OX—Only create boot disks

  The /O switch causes WINNT.EXE to create only the three required boot disks. A complete installation is *not* performed. The three disks created using this switch are identical to the disks that a regular installation creates.

  The /OX switch causes WINNT.EXE to create a set of the three boot disks that can be used to perform an installation from CD or disk.. This switch is useful if you need the three Setup disks to start a CD-ROM installation and the disks have been misplaced.

- /B—Diskless Installation

  This switch allows WINNT.EXE to be used to perform an installation or upgrade without the three Setup disks. The /B switch does not create the three Setup disks, nor are the Setup disks required when the computer restarts and begins installing Windows NT Server. The /B switch requires an extra 4–5 MB of hard disk space to complete the process.

- /U—Unattended Installation

  This switch allows the WINNT.EXE portion of an installation or upgrade to proceed unattended. This is done by skipping the screen that asks for the location of the Windows NT Server source files, and it requires the use of the /S switch to specify the location. The /U switch automatically uses the /B switch and does not create the boot disks. Using /U also bypasses the final reboot screen of the text mode portion of WINNT.EXE, causing the computer to restart automatically.

- /S—Windows NT Server Source Files

  This switch allows you to specify the location of the Windows NT Server source files. It can be used in conjunction with the /U switch to bypass the normal prompt for source file location.

- /F—This switch does not verify files as they are copied to the Setup boot disks.
- /I:*inffil*—This switch specifies the filename (no path) of the Setup information file. The default is DOSNET.INF.
- /C—This switch skips the free-space check on the Setup boot disks you provide.
- /D:*\winnt_root*—This switch removes Windows NT system files from the installation in *\winnt_root.*
- /T:*tempdrive*—This switch specifies a drive to contain temporary Setup files. If not specified, Setup attempts to locate a drive for you.

WINNT32.EXE recognizes the following switches: /B, /U, /S, /I, and /T.

Setting Up Windows NT Server

Now that you know how the Setup program works, and about the switches that are available to customize the Setup process, you are ready to run the Setup program.

► To start the Setup program from a SCSI CD-ROM on *x86*-based computers

In this procedure you install Windows NT Server from CD-ROM on *x86*-based computers. All installation methods are similar, with the exception of how to start the installation.

Note For detailed instructions on starting Windows NT Setup from disk or over the network, and for information on starting Setup on RISC-based systems, see Chapter 1, "Installing Windows NT Server," in the *Windows NT Server Installation Guide.*

---

1. With your computer turned off, insert the Windows NT Server Setup Boot Disk in drive A, and then turn on your computer.

2. When Setup prompts you for Setup Disk #2, insert the disk in drive A and then press ENTER.

   The Setup screen appears.

3. Read the next section about Express and Custom Setup before continuing the Setup process.

Note For problem-solving tips, see the section "Hardware Configuration Problems" in Chapter 2, "Troubleshooting," in the *Windows NT Server Installation Guide*.

Express and Custom Setup

Like all Windows Setup programs, Windows NT Server has two installation options: Express and Custom. For each of these, you are required to provide certain information.

The Setup program copies the appropriate files to your computer's hard disk and configures the software that you need to run applications and use the network.

Express Setup

This is the easiest way to install Windows NT Server. It is recommended for most standard installations. Express Setup asks a minimum number of questions and installs all standard Windows NT Server components.

Express Setup will:

- Identify and configure hardware and software.
- Install all Windows NT components.
- Set up program items for existing applications.

Custom Setup

Custom Setup allows greater control over the installation process. This Setup method is preferred if devices or network adapter cards cannot be detected properly.

With Custom Setup, you can:

- Specify one or more network adapter cards not recognized by the automatic detection process.
- Limit the installation of components, such as games, that might not be appropriate for the installation.
- Customize the location or size of the PAGEFILE.SYS file.

► To specify the type of setup

At this point, Setup has loaded a limited version of Windows NT Server from disk. You are ready to specify the setup method. You need your Configuration Table for this procedure.

Important In this procedure, you install a new version of Windows NT Server. You do not perform an upgrade.

---

1. From the Windows NT Server Setup screen, press ENTER to continue.

   You are prompted to select a setup method.

2. Press ENTER for Express Setup.

   The Setup program prompts for Setup Disk #3.

3. Insert Setup Disk 3 into drive A, and then press ENTER.

   A screen appears indicating any devices, such as a SCSI controller, that Setup recognized in your computer.

4. Make any required corrections, and then press ENTER to continue.

   The Setup program loads device drivers for the supported file systems, then prompts for installing from CD-ROM or floppy disk.

   Important If Windows NT Setup does not display this prompt, then Setup did not find the CD-ROM drive. This could indicate that the CD-ROM is unsupported; in that event you would have to follow the instructions for installing from the network or an unsupported CD-ROM device, at the bottom of page 5, Chapter 1, "Installing Windows NT Server" of the *Windows NT Server Installation Guide.*

   ---

5. Press ENTER to install from CD-ROM.

   Setup then looks for any existing Windows NT or Windows 3.*x* installation on your hard disk.

6. If it detects one, press N to cancel the upgrade and install a new version of Windows NT Server.

   A screen appears showing existing partitions.

► To specify the installation directory

When you are installing a new version of Windows NT Server, you are given the option to specify the installation drive and directory. If you are performing an upgrade of an existing version of Microsoft Windows 3.*x* or Windows NT 3.1, you are not prompted to specify the installation drive and directory. Instead, the upgrade process installs Windows NT Server files in the same location as the existing software.

You need your Configuration Table for this procedure.

1. Select the *first domain PDC drive/partition* to install onto, and then press ENTER.

   A screen appears asking for the type of file system you want on this partition.
2. Select Leave the Current File System Intact (No Changes), and then press ENTER.

   If the hard disk is not partitioned, or if the partition is not formatted, you are prompted to format the selected partition to complete the installation.

   A screen appears asking for the location to install the files.
3. Type **\winnt35** for your directory name and then press ENTER.

   The Setup program prompts for the Windows NT Server CD-ROM, if not already inserted.
4. If not already inserted, insert the Windows NT Server CD-ROM in the CD-ROM drive, and then press ENTER.

   Setup copies files to your hard disk. When copying is complete, a screen appears asking you to remove the disk from drive A and restart your computer.
5. Remove Setup Disk 3 from drive A, and then press ENTER to restart your computer and continue Setup.

   Your computer starts and the Windows NT Setup dialog box appears.
6. Continue reading about domain issues before continuing Setup.

Domain Issues

At this point in the installation process, you have to decide the following:

- Whether the computer is becoming the first server (PDC, BDC, or server) in a new domain.
- Whether to join a workgroup or domain.
- What to name the domain and the computer.

In this section you create a domain and install the first Windows NT Server computer as a PDC. Setup displays dialog boxes that enable you to:

- Install the computer as a PDC, BDC or server in a domain.
- Join a workgroup or a domain.

Several things could go wrong when joining an existing domain:

- The wrong administrator's user name or password could be entered.
- The PDC could be down.
- The network could be down.
- The adapter could be configured incorrectly.
- The NetBIOS name could conflict with computer or domain names.

The best way to avoid most of these potential problems is to plan your installation before attempting to install. Then, if problems arise, they will likely be hardware problems, not the result of entering an incorrect name or indicating the wrong configuration.

Joining a Domain

When the Windows NT Server is a BDC or server in a domain, you must supply the name of an existing domain during the installation process. You do one of the following:

- Add an account for your computer to the domain before installation.
- Grant yourself privileges to create your computer account during installation.

If you are installing a PDC, you select a new domain name.

Naming a Domain

If you install the computer as a PDC in a new domain, be sure to choose a unique domain name that does not conflict with any existing network name. Two identical names on the network can have unpredictable results.

For example, having a workgroup and a domain with the same name on the network causes the workgroup to appear in Server Manager in the domain as a workstation. The workgroup computers are not members of the domain and cannot be administered from any of the domain's servers.

► **To install Windows NT Server as a domain controller**

The goal is to create the single domain model. In this procedure you set up a PDC. You need your Configuration Table for this procedure.

At this point, the graphical version of the Windows NT Setup program is visible on your screen. Continue with the following steps to install your PDC.

1. From the Windows NT Setup dialog box, type your name and company name, and then choose Continue.
2. When prompted, verify your name and company name, and then choose Continue.
3. From the Windows NT Setup dialog box, type your Product identification number, and then choose Continue.
4. When prompted, verify your Product ID, and then choose Continue.

   The Windows NT Server Security Role dialog box appears.
5. Select Domain Controller (Primary or Backup), and then choose Continue.

   You are prompted for a computer name to identify your computer.
6. In the Computer Name box, type **pdc-a**, and then choose Continue.
7. When prompted, verify your computer name, and then choose Continue.

   The Language (Locale) dialog box appears.
8. Select the appropriate language (locale), and then choose Continue.

   The Set up Local Printer dialog box appears.
9. Choose Cancel (do not set up a printer).

Note You do not have to install a printer to complete the lessons in this book.

---

10. Choose OK to acknowledge the Setup message.

    The Windows NT Setup program checks your system for network adapter cards.

    The Adapter Card Setup dialog box appears.
11. Continue reading about network adapters before continuing Setup.

Network Adapters

For Express Setup, Windows NT Setup automatically checks for a network adapter card in your computer and installs the first one it recognizes. Some types of network cards might not be recognized by Setup. If Express Setup cannot identify your adapter card, it asks whether you want to install Microsoft Remote Access Services (for users connecting to a network over telephone lines). If you do not choose this option, Setup displays the Network Adapter Setup dialog box and prompts you to select the name of the card you want to install.

You must know the correct network adapter card and settings for your computer to install Windows NT Server properly. Make sure you have verified the correct adapter card and settings before continuing.

At this point the Adapter Card Setup dialog box is on your screen. You now verify that Windows NT Setup has detected the correct adapter card, or you select the appropriate one for your system. You need the network adapter information from your Configuration Table in this procedure.

1. Verify that your correct network adapter appears in the box. If it does, go to Step 3. If it does not, choose Cancel.

   The Add Network Adapter dialog box appears.

2. Select the network adapter for your computer, and then choose Continue.

   The Adapter Setup dialog box appears.

3. Select the appropriate network adapter configuration settings for your network adapter card, and then choose Continue.

   The Windows NT Setup dialog box appears, asking to install network protocols.

4. Continue reading about default protocols before continuing Setup.

Default Protocols

When performing a new Windows NT Server 3.5 installation, the default network protocols are NWLink and NetBEUI. This is a change from Windows NT 3.1 and previous Microsoft network operating systems, including LAN Manager and Windows for Workgroups 3.*x*, in which NetBEUI was the default protocol.

Whether you choose Express or Custom Setup, Windows NT Setup prompts you to select one or more network protocols to install. The network protocols that are available to install during Setup are the following:

- NWLink IPX/SPX Compatible Transport
- TCP/IP Transport
- NetBEUI Transport

Each of these protocols has specific requirements for implementation. These protocols do not communicate with each other, so you need to install the appropriate protocols to communicate with the various types of computers on your network. For example:

- Install NWLink IPX/SPX Compatible Transport if you have a mixed environment of Microsoft and Novell clients and servers.

- Install TCP/IP if you have an internet consisting of clients and servers from multiple vendors, as TCP/IP is the protocol of choice for heterogeneous environments.
- Install NetBEUI if you have a local area network consisting of only Microsoft networking clients and servers.

Connectivity Problems

NWLink can potentially cause network connectivity problems on networks using previous Microsoft network operating systems. This is because NWLink does not communicate with computers using only NetBEUI.

To avoid these problems, it is very important for you to perform the following steps when installing Windows NT Server:

- Add NWLink, or its equivalent, to the other Microsoft network operating systems on the network that need to be able to communicate with Windows NT Server computers running NWLink.
- Install NetBEUI when performing a new Windows NT Server installation on a network that has computers running other Microsoft network operating systems.

Protocol Selection Dialog Box

To make it easier to see the default protocols and add additional protocols during Setup, the Windows NT Setup dialog box is displayed so that you can select the appropriate protocols. This dialog box has check boxes for the protocols included with Windows NT Server.

Note For more information on protocols see Chapter 1, "Installing Windows NT Server," in the *Windows NT Server Installation Guide.*

► **To install network protocols**

At this point you should see the Windows NT Setup dialog box on your screen, asking you to install network protocols. You need your Configuration Table for this procedure.

1. Select the appropriate network protocol(s) for your network and then choose Continue.

   Setup installs the network card, protocols, and services, and copies the appropriate files.

2. Complete any additional configuration required for your selected protocol(s).

   The Domain Settings dialog box appears.

► To configure the primary domain controller

You are now ready to name your domain. You need your Configuration Table for this procedure.

1. From the Domain Settings dialog box, select Primary Domain Controller.
2. In the Primary Domain Controller box, type **domain-a** and then choose OK.

   The Setup program checks that this domain does not already exist, and then configures your computer.

   The Administrator Account Setup dialog box appears.
3. Choose Continue (do not type a password for the Administrator account).

   A Setup message appears, indicating that no password has been entered.
4. Choose OK to leave the password blank.

Note For the purpose of this course, it is recommended that you leave the password blank.

Setup configures your hardware options and builds program groups.

The Date/Time dialog box appears.

► To complete the Windows NT Server configuration

After the adapters, protocols, and domain name are established, you must complete the installation.

1. Select the correct date, time, and time zone, and then choose OK.

   The Detected Display message appears.
2. Choose OK to acknowledge the message.

   The Display Settings dialog box appears.
3. Choose Cancel to accept the default display settings without testing them.

   A status box appears while Setup saves your configuration.

   A Setup message appears describing the Emergency Repair Disk.
4. Choose Yes, and then insert a blank disk when prompted.

5. Choose OK.

   The disk is formatted, and the Windows NT Registry information is copied to the disk.

   A Windows NT Setup message appears indicating that the installation is complete.

6. Remove the Emergency Repair Disk from Drive A, and choose Restart Computer.

   Your Windows NT Server primary domain controller is now installed.

Lesson Summary

Planning your installation is essential to creating a smooth-running network. The installation process of Windows NT Server is a straightforward process, which starts from a set of boot disks to load a limited version of Windows NT Server, then copies the files from the source media (CD-ROM, disk, or over the network) to a local hard disk, and finally configures the server according to information you supply during the Setup process.

For more information on	See
Installing Microsoft Windows NT Server	Chapter 1: "Installing Windows NT Server," in the *Windows NT Server Installation Guide*.

Lesson 3: Maintaining Backward Compatibility

In some situations you can keep Windows NT 3.1 workstations on your network. To maintain printer driver compatibility for these workstations, you can install a special set of print drivers on your Windows NT servers.

After this lesson you will be able to:

- Update printer drivers to maintain backward compatibility with Windows NT 3.1 print servers.

Estimated Completion Time: 5 minutes

Updating Printer Drivers

You can install printer drivers for both Windows NT Server and Windows NT 3.1 to provide backward compatibility to Windows NT 3.1 printer servers.

Directory Location of Printer Drivers

Storing drivers separately allows remote Windows NT 3.1 computers to use the Windows NT 3.1 version of the printer driver and allows the Windows NT Server computers to use the Windows NT Server version of the printer drivers.

Type	Stored in
Windows NT 3.1 printer drivers	*winnt_root*\SYSTEM32\SPOOL\DRIVERS *processor_type*\0
Windows NT 3.5 printer drivers	*winnt_root*\SYSTEM32\SPOOL\DRIVERS *processor_type*\1

To provide Windows NT Server print servers with backward compatibility for Windows NT 3.1 users, Windows NT 3.5 allows administrators to install printer drivers for both Windows NT Server and Windows NT 3.1. Because the Windows NT 3.5 print drivers do not function correctly on a Windows NT 3.1 system, the print drivers are version-stamped so that the correct drivers are always used by the computer.

Installing Windows NT 3.1 Drivers

Windows NT Server does not automatically add the Windows NT 3.1 version of the printer driver when a Windows NT Server printer driver is installed. This must be done manually. The process is identical to the way in which printer drivers were added for the other supported processors.

If the Windows NT 3.1 printer driver is not installed on the print server, remote Windows NT 3.1 computers receive the following message, "The server on which the printer resides does not have a suitable driver installed." when trying to connect to a printer through Print Manager.

Lesson Summary

In a mixed environment of Windows NT 3.1 and Windows NT Server computers, it is necessary to maintain printer drivers for both versions on the Windows NT Server computers.

For more information on	See
Installing printer drivers	Chapter 6, "Print Manager," in the *Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Installing printer drivers	Print Manager Help, Creating a Printer and Installing a New Printer Driver

Lesson 4: Removing Windows NT Server

Windows NT Server is now installed on your computer as a PDC. It can sometimes become necessary to remove programs from your computer. The procedures for removing Windows NT Server depend on the file system of the partition.

After this lesson you will be able to:

- Remove Windows NT Server from a FAT, HPFS, or NTFS partition.

Estimated Completion Time: 5 minutes

Removing Windows NT Server from a FAT Partition

If your computer was configured to boot from a FAT partition, it is possible to return the system to an exclusively MS-DOS system. The following steps must be performed to eliminate the Windows NT Boot Loader:

1. Boot the computer from an MS-DOS system disk that contains the SYS.COM program.
2. From drive A, type **sys c:**

   This transfers the MS-DOS system files to the boot track on drive C.
3. After the system files are successfully transferred, reboot the system from the hard disk.
4. To free space on the hard disk, delete the following:
   - c:\boot.ini (marked as system and read only)
   - c:\nt*.* (marked as hidden, system, and read only)
   - c:\bootsect.dos (marked as hidden, system, and read only)
   - *winnt_root*, \TEMP, \USERS, and \WIN32APP directories
   - pagefile.sys

Important The *winnt_root*, \TEMP, \USERS, and \WIN32APP directories, and the PAGEFILE.SYS file, might reside on a partition other than C.

Removing Windows NT Server from an NTFS or HPFS Partition

Perform the following steps to remove Windows NT Server from an NTFS or HPFS partition:

1. Start the computer from the Windows NT Setup boot disk.
2. When prompted to create or choose a partition, select the NTFS or HPFS partition where the Windows NT Server files are located, and then press D to delete the partition.
3. When prompted, press F3 to exit Setup: this removes Windows NT Server from the computer.

Older versions of FDISK do not remove an NTFS or HPFS partition. However, any of the following can be used to remove an NTFS partition:

- The Resource Kit utility DELPART.EXE
- The Windows NT Server Setup program
- MS-DOS 6.22
- OS/2 1.*x* installation disk A (deletes all partitions)

Lesson Summary

If it is necessary to remove Windows NT Server, the process is as follows: restore the MS-DOS boot sector and then delete all Windows NT Server files from all partitions.

For more information on	See
Removing NTFS partitions	Chapter 2, "Troubleshooting," in the *Windows NT Server Installation Guide.*

Lesson 5: Installation Issues

During the installation of Windows NT Server, you might encounter some difficulties. Most difficulties can be overcome very easily with proper planning. This lesson describes some common problems that can occur during the installation process.

After this lesson you will be able to:

- Identify common installation issues related to installing Windows NT Server.
- Describe possible solutions to the installation issues during installation of Windows NT Server.

Estimated Completion Time: 5 minutes

There are several problems that can arise during the installation process. The following table lists common installation problems and possible resolutions.

Problem	Possible resolution
Media errors	Try other media, or another method, such as an over-the-network installation.
Non-supported SCSI adapter	Boot computer under another operating system that can read from the SCSI adapter and CD-ROM drive, change to the CD-ROM drive, and run WINNT.EXE from the I386 directory.
	Try another method of installing, such as an over-the-network installation. Then add the adapter card driver.
	Replace adapter with a supported adapter card.
Not enough disk space	Use the Setup program to format an existing partition to create more disk space, or remove partitions and create new ones large enough to install into (approximately 90 MB).
The Dependency service failed to start	Return to the Network Settings dialog box. Verify that the correct protocol and network adapter are installed, that the network adapter has the proper configuration settings, including transceiver type, and that the local computer name is unique on the network.
Unable to connect to the domain controller	Verify that you have specified the correct name of the domain you joined and the correct administrator account and password (if you are creating the computer account during installation).
	Verify that the primary domain controller is running.
Error in assigning a domain name	If you are installing a primary domain controller, verify that the domain name you typed is a unique name on the network (it cannot be the same as any other domain or computer name).

Lesson Summary

It is possible to encounter errors during the installation of Windows NT Server. Most errors are due either to faulty hardware or media, or to user input errors when assigning configuration values, such as the computer, domain or workgroup names.

For more information on	See
Common installation problems	Chapter 2, "Troubleshooting," in the *Windows NT Server Installation Guide*.

CHAPTER 2

Using Groups to Manage Users

Before You Begin

This chapter requires that you have completed Chapter 1, "Installing Microsoft Windows NT Server 3.5." All of the exercises in this chapter require at least one Windows NT Server functioning as a primary domain controller.

You should review the groups section of the video included with this course.

Lesson 1: Overview of Groups

One very useful capability of Windows NT Server is the ability to use groups for administration. In this lesson, you learn about the different types of groups and their functions.

After this lesson you will be able to:

- List the types of groups used by Windows NT Server.
- Explain the differences between the types of groups.

Estimated Completion Time: 10 minutes

Introduction to Groups

A group is an account that contains other user and group account information. The accounts contained within a group are members of that group.

By default, user accounts have no rights. They obtain rights either by explicit assignment of rights to the user account or through membership in a group that has rights. Groups are useful because they simplify administration by organizing many separate accounts into one administrative unit. Groups can be used to:

- Give rights to users who perform the same system tasks, such as back up and restore files, or change the system time.
- Grant access permissions to resources, such as files, directories, and printers.

The permissions and rights granted to a group are automatically granted to its members, which makes it possible for an administrator to treat large numbers of users as one account.

Types of Groups

Microsoft Windows NT Server uses three types of groups. Each type of group has its own purposes, capabilities, and limitations. The groups are as follows:

- Local—This type of group is implemented in each computer's account database. Local groups consist of the individual user accounts that have rights and permissions on the local computer, and other group accounts that are used to simplify administration (such as global or built-in groups). The administrator for the computer can create additional local groups for managing resource access.

- Global—This type of group is used across an entire domain (and trusted domains; see Chapter 5 for more information on Trust Relationships). Global groups are created on a PDC and can contain user accounts only from their own domain's account database.
- Special—These groups are generally used by Windows NT Server for internal system access to resources and permissions. Administrators cannot add users to special groups. The special groups contain predefined sets of users, such as creator/owner of resources.

The terms "local" and "global" have special definitions in the server environment; in some instances, you will find that "local" can be more inclusive than "global." Please keep this in mind as you go through this chapter.

Built-in Groups

Because there are certain system tasks that are performed on every system, Windows NT Server 3.5 comes with a set of built-in local and global groups. These built-in groups are designed to automatically group users who need to perform similar tasks into easily administered groups. Built-in groups are used to give users rights to perform system tasks such as back up and restore files, change the system time, administer system resources, and so on.

Experienced network administrators plan groups as part of basic network installation. As you create each new user account, you assign the new users to the proper groups as part of the process. It is important that you investigate what each user account will do on the network and which local and network resources each account needs to access.

Lesson Summary

Groups are used to refer to a set of users as a single account for purposes of administration and resource access assignment. There are three types of groups: global, local, and special. Each type of group has its own purposes, capabilities, and limitations.

For more information on	See
Windows NT user groups	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*
	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
Using global groups	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*

Lesson 2: Local Groups

Each computer has a database that contains information about users defined on that computer. This database is considered the local accounts database.

While you could enter every potential user individually in the local accounts database on each computer, local groups allow you to assemble multiple users who have the same rights and permissions into a single administrative unit. This lesson introduces local groups and their purpose, use, and implementation.

After this lesson you will be able to:

- List the capabilities and limitations of local groups.
- Explain the use of built-in local groups.
- List the possible members of a local group.

Estimated Completion Time: 20 minutes

Local Groups

A local group is a single administrative unit that contains account information about multiple users who have similar rights and permissions on a specific computer. Local groups are useful for organizing user accounts into one manageable unit.

A local group is available only in the account database in which it resides. In other words, local groups are assigned user rights and permissions to resources on the computer where the local group resides.

The following table summarizes where local groups are effective.

Local group created on...	Can be used on...
Windows NT Workstation or Windows NT Server computer (when installed as a server)	Only that computer
Windows NT Server domain controller	The domain database and where that database is copied, for example, other Windows NT Server domain controllers within the domain where the group was created

Built-in Local Groups

Because there are system administrative tasks that are common to almost every system, Windows NT Server comes with several built-in local groups. These groups exist to make your administrative tasks simpler. Rather than creating a custom local group for a common set of functions, these groups are already created for you. You should consider using the built-in local groups whenever possible.

Built-in local groups are used to give users rights to perform system tasks such as back up and restore files, or change the system time, and also to administer system resources. Some of the built-in local groups exist only on Windows NT Servers (those that are not domain controllers), and others only on Windows NT Servers functioning as domain controllers.

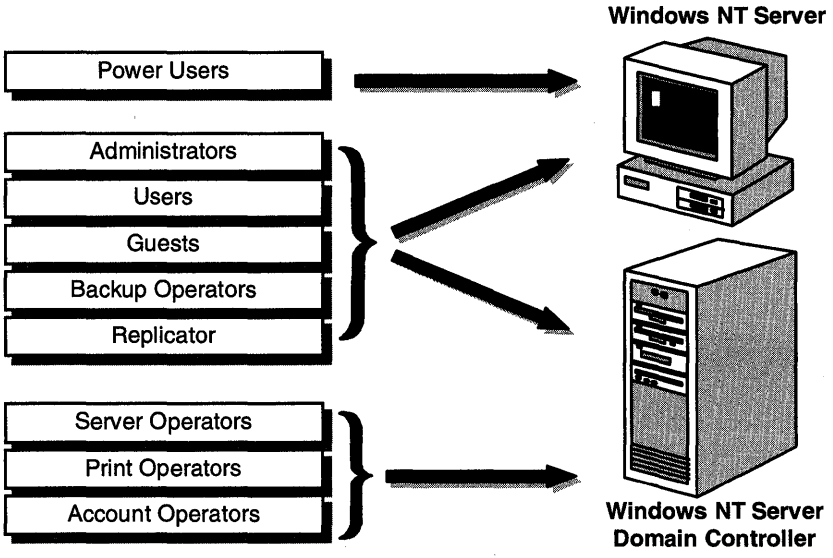


Figure 13: Built-in local groups and where they are created

Built-in local groups are divided into three categories:

- Administrators—Members of this group have full capabilities on a computer.
- Operator-type groups—Members of these groups have limited administrative capabilities to perform specific tasks. These groups include Account Operators, Backup Operators, Server Operators, Print Operators, Power Users, and Replicator.
- Other user-type groups—Members of these groups have limited capabilities on the system, such as accessing applications and printers. These groups include Users and Guests.

The following table lists the local groups provided on Windows NT Server domain controllers.

Local group	Initial contents	Who can modify?	Capabilities
Administrators	Domain Admins (global group) Administrator (user account)	Administrators	Create, delete, and manage user accounts, global groups, and local groups Share directories and printers, grant resource permissions and rights Install operating system files and programs
Users	Domain Users (global group)	Administrators, Account Operators	Perform tasks for which they have been given rights Access resources to which they have been given permissions
Guests	Domain Guests (global group)	Administrators, Account Operators	Perform tasks for which they have been given rights Access resources to which they have been given permissions
Server Operators	None	Administrators	Share and stop sharing resources Lock or override the lock of a server Format the server's disks Log on at servers Back up and restore servers Shut down servers
Print Operators	None	Administrators	Share and stop sharing printers Manage printers Log on locally at servers and shut servers down
Backup Operators	None	Administrators	Back up and restore files and directories Log on locally Shut down the server

(continued)

Local group	Initial contents	Who can modify?	Capabilities
Account Operators	None	Administrators	Create, delete, and modify users, global groups, and local groups Cannot modify administrator or server operator groups
Replicator	None	Administrators, Account Operators, Server Operators	Used in conjunction with the Directory Replicator Service

Note The Power Users group is a special local group set up specifically for computers running Windows NT Workstation and Windows NT Server (installed as a server and not as a domain controller). Power Users can create and modify accounts and share resources.

Built-in local groups cannot be deleted. The challenge for an administrator is to determine how to use built-in local groups most efficiently. To do that, you have to determine what tasks need to be performed and which group can best perform those tasks.

► To view the built-in groups that are allowed to log on locally by default

In this procedure, you determine which built-in local groups can log on locally at your domain controller.

Important Complete this procedure logged on as Administrator of DOMAIN-A.

1. From the Administrative Tools group, start User Manager for Domains.
2. From the Policies menu, select User Rights.

   The User Rights Policy dialog box appears.
3. In the Right box, select Log on Locally.

   In the Grant To box you see the list of local built-in groups that by default are assigned the right to log on locally at a domain controller.
4. Which built-in groups are assigned the right to log on locally at a Windows NT Server domain controller?

5. Choose Cancel to return to User Manager For Domains.

Custom Local Groups

You might have situations in which the built-in groups do not meet the needs of your system. In such a situation, you can create a local group that meets your specific needs.

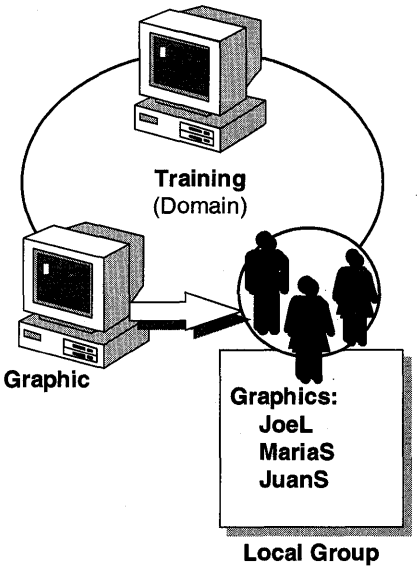


Figure 14: Custom local group

For example, you have a special-purpose computer dedicated to graphics creation. You want a certain set of users to be able to access this computer and configure the monitor. You can create a local group consisting of only the users and assign them the appropriate rights and permissions.

► To create local groups

In this procedure, you create local groups. You need your Configuration Table for this procedure to name your local groups.

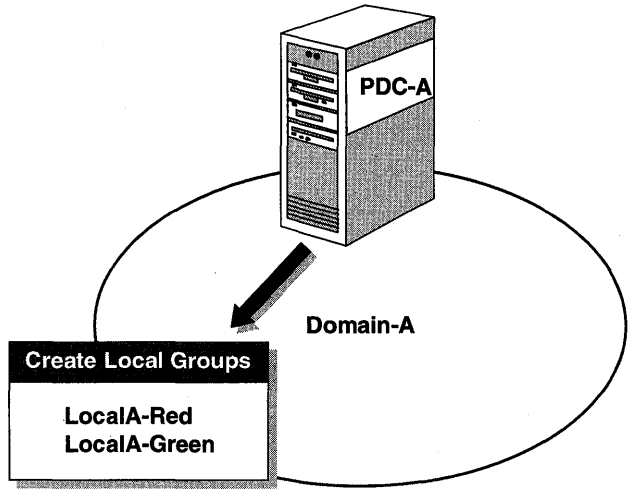


Figure 15: Create local groups

Important Complete this procedure logged on as Administrator of Domain-A.

1. Using User Manager for Domains, create a local group named LocalA-Red.
2. Remove any members from LocalA-Red.
3. Create a local group named LocalA-Green.
4. Remove any members from LocalA-Green.

Local Group Membership

In a workgroup environment, a Windows NT computer's local group can include only user accounts from that computer's account database.

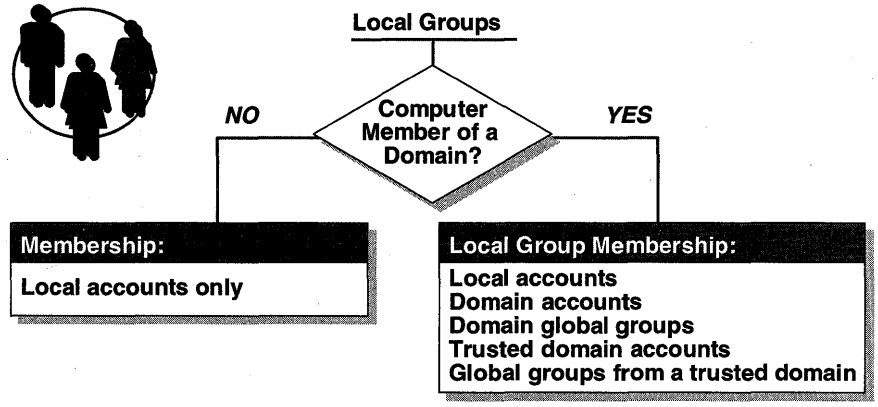


Figure 16: Local group membership

A local group on a computer running Windows NT Workstation or Windows NT Server installed in a domain can include the following members:

- User accounts from the local computer.
- Users and global groups from the local computer's domain.
- Users and global groups from domains trusted by the local domain.

Important Local groups cannot contain other local groups.

You can use local groups to assign the following:

- User rights
- Permissions on NTFS files and directories
- Permissions on share names

Lesson Summary

One of the best ways to simplify administration is to make use of the built-in groups of Windows NT. On a Windows NT server, the built-in groups are as follows:

- Power Users
- Administrators
- Users
- Guests
- Backup Operators
- Replicator

On a Windows NT Server domain controller, the built-in groups include all of the above (except Power Users) and the following:

- Server Operators
- Print Operators
- Account Operators

Local groups are useful in assigning user rights or resource access permissions to local user accounts and to domain user and global group accounts. Another advantage of a local group is the ability to include as members both user and global group accounts from not only the local domain, but also from any trusted domains.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. List two local groups provided for Windows NT Server that are configured as a server and domain controller.

2. List two operator groups provided only for Windows NT Server domain controllers.

3. Name an existing group that would provide an account with authority limited to managing printers.

For more information on	See
Built-in local groups	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*
Using local groups	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*

For online information about	From the Help menu, choose Contents and then
Creating local groups	User Manager for Domains Help, Manage Local Groups

Lesson 3: Global Groups

The concept of global groups is somewhat similar to the concept of local groups, except that global groups extend across a domain, which makes them very efficient in managing access to resources across the domain. Global groups can also be added to local groups for local computer access. This lesson describes the uses of global groups, including the built-in groups that are automatically created in Windows NT Server.

After this lesson you will be able to:

- Identify the built-in global groups.
- Explain the functions of the built-in global groups.
- Indicate which accounts can be members of a global group.

Estimated Completion Time: 20 minutes

Global groups are different from local groups in that they cannot contain other group accounts. The global groups account information resides on the primary domain controller as part of the user accounts database, and it is therefore copied to the backup domain controllers.

Global groups can contain one or more users from their own domain's account database. Global groups can be assigned user rights and permissions to resources on the domain where the global group resides, or on any trusting domain. Global groups can also be assigned user rights or permissions to a resource by including them in local groups that have the necessary permissions.

Built-in Global Groups

Windows NT Server also has built-in global groups. Like local groups, it is recommended that, whenever possible, you use the built-in global groups to simplify the administration of your system. The built-in global groups are the following:

- Domain Admins—This built-in global group allows the grouping of user accounts, so that when Domain Admins is made a member of a local Administrators group, any domain administrator can perform any administrative function on any workstation or server that is a member of the domain.

For example, you might add all the administrative accounts in the domain to the Domain Admins group. When a Windows NT Workstation joins a domain, the Domain Admins group automatically becomes a member of the workstation's local Administrators group. This arrangement allows any user logged on as a domain administrator to perform administrative functions on a Windows NT Workstation, either locally or remotely. This arrangement of groups also means that users do not have to be familiar with the administrative functions of Windows NT because these can be handled for them by a domain administrator.

- Domain Users—This built-in global group is similar to the Domain Admins group in that it groups user accounts. When Domain Users becomes a member of a local Users group which has been given appropriate access, any member of this group can access shared resources in the domain. However, members cannot perform administrative functions.
- Domain Guests—This built-in global group is similar to Domain Users, but it allows you to limit guest access to resources.

► **To determine built-in global group membership**

In this procedure, you determine the default members of each of the built-in global groups.

Important Complete this procedure logged on as Administrator of DOMAIN-A.

---

1. From User Manager for Domains, select Domain Admins. Which default users are automatically members of Domain Admins?

2. Choose Cancel.
3. Select Domain Guests. Which default users are automatically members of Domain Guests?

4. Choose Cancel.
5. Select Domain Users. Which default users are automatically members of Domain Users?

6. Choose Cancel.

Custom Global Groups

While using the built-in global groups makes your administrative tasks easier, you might encounter situations in which you need to create your own global group.

Global groups do not have the inherent authority to perform network administrative functions. To perform administrative tasks, global groups must either be added to a local group (for example, adding the global group Domain Admins to the local group Administrators) or be explicitly assigned the user right.

Instead of assigning permissions to each global group, you assign permissions to the local group to which global groups have been made members. This allows a local group to be assigned a right or permission in a single administrative operation.

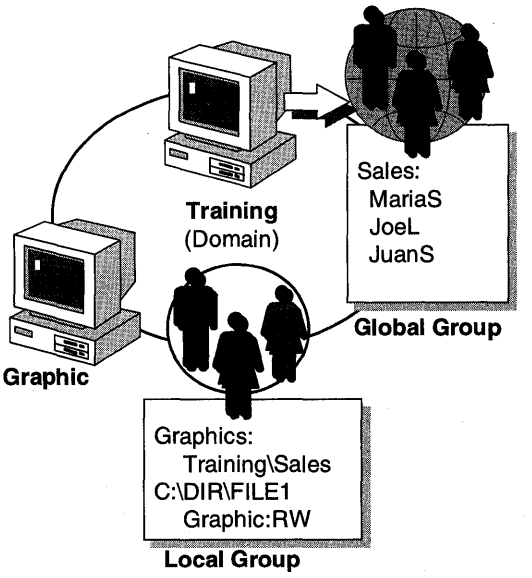


Figure 17: Relationship between local and global groups

For example, the global group Sales consists of users from the TRAINING domain. These users need access to a resource on the computer GRAPHIC. The users could be assigned permissions individually to the GRAPHIC's resource, but because they are already members of the global group SALES, it is easier to add the global group SALES to the local group GRAPHICS on the computer GRAPHIC, and then assign resource permissions to the local group.

The local group might even contain users and global groups from multiple domains. If more users are hired, you simply add the new users to the appropriate global group that is part of a local group. The new users have immediate access to the appropriate resources and user rights.

By default, when a user account is created in a domain, it is automatically assigned to the global group Domain Users.

Important Local and global groups cannot use the same name. Group names must be unique within the database.

Global Group Membership

Global groups can contain only user accounts as members. They cannot contain either local groups or other global groups.

Because local groups are limited to the account database in which they are defined, it is recommended to use global groups to ensure that groups of users are equally available (with a minimum of administration) on Windows NT Workstation and Windows NT Server computers.

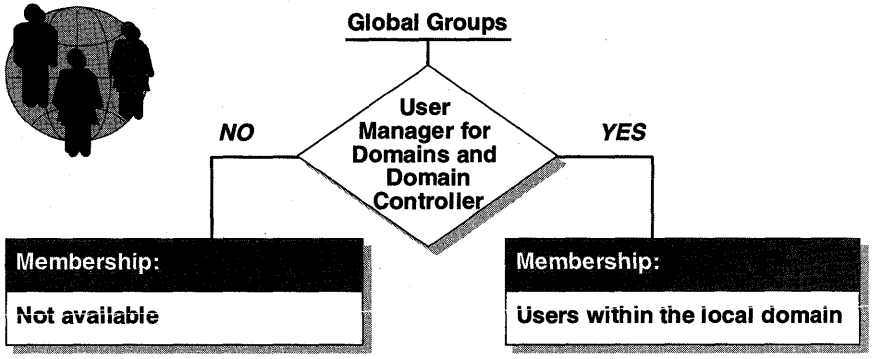


Figure 18: Determining global group membership

Creating Groups

Both local and global groups are created using User Manager for Domains. However, global groups can be created only on a computer running Windows NT Server configured as a domain controller.

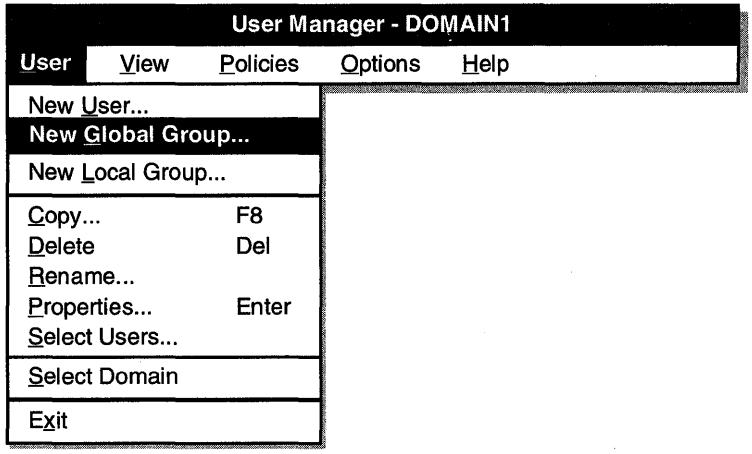


Figure 19: Creating groups with User Manager

The following table outlines the configuration required to create local and global groups.

Group	Windows NT Workstation or Windows NT Server (configured as a server)	Windows NT Server (configured as a domain controller)
Local	■	■
Global	❑	■

You can use global groups to assign the following:

- User rights
- Permissions on NTFS files and directories
- Permissions on share names

► To create a global group

In this procedure, you create three user accounts and two global groups. Make the users members of the appropriate global group. You need information from your Configuration Table in this procedure.

Important Complete this procedure logged on as Administrator of DOMAIN-A.

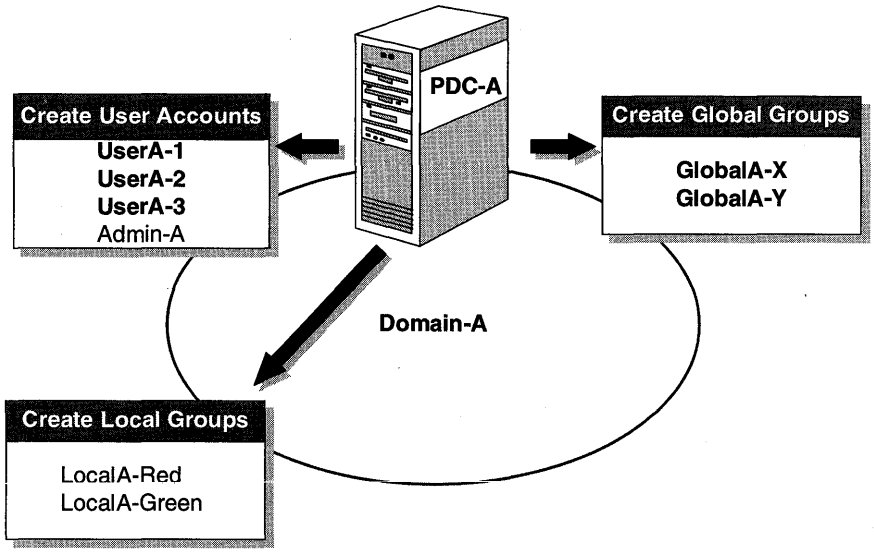


Figure 20: Create users and global groups

1. Use User Manager for Domains to create user accounts for UserA-1, UserA-2, and UserA-3, using the following information:

   Clear the User Must Change Password at Next Logon check box.
2. From the User menu, choose New Global Group.

   The New Global Group dialog box appears.
3. In the Group Name box, type **GlobalA-x**
4. In the Members box, add **UserA-1** and **UserA-2**, and then choose OK.
5. Create a global group named GlobalA-Y, and then add **UserA-3** as a member.

   You have created the users and the global groups, and have made the users members of the global groups.

► To determine the effects of global group membership

In this procedure, you determine the effects of global group membership by creating a user account and attempting to log on to the PDC as a user. You need your Configuration Table in this procedure to name your administrator user.

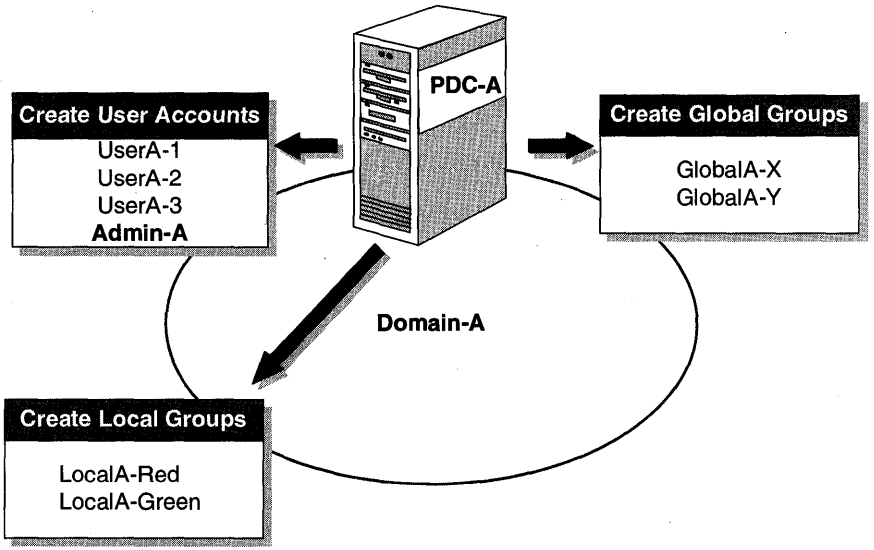


Figure 21: Add user Admin-A

Important Complete this procedure logged on as Administrator of DOMAIN-A.

1. Create a user named Admin-A, clearing the User Must Change Password at Next Logon check box.
2. To which built-in global group(s) is Admin-A automatically assigned?

3. Exit User Manager for Domains, and log off.
4. Attempt to log on as Admin-A.
5. Were you successful? Why or why not?

6. Log on as Administrator, and then start User Manager for Domains.
7. Add Admin-A to the Domain Admins global group.
8. Exit User Manager for Domains, and log off.

9. Attempt to log on as Admin-A.
10. Were you successful? Why or why not?

11. Log off and then log back on as Administrator.

Lesson Summary

One of the best ways to simplify administration is to use the built-in groups of Windows NT. Global groups are effective in administration, because they can be used to assign access permissions to resources throughout the domain, and they can also be added to local groups for local computer access. Windows NT Server creates three built-in global groups: Domain Admins, Domain Users, and Domain Guests.

For more information on	See
Built-in global groups	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*
Using global groups	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*

For online information about	From the Help menu, choose Contents and then
Creating global groups	User Manager for Domains Help, Manage Global Groups

Lesson 4: Special Groups

When planning your network, you will have situations in which the location for accessing a resource is more important than who is accessing it. One example is giving only interactive users access to a resource. For these situations, there are special groups. This lesson explains the functions of special groups.

After this lesson you will be able to:

- List the functions of special groups.
- Identify the special groups used by Windows NT Server.

Estimated Completion Time: 10 minutes

Special Groups

In addition to the local and global groups, special groups organize users based on how they access various resources. Special groups do not take members in the usual sense. Administrators cannot assign users to them. Rather, users are either members of these groups by default, or they become members of these groups based on the users' activity.

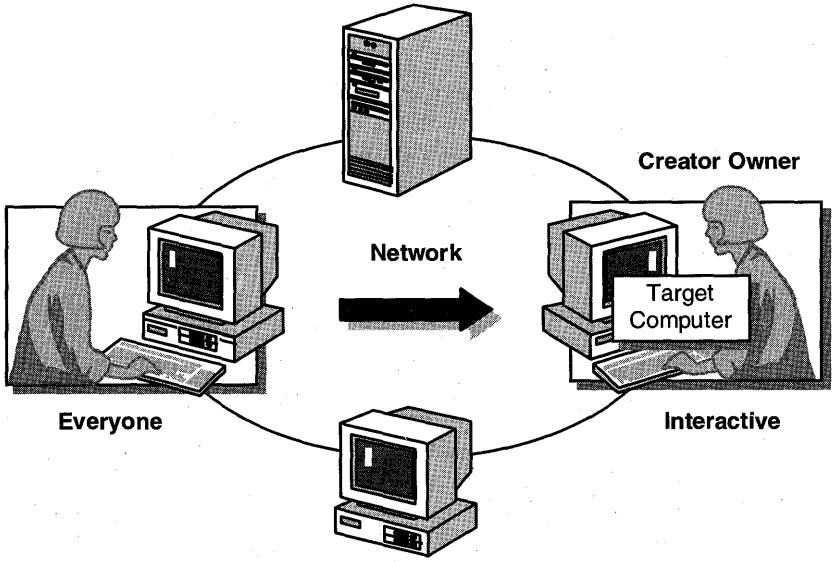


Figure 22: Special groups membership

There are four special groups: Network, Interactive, Everyone, and Creator Owner. These groups are created as part of the installation process.

Network

The special Network group includes any user, current or future, who connects to a shared network resource. If a user goes over the network to access a resource using the user's own account or an enabled guest account, that user is considered a network user.

Interactive

The user who logs on locally is automatically included in the Interactive group at logon. Interactive members access resources on the computer at which they are physically sitting. They log on and access resources by "interacting" with the computer.

The distinction between Network and Interactive is important in terms of permissions. For example, if a user sits down at computer A and acts as a local user to access a resource on that computer, that user is thought of as an interactive user and has permissions assigned to the Interactive group.

However, if the same user moves to another computer and uses the network to access the same resource on computer A, that user is now working with permissions assigned to the Network group. The permissions assigned to the Interactive group are no longer available to the user connecting over the network, and thus the user's use of the resource might differ from earlier access as an Interactive user.

Everyone

The Everyone group automatically includes any user who accesses the computer. This includes guests and users from other domains, as well as interactive and network users. Administrators can assign any User Right to Everyone and grant Everyone access permissions to files, directories, share names (shared resources), printers, and Registry keys.

Because all users are members of the Everyone group by default, there is no need to add user accounts to the Everyone group. You can remove the Everyone group from the permission lists to prevent resource access. For example, by default the Everyone group has Full Control permissions to shared directories. You might modify or even remove the Everyone group's Full Control permissions and add appropriate permissions as needed.

Creator Owner

This group includes the user account (or the Administrators group if the user is an administrator) that created or took ownership of a resource.

On an NTFS partition, the Creator Owner group permissions are assigned at the directory level. The owner of any directories or files created under this directory is given the permissions assigned to Creator Owner.

This special group can be used to manage assigned permissions to files and directories created in a public area on an NTFS partition. For instance, on a public directory you can assign the Everyone group Read access while giving the Creator Owner group Full Control access. Any user that creates files or subdirectories in this directory has Full Control over them.

Viewing the Special Groups

Viewing the special groups in Windows NT Server can be done in three different ways: on an NTFS partition, an installed printer, and a shared directory. Select the appropriate method below for your use:

Important Complete this procedure logged on as Administrator of DOMAIN-A.

► **To view the special groups if you have an NTFS partition**

1. From File Manager, select an NTFS partition.
2. From the Security menu, choose Permissions.
3. From the Directory Permissions dialog box, choose Add.
4. Scroll through the Names list box to see Special groups.
5. Choose Cancel twice and exit File Manager without saving any changes.

► **To view the special groups if you have an installed printer**

1. From Print Manager, select the printer.
2. From the Security menu, choose Permissions.
3. From the Printer Permissions dialog box, choose Add.
4. Scroll through the Names list box to see Special groups.
5. Choose Cancel twice and exit Print Manager without saving any changes.

► **To view the special groups when sharing a directory**

1. Start File Manager, and then select \USERS\DEFAULT on your PDC-A drive.
2. From the Disk menu, choose Share As.
3. In the New Share dialog box, choose Permissions.
4. In the Access Through Share Permissions dialog box, choose Add.
5. Scroll through the Names list box to see Special groups.

   Notice that Creator Owner is not a valid choice for a shared directory. It applies only to NTFS directories and installed printers.
6. Choose Cancel three times and exit File Manager without saving the shared directory.

Lesson Summary

Windows NT Server includes four special groups that can assist in securing or controlling access to resources on the network. These groups are Creator Owner, Everyone, Interactive, and Network. By default, any resource that is created assigns Full Control permissions to the group Everyone.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You are implementing Windows NT Server in your network, and have decided that you do not want to allow all users to have complete access to the NTFS partitions on the servers. How can you secure the NTFS partitions?

2. You are creating a shared directory for user access. You have decided to ensure that all users accessing the resource over the network can view the files but not change them. How can you secure the shared files?

For more information on	See
Built-in special groups	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*
Using special groups	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*

Lesson 5: Using Groups to Manage Resource Access

When you have an understanding of local, global, and special groups, you can design a strategy for implementing the various groups. The strategy should involve using the built-in groups when applicable, and creating groups when necessary.

After this lesson you will be able to:

- Plan groups to organize network management tasks.
- Analyze a set of tasks and determine the appropriate groupings.
- Assign users to the appropriate groups.

Estimated Completion Time: 10 minutes

Using Groups to Manage a Network

You can use groups to simplify network management tasks.

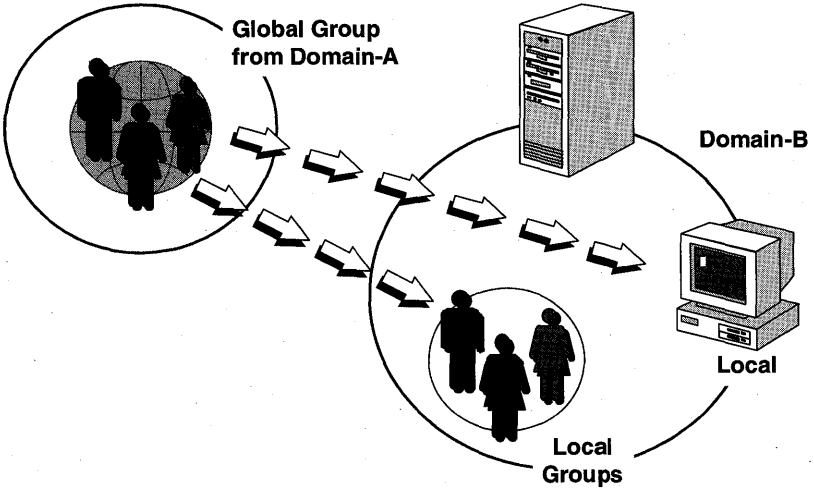


Figure 23: Using groups to manage a network

In the figure above, you see an example of a global group from DOMAIN-A being made a member of a local group in DOMAIN-B.

The following table outlines which type of group you should use to manage specific administrative activities.

Administrative activity	Best type of group to use	Explanation
Group domain users into a single unit for use in other domains.	Global	A global group can be added as a member of local groups or can be given permissions and rights directly in other domains.
Manage permissions and rights in a particular domain.	Local	The local group can contain users and global groups from trusted domains.
Need permissions on Windows NT workstations or servers in a domain.	Global	Local groups in a domain work only on Windows NT Server domain controllers.
Contain other groups.	Local	Local groups can contain users and global groups.
Include many users from many domains.	Local	A local group can include users and global groups from trusted domains.

Global groups have no built-in user rights. Global groups obtain their user rights from the local group to which they are assigned.

Groups Strategy and Guidelines

Before you begin implementing groups, you should have a strategy for the implementation process. Keep in mind the following guidelines:

1. Determine what you need to accomplish. Is it one of the following?
   - A network responsibility (assigning administrative tasks, creating users)
   - Assigning permissions to resources
2. Use built-in global and local groups wherever possible. Determine whether there is an existing group that can perform the task.
3. At your primary domain controller, create any new user accounts and global groups that are necessary.
4. Assign the appropriate users to existing or newly created global groups for domain-wide access.
5. Where needed, create any new local groups.
6. Add global groups to the appropriate local groups.
7. Assign the local group to user rights and resource permissions.

After you have a groups strategy, you are ready to implement it.

▶ To test user rights and groups

In this procedure, you assign a local group the ability to log on locally at the domain controller. You need your Configuration Table in this procedure.

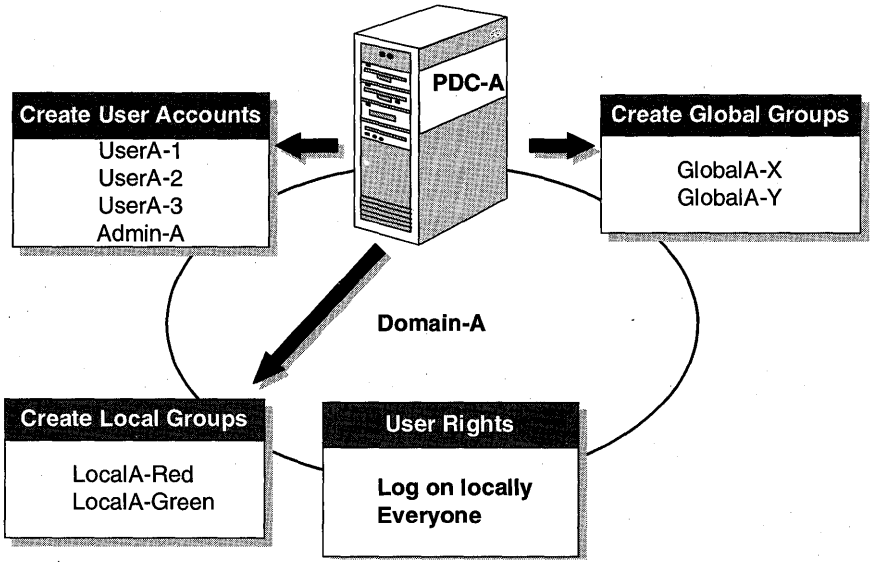


Figure 24: Assigning user rights

1. Log off, and attempt to log on to PDC-A as UserA-1.
2. Were you successful? Why or why not?

3. Log on as Administrator, and then start User Manager for Domains.
4. From the Policies menu, choose User Rights.

   The User Rights Policy dialog box appears.
5. In the Right box, select Log on Locally.

   Notice that only Administrators and the Operators built-in groups are allowed to log on to the domain controller.
6. Choose the Add button.

   The Add Users and Groups dialog box appears.
7. Under Names, select Everyone, and then choose Add.
8. Choose OK to return to the User Rights Policy dialog box.

   Notice that Everyone is added to the list of accounts permitted to log on locally at the domain controller.

9. Choose OK to return to User Manager for Domains.
10. Log off as Administrator, and attempt to log on as UserA-1.
11. Were you successful? Why or why not?

12. Log off as UserA-1, and then log on as Administrator.

    Your computer is now ready for the next procedure.

► To add a global group to a local group

In this procedure, you add a global group to a local group.

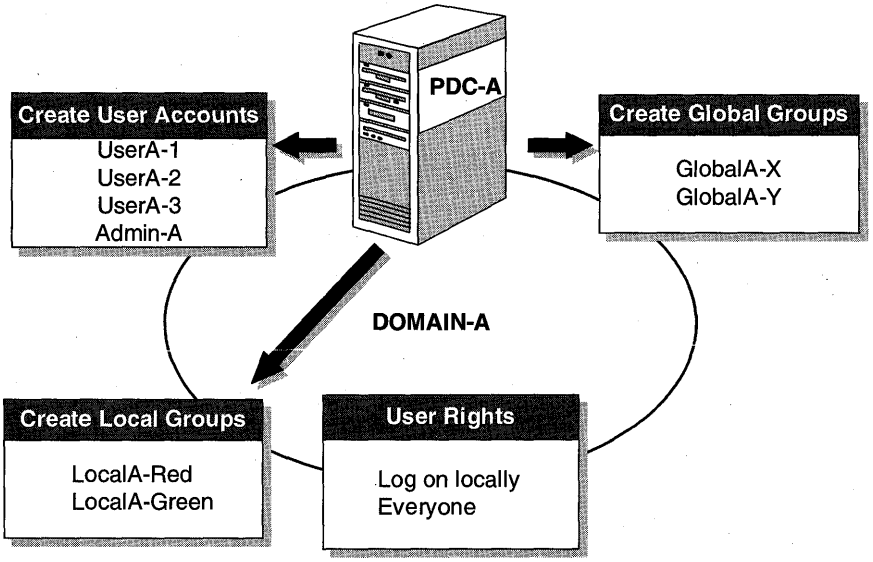


Figure 25: Add global groups to local groups

Important Complete this procedure logged on as Administrator of Domain-A.

1. Using User Manager for Domains, access the local group properties of LocalA-Red.

   The Local Group Properties dialog box appears.
2. Choose Add.

   The Add Users And Groups dialog box appears.
3. Select GlobalA-X and then choose Add.

4. Choose OK.

   The Local Group Properties dialog box appears, indicating that GlobalA-X is now a member of LocalA-Red.

5. Add GlobalA-Y as a member of LocalA-Green.
6. Which user account(s) receive permissions and rights based on group memberships of LocalA-Red?

7. Which user account(s) receive permissions and rights based on group memberships of LocalA-Green?

► To assign permissions using groups

In this procedure, you create a shared directory and assign the appropriate access permissions. You need your Configuration Table in this procedure.

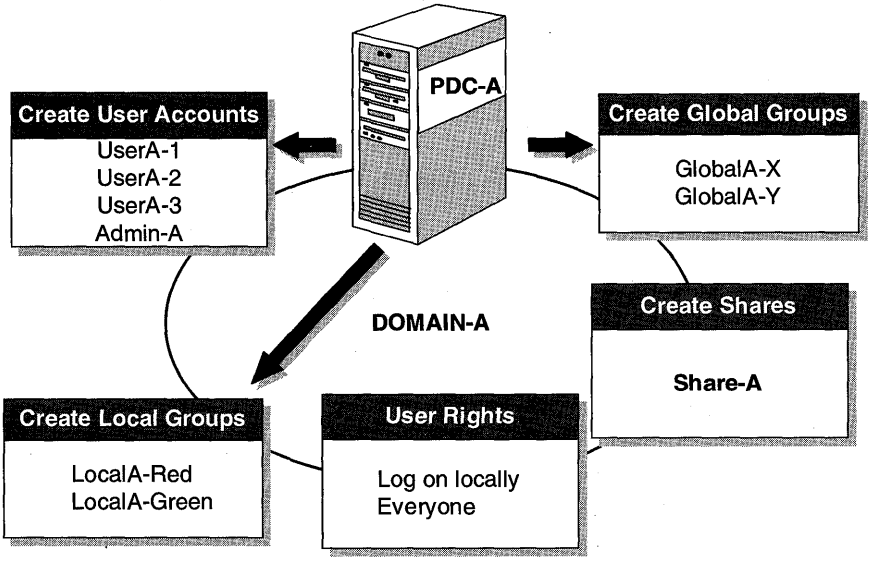


Figure 26: Create Share-A

Important Complete this procedure logged on as Administrator of DOMAIN-A.

1. Start File Manager, and select \USERS\DEFAULT on the PDC-A drive.
2. From the Disk menu, choose Share As.

   The New Share dialog box appears.
3. In the Share Name, type **share-a** and then choose Permissions.

   The Access Through Share Permissions dialog box appears. Notice the default permissions of Full Control on the group Everyone.
4. Choose Remove to not permit access to Everyone.
5. Choose Add.

   The Add Users And Groups dialog box appears.
6. Under Names, select LocalA-Green, and then chose Add.
7. In the Type of Access box, select Read, and then choose OK.
8. Choose Add, and add Administrators with Full Control permissions.

   In the Access Through Share Permissions dialog box, verify that the local group Administrators has Full Control and that the local group LocalA-Green has Read permissions.
9. Choose OK to return to the New Share dialog box.
10. Choose OK to share the directory.
11. Exit File Manager, and log off as Administrator.
12. Log on as UserA-1, and then start File Manager.
13. Attempt to connect to \\PDC-A\Share-A and read the directory.
14. Were you successful? Why or why not?

15. Disconnect from the directory, and log off as UserA-1.
16. Log on as Administrator, and attempt to connect to \\PDC-A\Share-A and read the directory.
17. Were you successful? Why or why not?

18. Disconnect from the directory.

Lesson Summary

Securing access to resources is one of the goals of network administration. By properly making use of local and global groups, you can effectively manage access to local files, directories, and printers, as well as access to network resources and user rights.

For more Information on	See
Implementing groups	Chapter 3, "How Network Security Works," in the Microsoft Windows NT Server Concepts and Planning Guide.

CHAPTER 3

Configuring the User Environment

Before You Begin

This chapter requires that you have completed Chapter 1, "Installing Microsoft Windows NT Server 3.5," and Chapter 2, "Using Groups to Manage Users." All of the procedures in this chapter require at least one Windows NT Server functioning as a primary domain controller.

You need your lesson disk to complete this chapter.

Lesson 1: User Manager for Domains

User Manager for Domains is the main tool you use to configure the user environment. This lesson explains how you can use User Manager for Domains to configure the account properties for a user. You learn how to specify a home directory, restrict domain logon hours, determine which workstations can be used to log on to a domain, and set an expiration date for the account.

After this lesson you will be able to:

- Configure account properties.
- Specify a home directory for a user.
- Restrict users from logging on to the domain during a specific time period.
- Restrict users from logging on to specific workstations.
- Specify an account expiration date.
- Specify an account type.

Estimated Completion Time: 60 minutes

User Manager for Domains

User Manager for Domains is the tool used to create and manage user accounts, create and manage groups, and manage security policies.

A Windows NT user account consists of the user name and password required for the user to log on, the groups in which the user account has membership, and the rights the user has for using the system. It also includes other information, such as the user's full name, the account description, the user environment profile information, a list of logon workstations, a schedule of logon hours, and more.

Like groups, some built-in user accounts are provided when a Windows NT Server domain is created. These accounts are:

- Administrator—The account you use when you first administer a new server or workstation, before you create an account for yourself. It is used for local administration of the computer and the domain's account database.
- Guest—An account used for guest logons, which are logons by people who do not have a valid user account. The Guest account is disabled by default when Windows NT Server is installed.

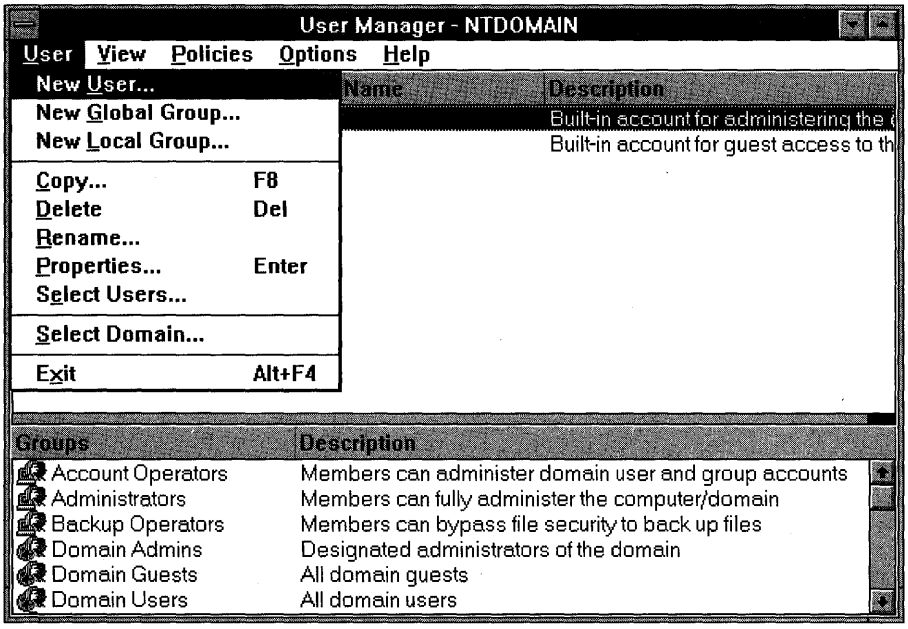


Figure 27: Creating a new user with User Manager for Domains

You can use User Manager for Domains to create additional user accounts for other users who will be logging on, and you can modify existing accounts.

Note Do not confuse the User Manager for Domains with the User Manager available in the Microsoft Windows NT Workstation product. User Manager for Domains can manage properties for the local domain and for remote domains and computers.

Each domain has one security database, located on the primary domain controller (PDC), which:

- Contains user and group accounts.
- Defines the security policies for the domain.

To use User Manager for Domains you must be one of the following:

- An Administrator—Has full functionality in User Manager for Domains.
- A member of the Domain Admins global group—Has full functionality in User Manager for Domains, provided that Domain Admins is a member of the Administrators local group. For the local domain, Domain Admins is a member of the Administrators local group. If you want to have account administration between domains, you need to add the local domain's Domain Admins global group to the other domain's Administrators local group.

- A member of the Account Operators group—Has limited functionality in User Manager for Domains.
- A user—Has the ability to create local groups and manage local groups that the user has created.

If a user does not have sufficient authority to perform an action in User Manager for Domains, that command or option is usually shown as unavailable. For example, a user (member of the Users local group) cannot use User Manager for Domains to create a new user or global group. In some cases the command is displayed as available and the user is able to invoke it, but the command is not executed. For example, a user (member of the Users local group) will not be successful in renaming an existing user or group account.

Account Properties

To see or change a user's account properties, select a user account, and then choose Properties from the User menu.

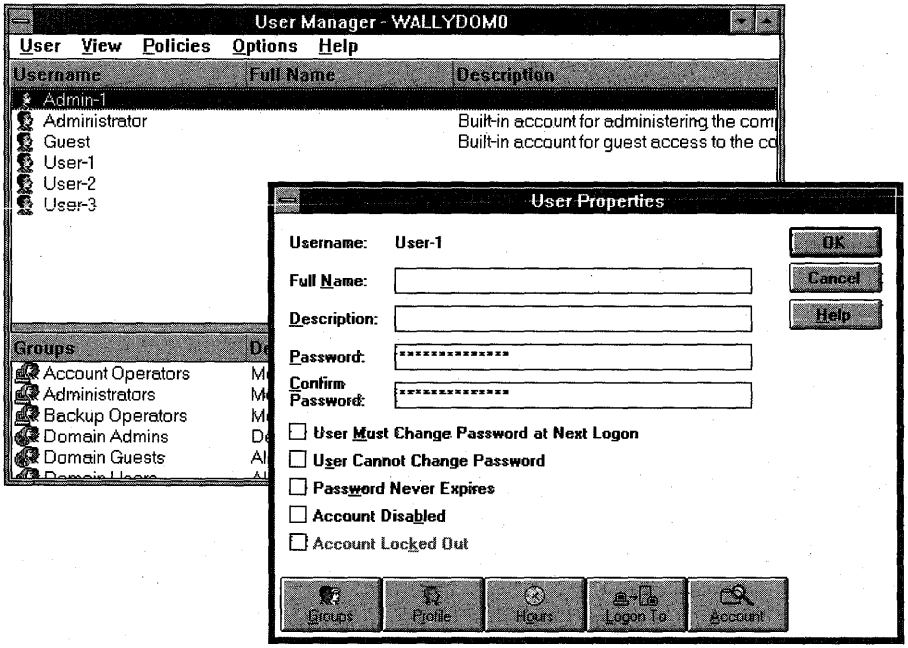


Figure 28: User Properties dialog box

From the User Manager for Domains User Properties dialog box, you can do the following:

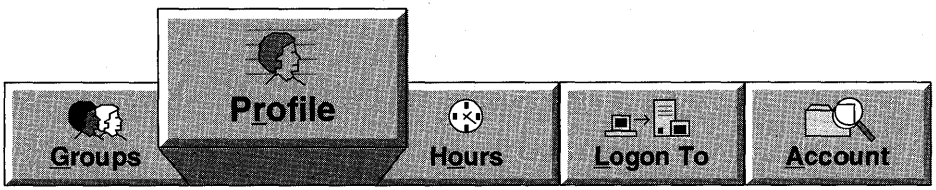
- Adjust a variety of properties for an account, including full name and description of the user and password attributes.
- Add and remove users from Groups.
- Disable the account.

Profiles

Windows NT saves specific information in user profiles for each user account in a domain. This information includes settings in Program Manager, File Manager, Control Panel, Print Manager, and Accessories.

More details about Profiles are given in the next lesson.

The Profile option is used to define the user profile path, logon script name, and home directory for the selected user accounts.



To access the profile information, from the User Manager for Domains Account Properties dialog box, choose the Profile button.

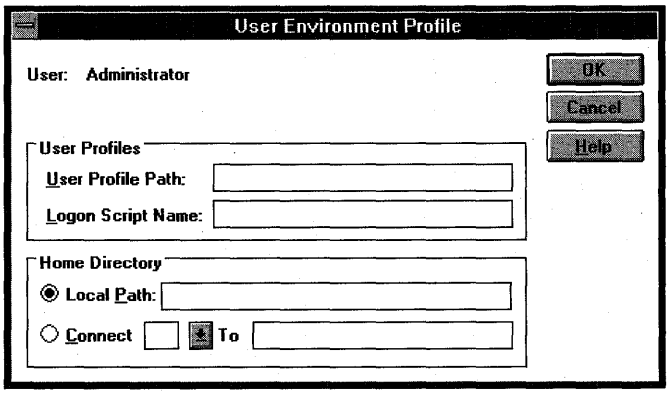


Figure 29: User Environment Profile dialog box

► **To create a shared home directory**

In this procedure, you create a share that will be used as a home directory.

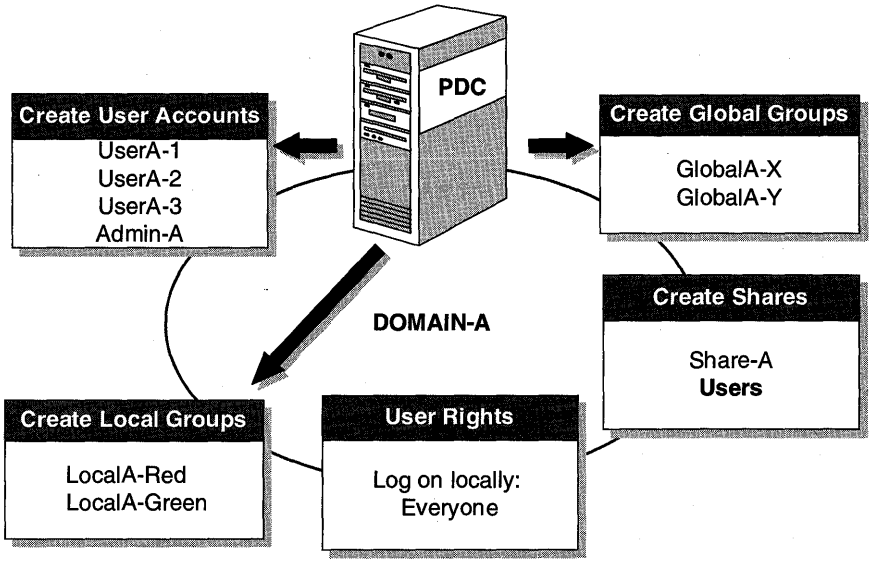


Figure 30: Create share USERS

Note Complete this procedure logged on as Administrator of DOMAIN-A.

1. Start File Manager, and then select the \USERS\DEFAULT directory on the PDC-A drive.
2. From the Disk menu, choose Share As.

   The Shared Directory dialog box appears.
3. Choose New Share.

   The New Share dialog box appears.
4. In the Share Name box, type **users**, and then choose Permissions.

   The Access Through Share Permissions dialog box appears.
5. Complete the share by removing the special group Everyone, and then adding the local group Users with Full Control permissions.
6. Choose OK twice to return to File Manager.

▶ To assign a home directory

Note Complete this procedure logged on as Administrator of DOMAIN-A.

1. Start User Manager for Domains, and then select the following users: UserA-1, UserA-2, and UserA-3.
2. From the User menu, choose Properties.

   The User Properties dialog box appears with all three users in the Users box.
3. Choose Profile.

   The User Environment Profile dialog box appears.
4. Under Home Directory, assign the home directories using the following information:
   - Select Connect.
   - Assign drive H:
   - In the To box, type **\\PDC-A\users\%username%**
5. Choose OK twice to complete the update.
6. Select UserA-1, and then from the User menu, choose Properties.

   The User Properties dialog box appears.
7. Choose Profile.

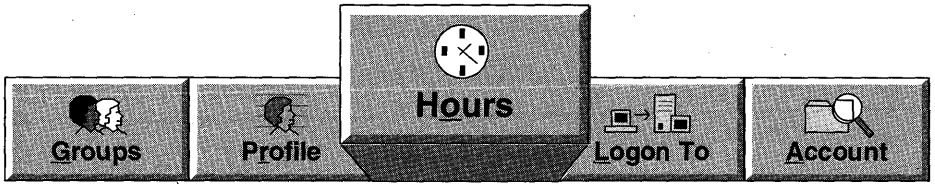
   The User Environment Profile dialog box appears.
8. What is the path to UserA-1's home directory?

9. Close the User Environment Profile and User Properties dialog boxes.
10. Switch to File Manager, and view \USERS\DEFAULT.

    Notice the new directories created named UserA-1, UserA-2, and UserA-3. They were created as a result of assigning the home directory path of %username%.
11. Exit File Manager.

Logon Hours

The Logon Hours option configures any restrictions to the days and hours during which a user can log on to the domain and connect to the server. The default allows for all hours of all days of the week, but you can optionally restrict a user to certain days and hours. This does not affect a user's ability to use a workstation account.



To change the logon hours, from the User Manager for Domains Account Properties dialog box, choose the Hours button.

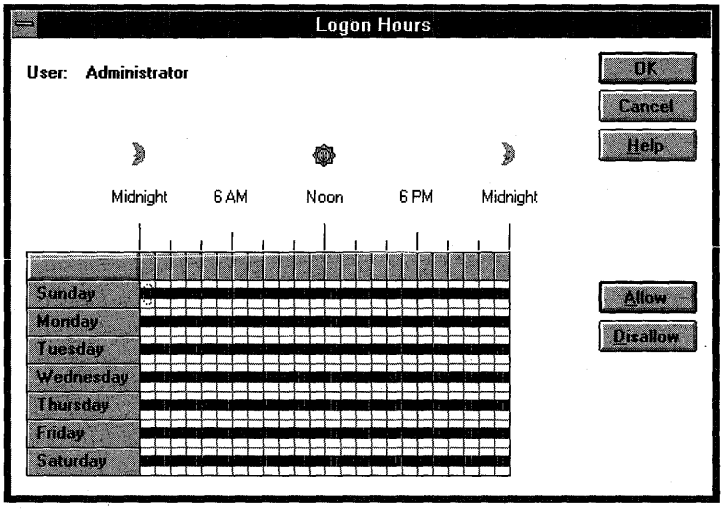


Figure 31: Logon Hours dialog box

The blue bars in the dialog box indicate the hours when logon is permitted. During the hours that logon is *not* permitted, the graph is empty.

To restrict a user's ability to log on during certain hours, use the mouse to select the hours when the user is *not* permitted to log on. With the hours selected, choose Disallow. The blue bar is removed from the selected hours.

To reenable logon during the disallowed period, select the appropriate time span, and then choose Allow. The blue bar is added for those hours.

► To restrict user logon hours

In this procedure, you restrict the logon hours so that UserA-2 cannot log on between 8:00 A.M. and midnight.

Note Complete this procedure logged on as Administrator of DOMAIN-A.

1. From User Manager for Domains, select UserA-2, and then from the User menu, choose Properties.
2. Choose Hours.

   The Logon Hours dialog box appears.
3. Select the time period from Sunday through Saturday, 8:00 A.M. through Midnight.
4. Choose Disallow.

   Notice that the boxes for Sunday through Saturday, 8:00 A.M. through Midnight are now clear.
5. Choose OK to return to the User Properties dialog box.
6. Choose OK to return to User Manager for Domains.

► To test the ability of the user account to log on

1. Log off as Administrator, and then attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log on as Administrator.

► To clear the logon hours restriction for your user

1. In User Manager for Domains, select UserA-2.
2. From the User Menu, choose Properties.
3. In the User Properties dialog box, choose Hours.

   The Logon Hours dialog box appears.
4. Select Sunday through Saturday, 8:00 A.M. through Midnight.
5. Choose Allow.

   Notice that the boxes for Sunday through Saturday, 8:00 A.M. through Midnight now have a colored bar through them.
6. Choose OK to return to the User Properties dialog box.
7. Choose OK to return to the User Manager dialog box.

► **To test the ability of the user account to log on at the PDC**

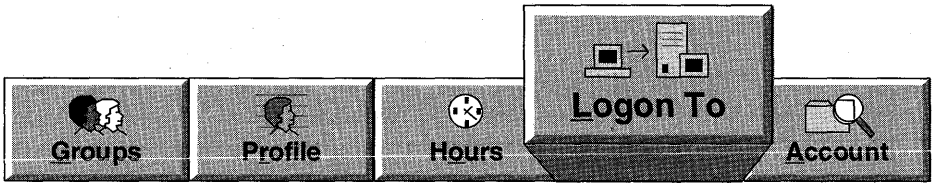
1. Log off as administrator, and then log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Start File Manager.
4. What is the default directory?

5. Exit File Manager, and then log off as UserA-2.
6. Log on as Administrator, and then start User Manager for Domains.

Logon To

Windows NT Server allows you to restrict the workstations from which users can log on to domain accounts. The default is to allow a user to log on from any workstation.



To configure the logon workstations, from the User Manager for Domains User Properties dialog box, you would choose the Logon To button.

► **To restrict logon workstations**

In this procedure, you restrict the computers to which UserA-2 can log on so that the primary domain controller is not included.

1. In User Manager for Domains, select UserA-2.
2. From the User menu, choose Properties.
3. From the User Properties dialog box, choose Logon To.

The Logon Workstations dialog box appears.

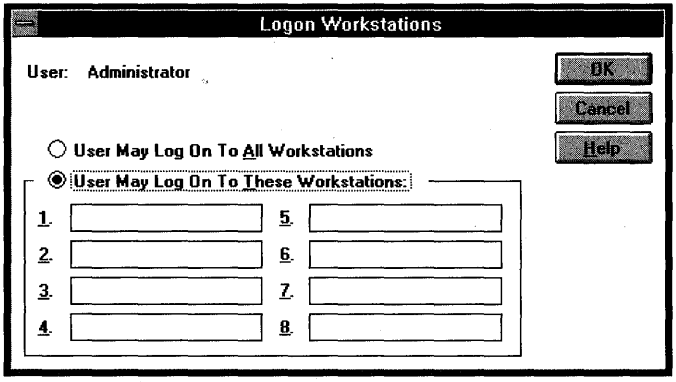


Figure 32: Workstations that allow you to log on

4. Select User May Log On To These Workstations.
5. In the 1. box, type **BDC-A**, and then choose OK.

Note For this procedure, it does not matter what computer name you supply here (except PDC-A). You simply want to restrict UserA-2 from logging on to PDC-A.

---

6. Choose OK to update UserA-2, and then exit User Manager for Domains.

► **To test the ability of the user account to log on at PDC**

1. Log off as Administrator, and then attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log on as Administrator, and then start User Manager for Domains.

► **To clear the workstation restrictions**

In this procedure, you restore UserA-2's ability to log on at any workstation.

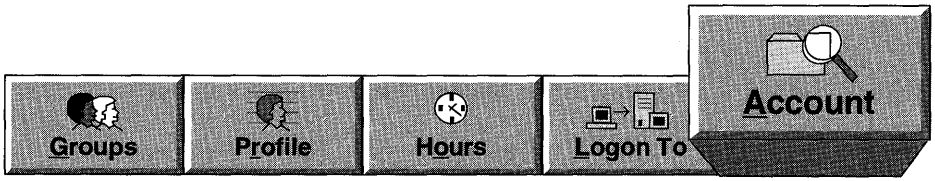
1. From User Manager for Domains, access the User Properties for UserA-2.
2. Choose Logon To to access the Logon Workstations dialog box.
3. Select User May Log On To All Workstations, and then choose OK.
4. Choose OK to update the properties of UserA-2.

5. Log off as Administrator, and then attempt to log on as UserA-2.
6. Were you able to log on? Why or why not?

7. Log off as UserA-2, and then log on as Administrator.

Account

If you have users who need only temporary access to the domain, you can set their accounts to expire after a certain date. The Account option is used to define an account expiration date (if any) and to specify the account type for the selected user accounts.



To change the account expiration date, from the User Manager for Domains User Properties dialog box, choose the Account button.

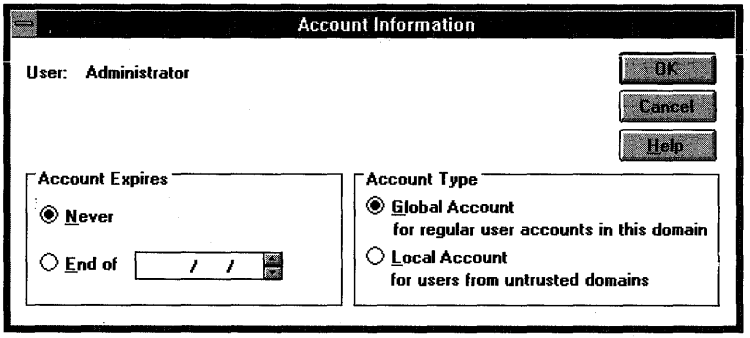


Figure 33: Setting an account expiration date

When an account has an expiration date, the account is disabled at the end of that day. Expired accounts are not deleted, merely disabled. When an account expires, a user who is logged on remains logged on but cannot establish new network connections or log on again after logging off.

► **To set the expiration date**

In this procedure, you set an expiration date for UserA-2 of yesterday.

1. In User Manager for Domains, access the User Properties for UserA-2.
2. In the User Properties dialog box, choose Account.
   The Account Information dialog box appears.
3. Under Account Expires, select End of.
   Notice that the default expiration date is approximately one month from today.
4. In the End of box, set the date to yesterday.
5. Choose OK to return to the User Properties dialog box.
6. Choose OK to update UserA-2's properties.
7. Exit User Manager for Domains, and then log off as Administrator.

► **To test the expiration date**

1. Attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log on as Administrator.

► **To clear the expiration date**

In this procedure, you clear the account expiration date for UserA-2.

1. From User Manager for Domains, access the User Properties for UserA-2.
2. In the User Properties dialog box, choose Account.
   The Account Information dialog box appears.
3. Under Account Expires, select Never.
4. Choose OK to return to the User Properties dialog box.
5. Choose OK to update UserA-2's properties.
6. Exit User Manager for Domains, and then log off as Administrator.

► **To test the expiration date**

1. Attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log off as UserA-2, and then log on as Administrator.

Specifying Account Type

In addition to specifying an account expiration date, the Account button allows you to designate the type of account: either a *global account* or a *local account*. Global accounts, the default setting for new accounts, are accounts that can be managed for the entire domain.

Local accounts are accounts that can be used to allow access to users from other domains that do not have a trust relationship with the local domain. This account is also useful for users with accounts in LAN Manager domains. No trust relationship can be established with a LAN Manager domain, so to permit access to users from the LAN Manager domain, you would create a local account for the LAN Manager user. However, the local account cannot be used to log on to Windows NT computers in the local domain; it can be used only for over-the-network access to local resources.

► **To create a local account**

In this procedure, you designate UserA-2 as a Local Account, thus restricting it from logging on at Windows NT computers in the domain.

1. In User Manager for Domains, access the User Properties for UserA-2.
2. In the User Properties dialog box, choose Account.

   The Account Information dialog box appears.
3. Under Account Type, select Local Account.
4. Choose OK to return to the User Properties dialog box.
5. Choose OK to update UserA-2's properties.
6. Exit User Manager for Domains, and then log off as Administrator.

► **To test the local account**

1. Attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log on as Administrator.

► **To create a global account**

You set the account type to Global Account for UserA-2.

1. In User Manager for Domains, access the User Properties for UserA-2.
2. In the User Properties dialog box, choose Account.

   The Account Information dialog box appears.
3. Under Account Type, select Global Account.

4. Choose OK to return to the User Properties dialog box.
5. Choose OK to update UserA-2's properties.
6. Exit User Manager for Domains, and then log off as Administrator.

► **To test the global account**

1. Attempt to log on as UserA-2.
2. Were you able to log on? Why or why not?

3. Log off as UserA-2, and then log on as Administrator.

Using a Low-Speed Connection

When administering accounts over a RAS or a low-speed network connection, the Low Speed Connection option (in the User Manager for Domains Options menu) should be selected. The Low Speed Connection option optimizes remote administration across slow-speed links by not displaying the following information and options:

- User list
- Group list
- Select Users option
- View menu options

User Manager for Domains saves the low-speed connection settings for future sessions.

Lesson Summary

There are many variables that can be configured to adjust a user's environment. Options such as configuring a user's home directory path and specifying logon hours, workstations, and account expiration dates are all possible using User Manager for Domains.

For more information on	See
Configuring user properties	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Configuring Home Directories	User Manager for Domains Help, Manage User Accounts, Creating a New User Account, Managing Profiles
Configuring Logon Hours	User Manager for Domains Help, Manage User Accounts, Managing Logon Hours
Configuring Logon Workstations	User Manager for Domains Help, Manage User Accounts, Managing Logon Workstations
Configuring Account Expiration and Type	User Manager for Domains Help, Manage User Accounts, Managing Account Information

Lesson 2: Profiles

User Manager for Domains is used to perform interactive changes to the user environment. If you want to configure the user environment for a group of users without changing each user individually, you can configure profiles instead. Profiles are used to configure and maintain a user's logon environment. In this lesson, you learn about what a profile can contain and how to configure it.

After this lesson you will be able to:

- Define profile.
- List the types of profiles.
- Use the profile editor to configure a user's logon environment.
- Distinguish between personal and mandatory server-based profiles, and know when to use each type.

Estimated Completion Time: 40 minutes

Profile Contents

User profiles are files that contain settings for a single user or a group of users. These settings determine the user's environment when the user logs on to the computer.

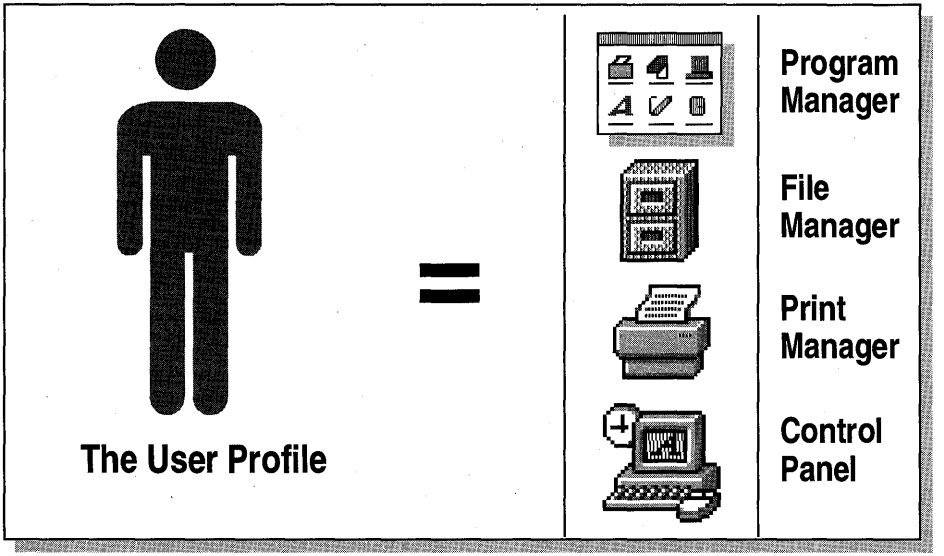


Figure 34: User profile information

The following table lists what is saved in the profile.

Source	Parameters saved
Program Manager	All user-definable settings for Program Manager, including personal program groups and their properties, and all settings saved by the Save Settings On Exit and Save Settings Now commands.
File Manager	All user-definable settings for File Manager, including network connections, and everything saved by the Save Settings On Exit command.
Command Prompt	All user-definable settings for the command prompt, including fonts, colors, settings for the screen size buffer, and window position.
Print Manager	Network printer connections and all settings saved by the Save Settings On Exit command.
Control Panel options	All settings for the Color, Mouse, Desktop Cursor, Keyboard, International, and Sound options. For the System option, only the entries in the User Environment Variables box. The other Control Panel options do not contain user-specific settings.
Accessories	All user-specific application settings affecting the user's Windows NT environment. These accessory applications include Calculator, Calendar, Cardfile, Clock, Notepad, Paintbrush™, and Terminal.
Third-party Windows NT–based applications	Any applications written specifically for Windows NT can be designed so that they track application settings on a per-user basis. If this information exists, it is saved in the user profile.
Help bookmarks	Any bookmarks placed in the Windows NT Help system.

Types of Profiles

There are four types of profiles:

Profile	Description
System default	Configures the display (colors and wallpaper) until a user logs on to the local computer.
User default	The default desktop configuration used the first time each user logs on to the computer. It is then copied to a local profile for the user.
Local	A profile stored locally and named after the user who is logged on to the computer. It is copied from the user default profile when the user logs on for the first time.
Server-based	A profile created by using the Profile Editor and stored on the server to control the user's desktop configuration at the workstation.

Note System default, user default, and local profiles are covered in the *Support Fundamentals for Microsoft Windows NT 3.5 Self-Paced Training* book.

User Profile Editor

The User Profile Editor can configure a user's logon environment so that there is a consistent, manageable set of network connections and program items.

A user profile stores configuration information on a user-by-user basis for each Windows NT computer. The saved information includes such things as the desktop arrangement, personal program groups and the program items in those groups, screen colors, screen savers, network connections, printer connections, mouse settings, and windows size and position.

As administrator, you can use the User Profile Editor, located in the Administrative Tools group of Program Manager, to preconfigure the logon environment so that it provides Windows NT Workstation or Windows NT Server users with a consistent, manageable set of network connections and program items.

With User Profiles, you can define:

- Program Manager groups.
- Program items and properties in those groups.
- Which programs will run from the File menu in Program Manager.
- Printer connections.
- Window size and positioning.
- Screen colors.
- Users' network connections.
- Available applications.
- The desktop appearance.

You can also set such environment variables as:

- The workstation's search path.
- Directory for temporary files.

It might be advantageous for you to structure a network environment for the user. This might be necessary if security requires complete or partial control, or if the users are not familiar enough with computers and networks to be able to use the technology on their own.

Profiles can ensure that several accounts will each have the same user environment. This can be done by either controlling the default environment or by locking the environment specifics. You can use profiles to create secure environments for a variety of jobs, and then assign the profile to users who fit that job description. For example, all bank tellers might have a profile called TELLERS.MAN.

To ensure consistency over time, you can use profiles to prevent a user from changing the desktop appearance.

► To test a local profile

In this procedure, you test the use of a local profile on Windows NT. These results will be contrasted with server-based profiles (discussed in the next section).

1. Log off as Administrator, and then log on as UserA-1.
2. Configure the local environment as follows:
   a. Tile the Main and Accessories windows
   b. Change the color schemes to Bordeaux
   c. Change the desktop wallpaper to Tile ZIGZAG.BMP
   d. Connect drive L: to \\PDC-A\Share-A
3. Log off, and then back on as UserA-1.
4. Were all the configuration changes you made restored?

5. Log off as UserA-1, and then log on as Administrator.

► To remove a local profile

In this procedure, you remove the local profile for UserA-1.

1. Start Windows NT Setup.
2. From the Options menu, choose Delete User Profiles.
3. The Delete User Profiles dialog box appears.
4. Under User Profiles on PDC-A, select DOMAIN-A\UserA-1, and then choose Delete.
5. Choose Close, and then exit Windows NT Setup.
6. Log off as Administrator.

► **To test logging on without a local profile**

In this procedure, you verify that the local profile for UserA-1 has been deleted.

1. Log on as UserA-1.
2. Were all the configuration changes you made earlier restored?

3. Configure the local environment as follows:
   a. Tile the Main and Accessories windows
   b. Change the desktop color to Bordeaux
   c. Change the desktop wallpaper to Tile ZIGZAG.BMP
   d. Connect drive L: to \\PDC-A\Share-A

4. Log off, and then log on as UserA-1 to verify that the configuration was restored properly.
5. Log off as UserA-1, and then log on as Administrator.

Server-Based Profiles

Server-based profiles are either personal profiles customized for individual users or mandatory profiles (used in structured or high-security environments) for single or multiple users.

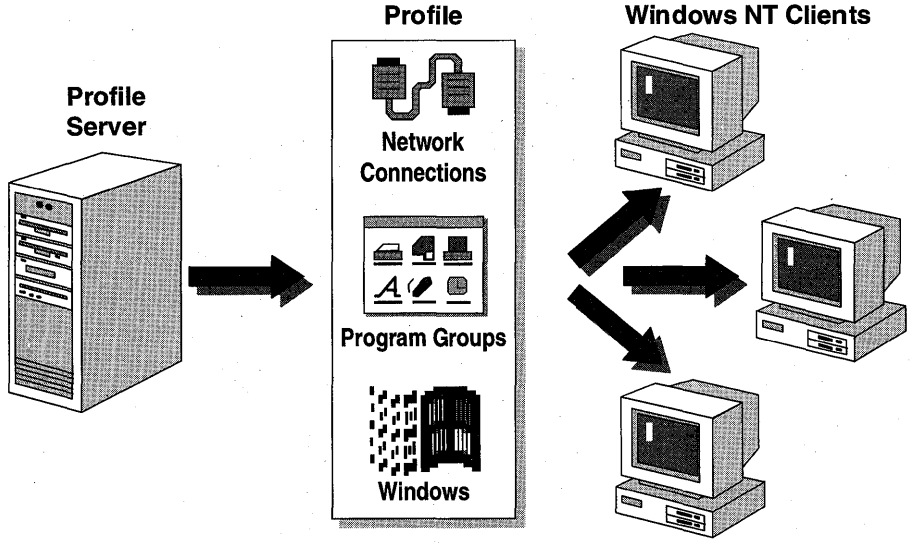


Figure 35: Use of server-based profiles

The fact that Windows NT computers can use server-based profiles has three important implications for network administration:

- The location of the server-based profile is specified in the domain's user accounts database for each account. The user will have the same user profile, no matter which Windows NT computer the user logs on to and no matter which Windows NT Server computer validates the logon. In other words, the user profile follows the user.
- You can create a user profile to restrict or structure the user's access to the workstation and prevent the user from changing the workstation's environment.
- The mandatory profile can be assigned to any number of users. This means that, by changing one profile, you can change several users' access to applications and environment.

Types of Server-Based Profiles

There are two types of server-based profiles—personal (.USR) and mandatory (.MAN). A user can have either a mandatory or a personal profile, but not both.

You assign both types of profiles to a user by specifying the location and filename of the profile in the user's account. A user account can have only one profile assigned to the account at a time.

These profiles must be stored on a server so that each user's settings and preferences follow the user, no matter which Windows NT computer is used for logon. If a user gets a new computer (for example, in the case of an upgrade), a personal profile restores the user's profile intact on the new computer. Each user has his or her own profile.

Personal Profiles

Users can change their personal profiles. Every time the user logs off, the profile is updated for current settings. When the same user logs on again, the profile is loaded as it was last saved. Because users can modify the contents of a personal profile, it is recommended that each personal profile be assigned to only one user. If more than one user is assigned to a personal profile, the personal profile settings are always set to the configuration of the last user using the personal profile.

A personal profile is indicated by the filename extension .USR.

Mandatory Profiles

Users cannot change a mandatory profile. Any environment changes made by users during a session are not saved to their mandatory profile. When a user logs off and logs on again, the environment the user created while working is gone and the original environment is restored.

Mandatory profiles are useful to administrators who want to restrict the ability of users to change their environments.

The mandatory profile is indicated by the filename extension .MAN.

Since changes are not saved to mandatory profiles, you can create a single mandatory profile and assign it to many users. By simply updating the single user profile, you can update many users at once. For instance, to add a new program to the users' environment, simply add it to the mandatory profile for those users.

Creating User Profiles

User profiles are created using the following tools:

- The User Profile Editor (creates the profile)
- User Manager for Domains (assigns existing profiles to users)

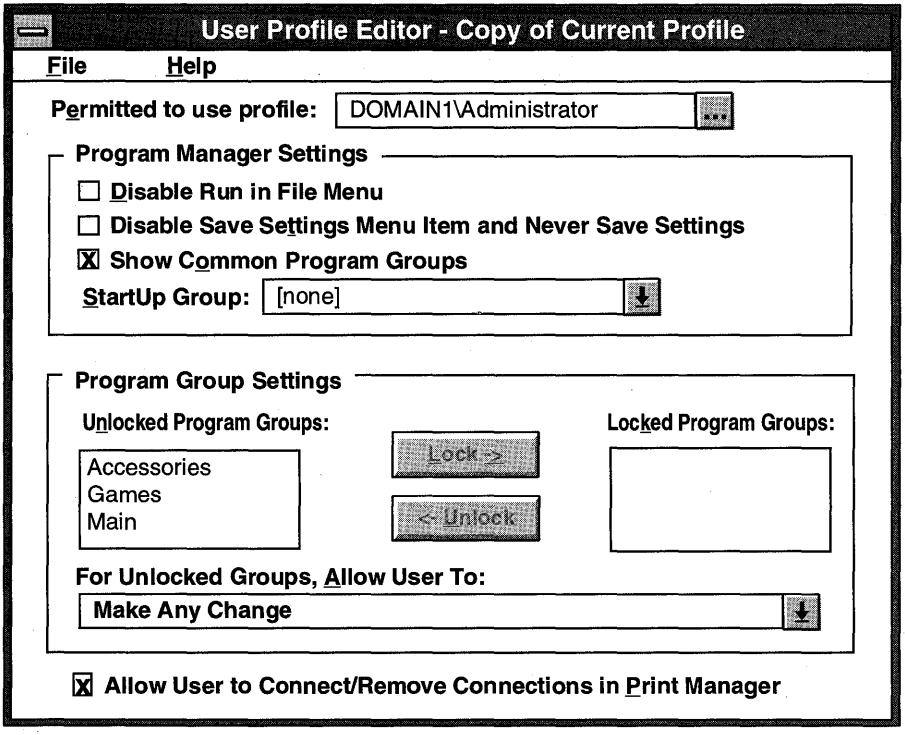


Figure 36: User Profile Editor dialog box

Note Management must be performed from a computer running Windows NT Server.

The first step in creating a user profile is to log on as a user with administrative privileges. It is recommended that you use a different administrative account from the Administrator to create a user profile: When you create a user profile, a copy of the existing environment settings is saved as the user profile for that computer; and you do not want the account that is used for normal network administration to be limited to the profile settings.

► To create a mandatory user profile

In this procedure, you create a mandatory profile and assign it to UserA-1 and UserA-2.

Note Complete this procedure logged on as Administrator of DOMAIN-A.

---

1. Configure the workstation environment for the profile as indicated below.
   - Tile the Main and Games program groups.
   - Connect drive N: to \\PDC-A\Netlogon.
   - Change the desktop color to Arizona.
   - Change the desktop wallpaper to tile Marble.
2. From the Administrative Tools group, start User Profile Editor.

   User Profile Editor appears.
3. Configure the profile settings using the following information:
   - Switch to Program Manager, close the Administrative Tools program group, and then switch back to User Profile Editor.
   - Select Disable Run in File Menu.
   - Lock the Administrative Tools program group.
4. From the Permitted to Use Profile box, choose the ellipse button to browse for a different user.

   The User Browser dialog box appears. It is used to select the appropriate user or group that is permitted to use this profile.
5. Under Names, select Users, and then choose Add.
6. Choose OK to return to User Profile Editor.

   Notice that DOMAIN-A\Users has been granted permission to use the profile.
7. From the File menu, choose Save As File.

   The Save As dialog box appears.
8. In the File Name box, type **users.man**
9. In the Directory box, select \<*winnt_root*>\SYSTEM32\REPL\IMPORT\SCRIPTS, and then choose OK.

10. From the File Menu, choose Exit.
11. Start User Manager for Domains, and then select UserA-1 and UserA-2.
12. From the User menu, choose Properties.

    The User Properties dialog box appears, displaying both user account names in the Users box.
13. Choose Profile to access the User Environment Profile dialog box.
14. In the User Profile Path, type **\\PDC-A\NETLOGON\USERS.MAN**, and then choose OK.
15. Choose OK to update the user profile path for the selected users.
16. Exit User Manager, and then log off as Admin-A.

► To test the mandatory user profile

In this procedure, you test the mandatory profile by logging on as UserA-1 to verify that the settings designated in the profile were implemented.

1. Log on as UserA-1.

   UserA-1 is logged on, and the user environment is configured.

   Verify that the correct profile (server-based vs. local user) was loaded by answering the following questions:
2. Is the desktop scheme what you set for UserA-1 (Bordeaux)?
3. Is the wallpaper a tiled ZIGZAG?
4. Is drive L: connected to \\PDC-A\Share-A?
5. Can you perform a File Run command from Program Manager?
6. Open the Administrative Tools group, and attempt to add a new Program Item.
7. Were you successful?
8. Which profile is loaded, local user or server-based mandatory?
9. Close the Games program group.

10. Log off as UserA-1, and then log back on as UserA-1.
11. Did the Games group remain minimized?

12. Log off as UserA-1.

    In this procedure, you verified that if a user has both a local profile and a server-based profile, the server-based profile is loaded (if available) and used in place of the local user profile.

Lesson Summary

Profiles help maintain a consistent user environment. Different users can log on to the same computer and have their own normal user environment. Server-based profiles allow users to log on to any Windows NT computer in the domain and still have their normal user environment. There are two types of server-based profiles—personal and mandatory. Personal profiles are assigned to individual users and can be modified by the user. Mandatory profiles can be assigned to multiple users, but cannot be modified by the users.

For more information on	See
Types of profiles	Chapter 4, "Managing User Environments," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
Creating profiles	Chapter 4, "Managing User Environments," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
	Chapter 14, "User Profile Editor," in the *Microsoft Windows NT Server System Guide.*
Assigning profiles to users	Chapter 14, "User Profile Editor," in the *Microsoft Windows NT Server System Guide.*
	Chapter 13, "User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Types of profiles	User Profile Editor Help, About User Profiles, Mandatory and Personal User Profiles and Default Profiles
Creating profiles	User Profile Editor Help, Manage User Profiles, Creating a New User Profile
Assigning a profile to a user	User Profile Editor Help, Manage User Profiles, Assigning User Profiles to User Accounts User Manager for Domains Help, Manage User Accounts, Managing Profiles

Lesson 3: Logon Scripts

While user profiles do offer you a lot of flexibility in assigning and controlling a user's environment, there are times when logon scripts must be used. This lesson introduces logon scripts, why to use them, how to create them, and how to implement them in a domain environment.

After this lesson you will be able to:

- Describe the differences between user profiles and logon scripts.
- Create a logon script to connect network resources at logon.
- Assign the logon script to users.

Estimated Completion Time: 30 minutes

What Are Logon Scripts?

Logon scripts have two main functions:

- To provide users with a set of consistent network connections
- To start applications automatically whenever a user logs on to the domain

Logon scripts are normally implemented as batch files. Net commands are used to maintain the network connections. The appropriate command line syntax is used to start an application. However, an executable file can be used as the user logon script if the result you want is to automatically start the executable file without maintaining the consistent set of network resource connections.

Logon Scripts vs. User Profiles

While user profiles can do everything a logon script can do, and more, they are available only to domain users who log on at a Windows NT computer. If your network consists of non–Windows NT computers, such as Windows for Workgroups, Microsoft Network Client, or LAN Manager client computers, users do not have access to the user profile features of Windows NT. For these environments, logon scripts can be used to offer some control over the user's environment.

A comparison between user profiles and logon scripts is shown in the following table.

User Profiles	Logon Scripts
Can control all facets of a user's environment (such as desktop arrangement and usage), including network connections and startup applications.	Can control network connections and start applications. Cannot control desktop arrangement or usage.
Local, default, personal, and mandatory profiles offer different levels of control to the user and/or administrator.	Usually a batch file for network connections.
Available only for users on Windows NT computers.	Available to all network clients that perform logon validation, including Windows NT computers.
Need a special tool (User Profile Editor) to create and manage.	You can use a standard text editor to create. You must know and understand command line syntax for net commands.
Available only in Windows NT.	LAN Manager, Novell NetWare, and other operating systems offer logon scripts. You can use LAN Manager logon scripts with Windows NT.

A logon script is typically a batch file that runs every time a user logs on. The logon script can be used to configure a user's working environment at each logon by making network connections and starting applications. For example, you might want each user to run a specific application every time the user logs on. For instance, this application could be a virus scan program that is located centrally on a network application server.

Logon scripts can also allow you to control parts of a user's environment without having to manage the complete environment. A logon script does not affect the user's desktop configuration, but it can affect the network resources available to the user, as well as startup applications.

For example, when creating a server-based user profile, you are configuring the user's desktop settings as well as network connections. If the server-based profile is saved as a personal profile, it allows the user to change the profile, but requires that a profile be created for each user. If the profile is mandatory, a separate profile is not required for each user, but the profile cannot be changed. This means that the user environment remains as determined by the administrator.

Using Logon Scripts

Logon scripts are optional and can be assigned to one or more user accounts. A single logon script can be created and assigned to an individual user or a group of users in a department, or it can be implemented network-wide. A logon script is typically a batch file (with a .BAT or .CMD filename extension), but any executable program (.EXE filename extension) can be used.

Logon scripts are assigned to a user by means of the User Environment Profile dialog box.

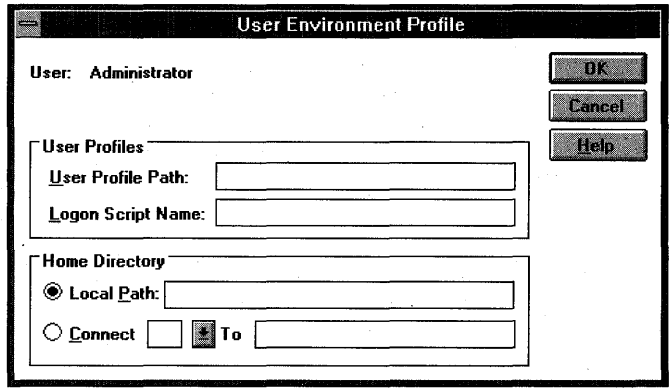


Figure 37: User Environment Profile dialog box

In the Logon Script Name box, you specify the logon script filename. By default, the file is stored in \<*winnt_root*>\SYSTEM32\REPL\IMPORTS\SCRIPTS. However, you can specify a location under the above path by including the relative path name in the filename. If you decide to change the entire path of the logon script, you can configure the logon script path in the Directory Replicator dialog box of Server Manager in the domain controller.

When the user logs on, the server authenticating the logon locates the script that is assigned to the user. The server that authenticates the user's logon must have a copy of the logon script. The authenticating server will not execute a script that resides on a different computer. The easiest way to maintain logon scripts on all domain controllers is by implementing the Directory Replicator service. When the validating server has located the local script, the script automatically executes.

A logon script can contain the following information:

- Any command line version of the **net** command. Most commonly used is **net use *d*: *server**share*** to connect the user automatically to the specified share.
- Any command line syntax to start an application, such as *drive:\path\appname*. For example, to start the MS-DOS version Anti-Virus program automatically, you might have a C:\DOS\MSAV C: command in the logon script.

- Environment variables—These variables are set only during the execution of the logon script. After the script has completed, the environment is returned to the settings in CONFIG.SYS and AUTOEXEC.BAT.
- Special Logon Script Variables as listed in the following table:

Parameter	Description
%HOMEDRIVE%	The drive letter connected to the user's home directory
%HOMEPATH%	The full path to the user's home directory
%HOMESHARE%	The sharename containing the user's home directory
%OS%	The operating system running at the user's computer
%PROCESSOR%	The processor type of the user's computer
%USERDOMAIN%	The domain name that contains the user's account
%USERNAME%	The name of the user's account

► To assign a user logon script

In this procedure, you assign a logon script to user accounts.

Note Complete this procedure logged on as Administrator of DOMAIN-A.

1. Insert the *Lesson Disk* into drive A, and then copy NETLOGON.BAT and DAILY.TXT to \<*winnt_root*>\SYSTEM32\REPL\IMPORT\SCRIPTS.
2. Start User Manager for Domains, and then select UserA-1 and UserA-2.
3. From the User menu, choose Properties to access the User Properties dialog box for all selected users.
4. Choose Profile to access the User Environment Profile dialog box.
5. In the Logon Script Name box, type **netlogon**, and then choose OK.
6. In the User Properties dialog box, choose OK to update the user environment profile of each selected user.
7. Exit User Manager for Domains, and then log off as Administrator.

   You now have a logon script that copies a file from the PDC, starts Notepad, and loads the copied file into Notepad.

► **To test the user logon script**

In this procedure, you log on as UserA-1 to test the logon script.

1. Log on as UserA-1.

   The server-based profile loads first, and then the logon script is executed.

   When the logon script has copied a file from the primary domain controller, it starts Notepad with the DAILY.TXT file loaded.
2. Exit Notepad.
3. Is the desktop environment as configured in the user profile?

4. Start File Manager, and open a window for drive H (home directory).
5. Is the file DAILY.TXT in UserA-1's home directory?

6. Log off as UserA-1, and then log on as Administrator.

Lesson Summary

User logon scripts can be used to configure a user's environment, providing a consistent set of network resource connections at every logon. Logon scripts are available not only to Windows NT computers, but also to MS-DOS-based computers running Windows for Workgroups, LAN Manager, and Microsoft Network Client software.

For more information on	See
Logon scripts vs. user profiles	Chapter 4, "Managing User Environments," in the Microsoft Windows NT Server Concepts and Planning Guide.
How logon scripts work	Chapter 4, "Managing User Environments," in the Microsoft Windows NT Server Concepts and Planning Guide.
Creating logon scripts	Chapter 4, "Managing User Environments," in the Microsoft Windows NT Server Concepts and Planning Guide.
Assigning logon scripts to users	Chapter 13, "User Manager for Domains," in the Microsoft Windows NT Server System Guide.

For online information about	From the Help menu, choose Contents and then
Creating logon scripts	User Manager for Domains Help, Manage User Accounts, Managing Profiles

CHAPTER 4

Configuring the Server Environment

Before You Begin

This chapter requires that you have completed Chapter 1, "Installing Microsoft Windows NT Server 3.5," Chapter 2, "Using Groups to Manage Users," and Chapter 3, "Configuring the User Environment." All of the procedures in this chapter initially require at least one Windows NT Server functioning as a primary domain controller.

During the procedures, you will install a backup domain controller.

In the procedures that require the use of two computers, the Windows NT Server computers are identified by their roles—primary domain controller (PDC) or backup domain controller (BDC).

To complete the procedures, you need your Configuration Table.

Lesson 1: Server Management

To keep a network functioning properly, server management tools are provided with Windows NT Server. Server Manager is one of these tools.

Server Manager can be used to verify that the domain is functionally operational by synchronizing the primary domain controller with all the backup domain controllers, replicating logon scripts and user profiles among all the domain controllers, controlling resources and users on a server, and configuring server properties.

This lesson explains some of the functions of Server Manager and how you can use it to manage the domain, a server, server resources, and users.

After this lesson you will be able to:

- List the functions of Server Manager.
- Configure server properties.
- Manage user sessions.
- Manage resources.

Estimated Completion Time: 60 minutes

Server Manager

Server Manager is a tool that you use to administer computers and domains in a Microsoft Windows NT Server environment. You administer local or remote domains by selecting the domain from the Server Manager window. You must be a member of the Administrators group, in the domain you select, to use Server Manager to manage that domain.

Server Manager is located in the Administrative Tools group of Program Manager. You use the Select Domain option, from the Computer menu, to view the domain computers in Server Manager.

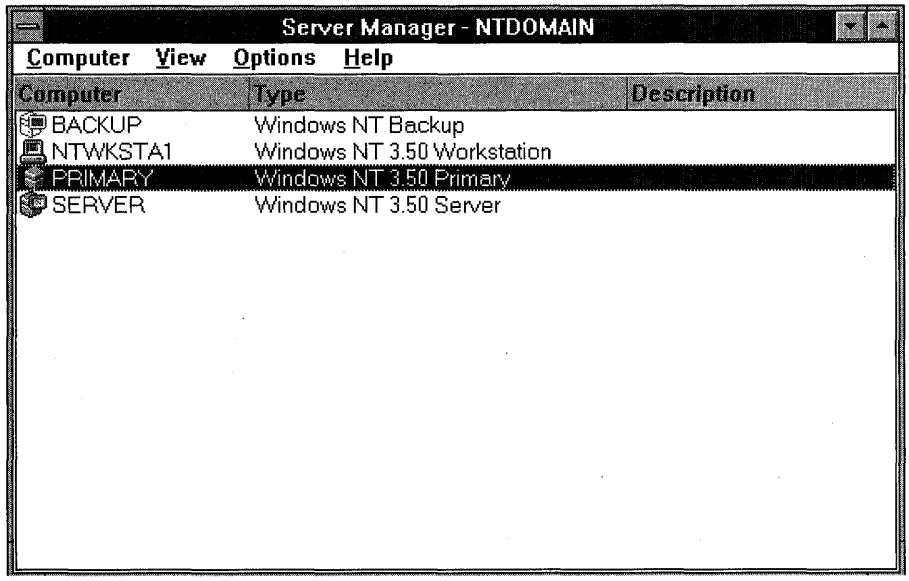


Figure 38: Server Manager

Important Do not confuse the Server application in Control Panel with Server Manager. The Server application in Control Panel can manage properties only for the local computer. Server Manager can manage properties for both local and remote computers. Server Manager also has enhanced capabilities, such as the ability to add computers to the domain, synchronize, promote, and demote domain controllers, and so on.

Server Manager allows you to manage both local and remote computers and domains. Server Manager can be used to do the following tasks in both Windows NT and in Microsoft LAN Manager 2.*x* domains:

- Display the computers of a domain
- Manage server properties and services for a selected computer
- Add computers to and remove computers from the domain
- Promote a backup domain controller to a primary domain controller
- Synchronize backup domain controllers with the primary domain controller
- Manage shared resources (directories, printers, and so on)
- Send messages to connected users

Note For more information on other functions of Server Manager see Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide*.

Server Manager Interface

You can configure the information displayed by Server Manager to your requirements. You can specify the domain and computers that you want to monitor (servers only, or servers and workstations).

The icons displayed by Server Manager represent the different computer members of the domain.

Represents a primary domain controller (PDC).

Represents backup domain controllers and servers.

Represents Windows NT Workstation computers that have joined the domain.

Important Icons for computers that are members of the domain but are currently inactive on the network are dimmed.

Server Manager also displays the following information for a selected computer:

- The computer name
- The operating system name and version number for the computer
- A description (configured by the user)
- Whether the computer is a domain controller, a server, or a workstation
- Whether it is currently active on the network

Before using menus and options in Server Manager, you must first select the name of the computer you want to work with. After the computer is selected, the menu, option, or action you select applies to that computer.

Sending Messages to Connected Users

Sometimes you might want to send a message to all users connected to a particular computer. For instance, you should let users know when one or more users are going to be disconnected from a resource, whether the Server service is being stopped, or when any other action occurs that otherwise disrupts network service.

To send a message to all users connected to a computer, from the Computer menu you select Send Message. You can then create a message and send it to all connected users.

The Messenger service must be running to send messages. It is started by default in Windows NT Server.

Note To send a message to an individual user, you can use the **net send** *username message* command.

► **To send a message to all connected users**

In this procedure, you establish a network connection to your own computer, and then use Server Manager to send a message.

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A.

1. Use File Manager to connect to \\PDC-A\Users.
2. From the Administrative Tools group, start Server Manager.

   Server Manager appears.
3. From the Computer menu, choose Send Message.

   The Send Message dialog box appears.
4. Under Message, type a short message, and then choose OK.

   A Messenger Service message box appears, displaying the message.
5. Choose OK to clear the message.

Managing Server Properties and Services

Server Manager can be used to configure server properties. To view the server properties for a computer, from the Computer menu, choose Properties.

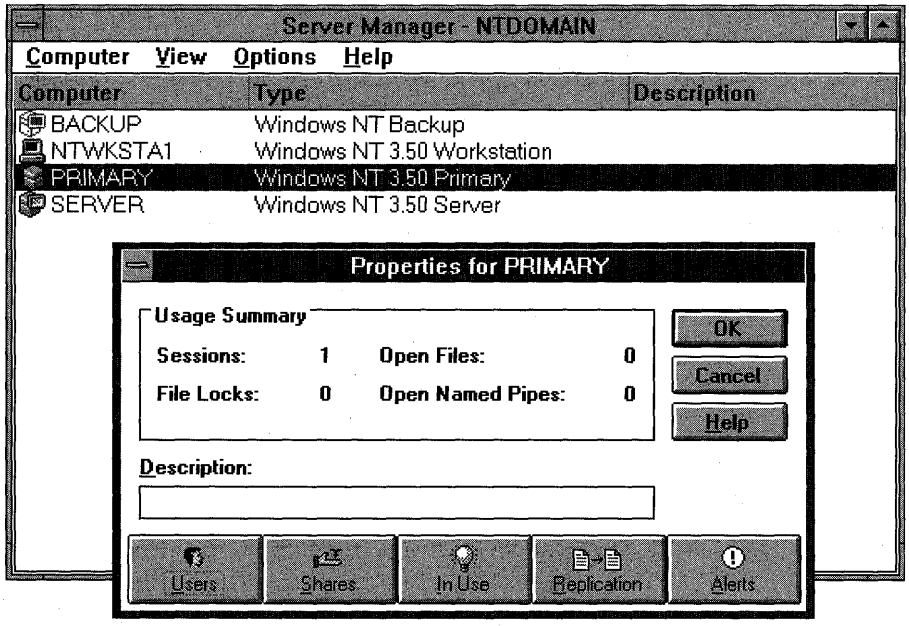


Figure 39: Server properties

The Properties dialog box displays the usage information, a description of the selected computer, and additional buttons for managing the following:

- Users—Provides information on user connections
- Shares—Provides shared resource information
- In Use—Provides information on resources that are currently in use
- Replication—Provides information on replicated directories
- Alerts—Provides information on users and computers targeted for administrative alerts

► To display properties

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A.

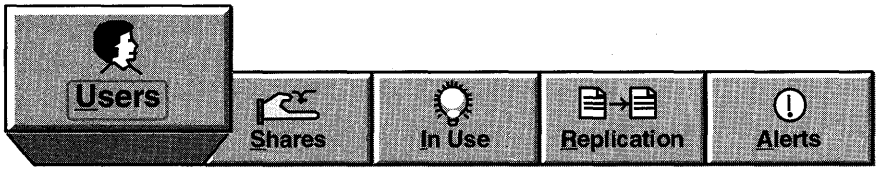
1. From the Server Manager window, select PDC-A.
2. From the Computer menu, choose Properties.

   The Properties dialog box for PDC-A appears with the following information:

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

Managing User Sessions

To view detailed information about user sessions, from the Properties dialog box, choose Users.



Viewing user sessions can be a great help in monitoring network usage of the computer.

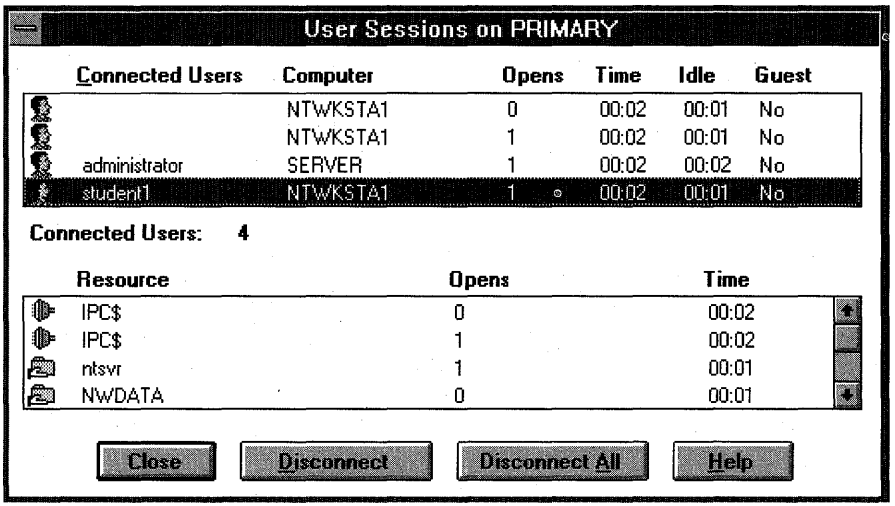


Figure 40: Viewing user sessions

In the User Sessions dialog box, you can view:

- All the users connected over the network to the computer. This can be beneficial in planning the capacity for your servers and the network as a whole.
- The resources opened by each user. This is useful in determining the usage of a resource.
- The total time and the amount of inactivity of the session. This information is useful to determine whether users are connecting to resources but are not disconnecting when finished using the resources, thus wasting server resources.
- Whether any users without accounts in the local domain are connecting to server resources. This can help in determining whether additional accounts should be created, whether a trust relationship is needed, and even whether there are security problems.

Disconnecting Users

You might want to disconnect users before you stop the Server service or shut down the computer for maintenance.

You can disconnect a user by selecting the user and choosing Disconnect. All the users connected to a server can be disconnected by pressing Disconnect All.

Important You should warn users before disconnecting them. Also, administrators must remember that this is a "passive" disconnection; users and applications can reconnect by using the connection. To prevent users from reconnecting, you need to pause or stop the server service.

Connected Users

The Connected Users box lists the users connected to the computer. You select a user, any shared resources the selected user is connected to are displayed in the Resource box.

The information displayed in this dialog box includes the items listed in the following table.

Item	Meaning
Connected Users	The user name of a connected user
Computer	The name of the computer where the user is logged on
Opens	The number of resources the user opened on this computer
Time	The time elapsed since this session was established
Idle	The time elapsed since the user last accessed the resource
Guest	Whether this user has guest status on the computer

Resources

When you select a user, the connections of that user are listed in the Resources box.

Resource	The name of the shared resource (shared directory, printer, or named pipe) to which the selected user is connected
Opens	The number of opens by this user against this resource
Time	The time elapsed since this resource was first opened

► To disconnect a user

In this procedure, you disconnect yourself from the shared resource Users.

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A. You should still have the connection to \\PDC-A\Users established.

---

1. If you have not already done so, from Server Manager select PDC-A.
2. From the Computer menu, choose Properties.

3. In the Properties for PDC-A dialog box, choose Users.

   The User Sessions on PDC-A dialog box appears.

4. Under Connected Users, select administrator.

   Under Resource, notice the connection to the USERS share.

5. Choose Disconnect.

   A Server Manager message box appears, asking whether you are sure you want to disconnect administrator from all connected resources.

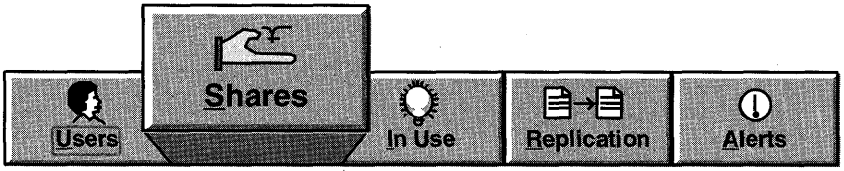
6. Choose Yes.

   The User Sessions on PDC-A dialog box appears. Notice that the session for administrator is no longer listed.

   Choose Close to return to the Properties for PDC-A dialog box.

Managing Shared Resources

To access the Shared Resources dialog box, from the Properties dialog box, choose Shares.



The Shared Resources dialog box appears, displaying the following information:

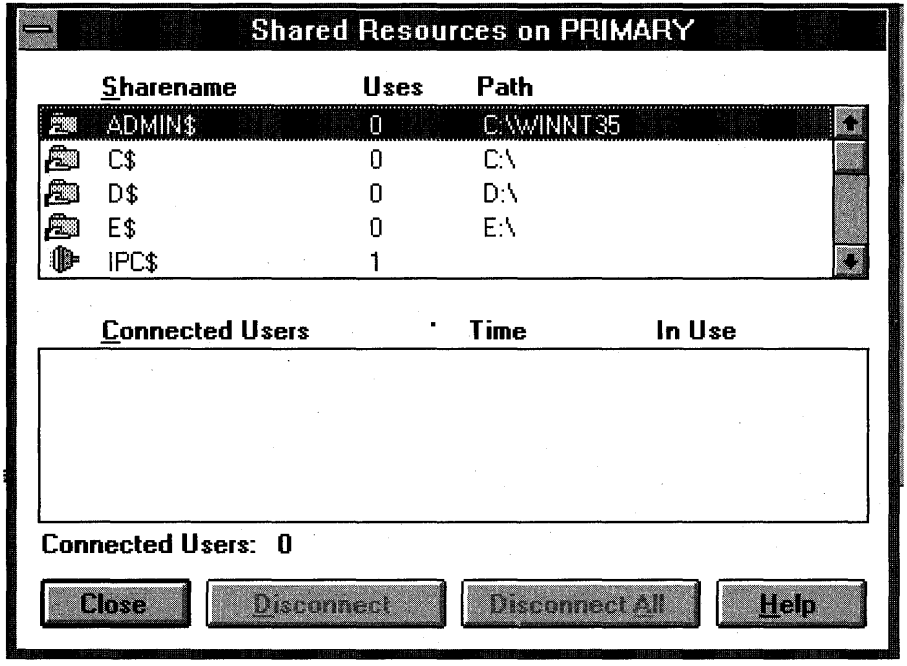


Figure 41: Viewing shared resources

The following information can be obtained from the Shared Resources dialog box.

Item	Description
Sharename	The name of the shared resource. This could be a shared directory, a printer, or a named pipe.
Users	The number of users connected to the shared resource
Path	The path of the shared resource
Connected Users	The user name of the user(s) connected to the selected shared resource
Time	The time elapsed since the user first connected to this resource
In Use	Whether the user currently has any files open from this shared resource

You can use this dialog box to disconnect one or all of the connected users from all shared resources on this computer. This might be appropriate, if you need to let another user connect to a shared directory that already has its maximum number of users connected. It would also be appropriate if users turned off their computers without either logging off or disconnecting network resource connections.

Always remember to warn users if they are going to be disconnected.

Note To create additional shared resources or to remove existing shared resources, you can use the Shared Directories command from Server Manager, or use File Manager. To share printers or manage shared printers, use Print Manager.

► To disconnect a user

In this procedure, you disconnect yourself from the shared resource Users.

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A.

---

1. If you have not already done so, from Server Manager select PDC-A.
2. From the Computer menu, choose Properties.
3. In the Properties for PDC-A dialog box, choose Shares.

   The Shared Resources on PDC-A dialog box appears.
4. Under Sharename, select USERS.

   Under Connected Users, notice that no connections currently exist.

Important If you had accessed the \\PDC-A\Users share after disconnecting it earlier, it would appear as a session again.

---

5. Close the Shared Resources dialog box.
6. Switch to File Manager and access the drive connected to \\PDC-A\Users.

   This reestablishes the session that was disconnected in the previous procedure.
7. Switch back to Server Manager, and in the Properties for PDC-A dialog box, choose Shares.
8. Under Sharename select USERS.

   Under Connected Users notice that administrator is now listed.
9. Choose Disconnect.

   A Server Manager message box appears, asking whether you are sure you want to disconnect administrator from all connected resources.
10. Choose Yes.

    The Shared Resources on PDC-A dialog box appears. Notice that the session for administrator is no longer listed.
11. Choose Close to return to the Properties for PDC-A dialog box.

Managing Resources in Use

To view more detail on the resources that are currently in use, from the Properties dialog box, choose In Use.

The Open Resources dialog box appears, displaying the following information:

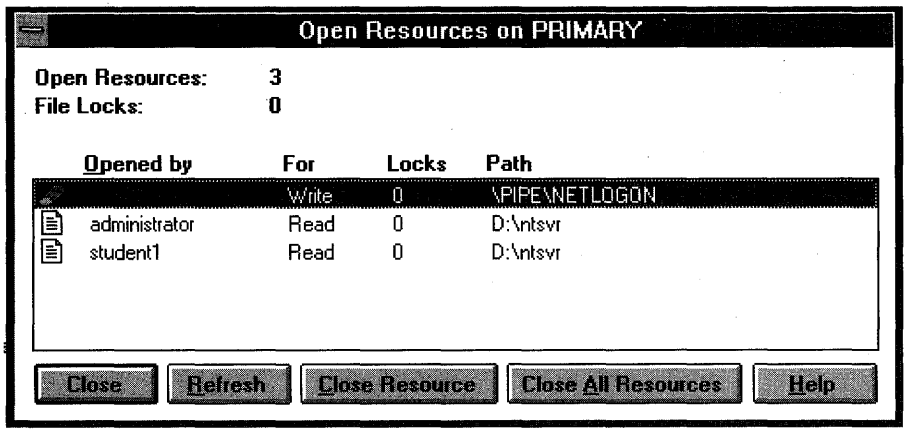


Figure 42: Viewing resources in use

The administrator can close one or all of the resources; however, the administrator should warn connected users before closing the resource.

The Open Resources dialog box offers the following options.

Item	Description
Open Resources	The total number of open resources (files, printers, or named pipes) on the computer
File Locks	The total number of file locks on open resources
Opened By	The user name of the user who opened the resource

(continued)

Item	Description
For	The permissions granted when the resource was opened
Locks	The number of locks on the resource by that user
Path	The path of the open resource

► To close an open resource

In this procedure, you open a resource and then close it.

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A.

1. Switch to File Manager and choose the drive icon assigned to \\PDC-A\Users, and then access the \USERA-1 directory.

   This reestablishes the session that was disconnected in the previous procedure.

2. Switch back to Server Manager, and in the Properties for PDC-A dialog box, choose In Use.

   The Open Resources on PDC-A dialog box appears, displaying all open resources on the computer, including open resources on \USERS\DEFAULT\USERA-1 opened for Read.

3. Choose Close All Resources.

   A Server Manager message box appears, informing you that some users have resources open for Read, and that closing them can result in data loss.

4. Choose Yes.

   The Open Resources on PDC-A dialog box appears. Notice that the open resource(s) are no longer listed.

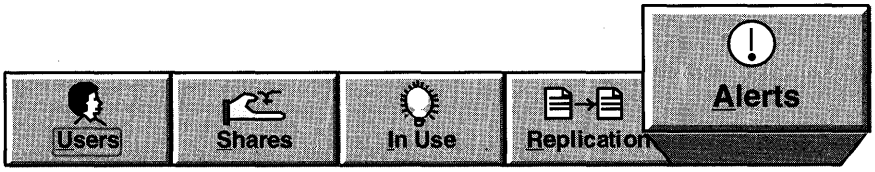
5. Choose Close to return to the Properties for PDC-A dialog box.

Alerts

Alerts are messages the system sends to inform the administrator that something is wrong with the system. For example, an alert might be sent when a hard disk partition is almost full, when the UPS service is notified by a UPS that power has been lost, or when the Directory Replicator service replicates files to another computer. Alerts notify the administrator that the network is experiencing problems with users accessing resources on a local computer.

You can configure the alerts to send them to various users.

To configure the appropriate computers and users to receive administrative alerts from the server, use the Alerts button from the Properties dialog box.



Note Replication is covered in Lesson 3.

The Alert dialog box appears, displaying the following information:

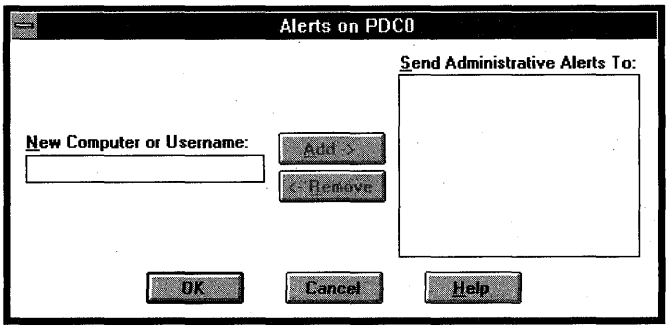


Figure 43: Configuring Alerts

In the Alerts dialog box, you enter a user name or computer name in the New Computer Username box, and Add it to the list of recipients under Send Administrative Alerts To. By doing so, when an administrative alert occurs, such as power loss from the UPS service, the recipients on the list receive the message so that appropriate action can be taken to correct the alert condition.

► To configure administrative alerts

In this procedure, you configure the administrative alerts to alert the Administrator and the primary domain controller computer in the event of an administrative alert condition. This will involve stopping and restarting both the Alerter and Server services.

Important Complete this procedure logged on as Administrator on the primary domain controller of DOMAIN-A. Start with Server Manager opened and the Properties for PDC-A dialog box displayed.

---

1. Choose Alerts.

   The Alerts on PDC-A dialog box appears.
2. In the New Computer or Username box type **administrator** and then choose Add.
3. In the New Computer or Username box type **pdc-a** and then choose Add.

   Under Send Administrative Alerts To, Administrator and PDC-A are added.
4. Choose OK to return to the Properties for PDC-A dialog box.
5. Choose OK to return to Server Manager.
6. From the Computer menu choose Services.

   The Services on PDC-A dialog box appears.
7. Under Service, select Alerter and then choose Stop.

   A Server Manager message box appears, asking whether you are sure you want to stop the Alerter service.
8. Choose Yes.
9. Choose Start to restart the Alerter service.
10. Under Service, select Server and then choose Stop.

    A Stopping message box appears, indicating that the Computer Browser and Net Logon services will also be stopped.
11. Choose OK.

    A Server Manager message box appears, indicating that Server Manager cannot find the Primary Domain Controller for Domain-A.
12. Choose OK.

    Notice that Server Manager no longer lists your computer. You have to restart the services using Control Panel Services.
13. Start the Control Panel Services option.

    The Services dialog box appears.
14. Under Service, select Server and then choose Start.

15. Under Service, select Net Logon and then choose Start.
16. Under Service, select Computer Browser and then choose Start.
17. Choose Close, and then close Control Panel.
18. Switch to Server Manager.
19. Press the F5 key to refresh the Server Manager.

    Notice that your primary domain controller now appears in Server Manager.
20. Exit Server Manager.

► **To test administrative alerts**

Important This procedure requires that you have enough hard disk space to create another partition. If you do not have the necessary hard disk space, you can skip this procedure.

In this procedure, you will generate an administrative alert by creating a small hard disk partition and then using all available disk space in that partition.

Important If you are able to create a small hard disk partition (2 MB in size) on this computer, complete this procedure on the primary domain controller of DOMAIN-A.

---

1. Use Disk Administrator to create a 2 MB partition on any hard disk.
2. Format the partition using any of the available file systems.
3. Copy directories and files to the new partition to use all the disk space.

   After a few minutes, a Messenger Service message box appears, indicating that a drive is nearly full and how much disk space is available.
4. Choose OK to close the message.

If you are unable to create a new partition to test administrative alerts, you can still view an administrative alert later in Lesson 3.

Lesson Summary

Managing a domain in a Windows NT Server environment encompasses many tasks. These tasks can be categorized into computer tasks and domain tasks. Management of servers allows the administrator to control shared resources and user access to those resources, determine current file access, and control replication and administrative alerts.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to verify that all sessions on your server are being initiated by users with accounts in your domain. How can you make sure that this is the case?

2. You need to shut down the server for maintenance, and you want to make sure that all users have closed all open files on the server before shutting it down. How can you verify that it is safe to shut down the server?

For more information on	See
Using Server Manager to manage a computer	Chapter 15, "Server Manager," in the Microsoft Windows NT Server System Guide. Chapter 10, "Managing a Running Server," in the Microsoft Windows NT Server Network Operations Quick Reference.

For online information about	From the Help menu, choose Contents and then
Sending messages to users	Server Manager Help, Send a Message to Connected Users, Sending a Message to Connected Users
Managing user sessions	Server Manager Help, Manage Server Properties, Viewing User Sessions
Managing shared resources	Server Manager Help, Manage Server Properties, Viewing Shared Resources
Managing open resources	Server Manager Help, Manage Server Properties, Viewing Resources in Use
Managing alerts	Server Manager Help, Manage Server Properties, Managing Administrative Alerts

Lesson 2: Domain Management

This lesson explains the importance of domain synchronization and demonstrates how to use the features of Windows NT Server to configure and optimize the synchronization of the user account database within a domain.

After this lesson you will be able to:

- Add a computer to the domain.
- Install a backup domain controller.
- Configure the Net Logon Service.
- Synchronize domain controllers.
- Configure the account database synchronization speed.
- Promote a backup domain controller to be a primary domain controller.

Estimated Completion Time: 90 minutes

Adding and Removing Computers in a Domain

If you want a Windows NT Workstation or Server to participate in domain security, that computer must join the domain. If it is no longer necessary for a computer to participate in domain security, that computer can be removed from the domain.

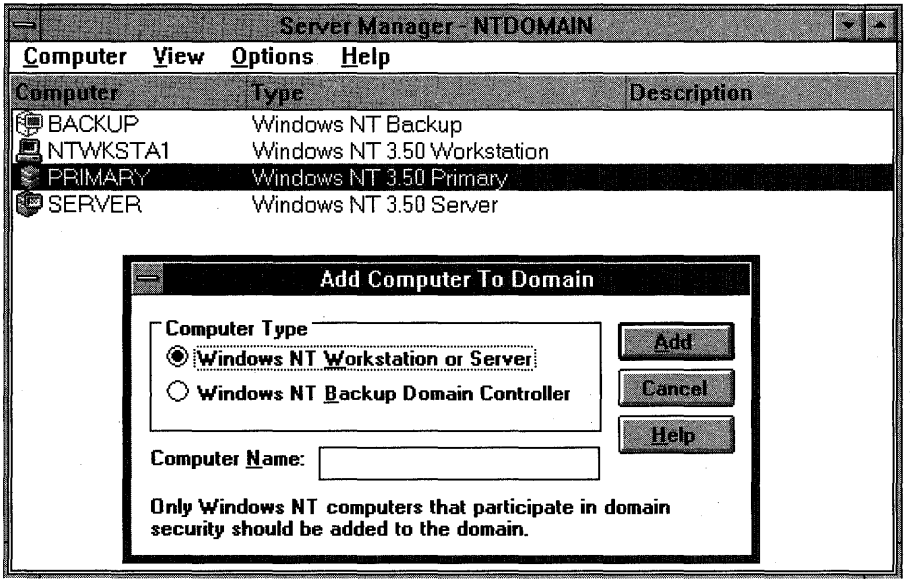


Figure 44: Adding a computer to a domain

To perform this task, you must be an administrator or have the Add Workstation to Domain user right.

► To add a computer account to the primary domain controller

In this procedure, you create a computer account for a backup domain controller in DOMAIN-A. To do this, you need the computer name of the BDC for DOMAIN-A. Refer to your Configuration Table for this information. In a later procedure, you will install the backup domain controller using the membership established in this procedure.

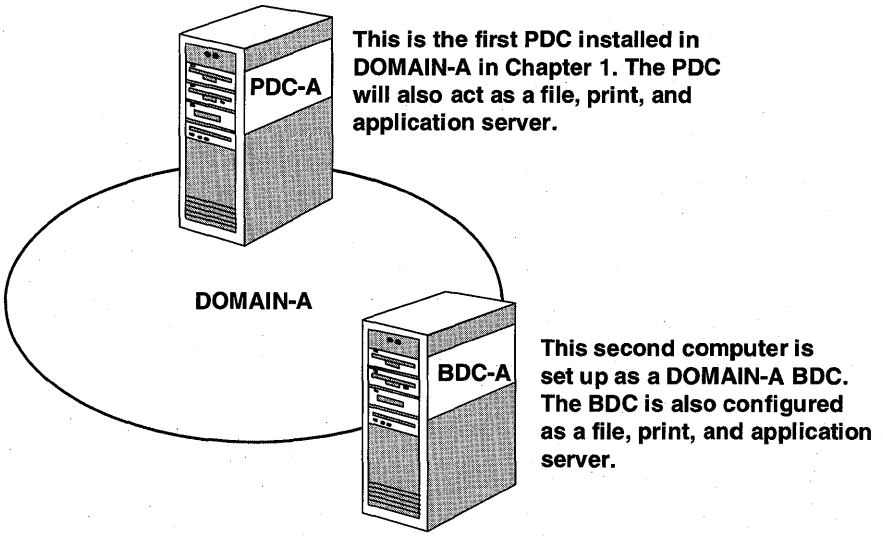


Figure 45: Creating a backup domain controller (BDC-A)

Important Complete this procedure logged on as Administrator at the primary domain controller of DOMAIN-A.

---

1. Start Server Manager.
2. From the Computer menu, choose Add to Domain.

   The Add Computer to Domain dialog box appears.
3. Under Computer Type, select Windows NT Backup Domain Controller.
4. In the Computer Name box, type **bdc-a**, and then choose Add.

5. Choose Close.

   Your Server Manager is updated with the name of the server.

6. What is the Type of the new computer account?

► To install a backup domain controller

In this procedure, you install a backup domain controller into DOMAIN-A. The installation of a BDC is very similar to that of a PDC.

Important Complete this procedure from the computer designated as a backup domain controller only. Do *not* use PDC-A. This computer should have a minimum of 210 MB free disk space. You need 90 MB to install the BDC. In later procedures, you install additional operating systems that require the additional space.

---

1. Install the backup domain controller. Refer to the Configuration Table when you are asked for system file location, computer name of the BDC in DOMAIN-A, network adapter card, network protocol(s), and domain name.

   Note For detailed steps on installing Windows NT Server, see Chapter 1, "Installing Windows NT Server," in the *Microsoft Windows NT Server Installation Guide.*

   ---

2. Log on to BDC-A as Administrator.

The Net Logon Service

Within a domain, the user account database is periodically copied from the PDC to each BDC. This allows all domain controllers to validate domain user logons.

The communication that occurs between domain controllers for user accounts database synchronization is managed by the Net Logon service. The Net Logon service is started by default after a Microsoft Windows NT Server installation. You can start or stop the Net Logon service using Server Manager or the Control Panel Services option.

The Net Logon service provides three major functions:

- Logon validation—When a user logs on to a Windows NT Server domain, the Net Logon service validates that the user has supplied a correct user name and password for the domain.
- Pass-through authentication—This occurs when a user account must be validated, but the account cannot be validated by the local computer or domain. In this case, the user name and password are forwarded to a Windows NT Server domain controller that can validate the user, and the user's information is returned to the requesting computer.

Important Each Windows NT computer participating in the domain must be running the Net Logon and Workstation services. Without these services, users cannot be validated and access shared resources.

- Synchronization of backup domain controllers with primary domain controllers—Keeps the domain's user accounts and security database synchronized between the primary domain controller and the backup domain controller(s).

Synchronizing Domain Controllers

User account database synchronization (replication) occurs when a PDC copies, or replicates, its user account database to the BDC(s) within the domain. A full synchronization occurs when the PDC sends its entire user account database to a BDC; a partial synchronization occurs when the PDC sends only the changes in its user account database.

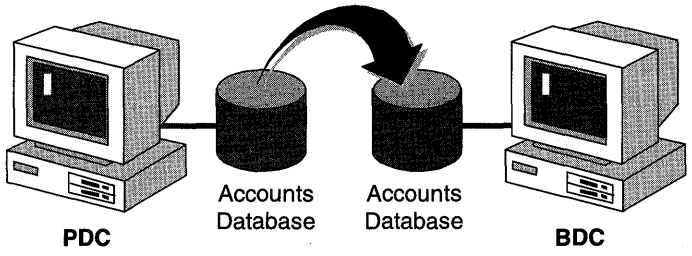


Figure 46: Account database synchronization between PDC and BDC

Synchronizing solves problems with password mismatches or outdated access tokens. You can synchronize in one of two ways using Server Manager:

- If you select any of the BDCs, you can synchronize the selected BDC's account database with the PDC.
- If you select the PDC, you will synchronize the domain's user account database from the PDC to all BDCs in the domain.

Synchronizing with the primary domain controller might be necessary when you are making changes to the user account database and are trying to test your implementation immediately. Any BDC can validate logons and supply account information, but if the changes you have made to the account database on the PDC have not been copied to the validating BDC by the time you run your test, your test will fail.

Synchronizing BDCs also solves problems related to password mismatches and access tokens that are created without the necessary group memberships. It can also help troubleshoot problems involving accessing a resource or performing a network task. Synchronizing the domain, logging out, and then logging back on again will build a new access token that contains updated information.

In the following procedure, you observe what might happen when a domain is not synchronized. You then synchronize the domain controllers in your domain.

▶ To prepare to test synchronization

In this step, you prepare to test synchronization by logging off the backup domain controller. This facilitates the logon process in a later procedure to be as quick as possible.

Important Complete this procedure from the backup domain controller of Domain-A.

- Log off the backup domain controller.

▶ To create a new domain user account

Next, you copy an existing user account to create a new user account in the domain's account database. This account is then used to test synchronization in the following procedure.

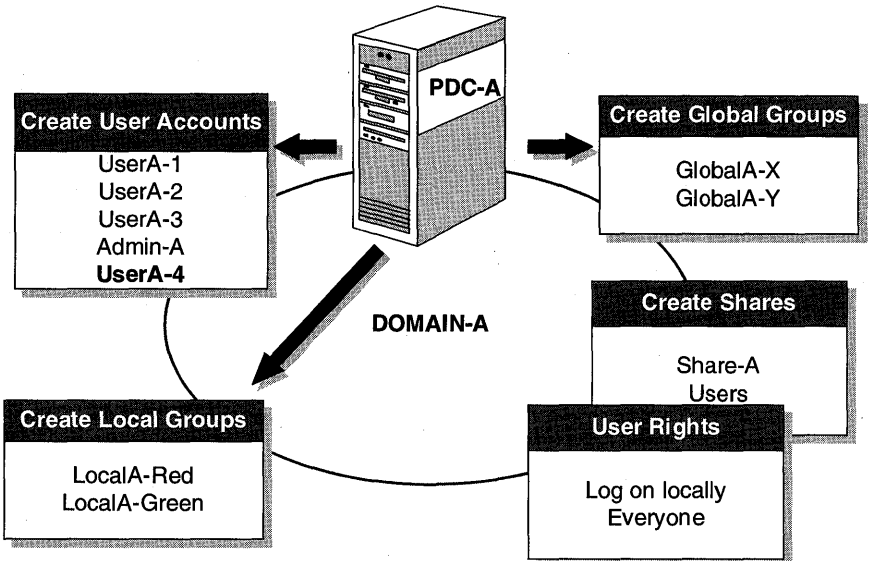


Figure 47: Create UserA-4

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. Using User Manager for Domains, create a new user named UserA-4 by copying UserA-1. Do not require this user to change password at next logon.
2. Proceed immediately to the next procedure.

► To verify that the domain is out of sync

Here you attempt to log on as UserA-4, to determine whether domain account database synchronization has occurred.

Important Complete this procedure from the backup domain controller of Domain-A.

---

1. Attempt to log on as UserA-4.
2. Were you able to log on? Why or why not?

► To synchronize the domain

Next, you force synchronization of the domain's account database between the PDC and the BDC.

Important Complete this procedure logged on as Administrator from the primary domain controller of Domain-A.

---

1. From Server Manager, select your Primary Domain Controller.
2. From the Computer menu, choose Synchronize Entire Domain.

   The Server Manager message box appears, indicating that the synchronization might take a few minutes.
3. Choose Yes.

   A Server Manager message box appears, informing you that the PDC asked the BDCs to synchronize and that you should check the Event Log on the BDC to verify that it was successful.
4. Choose OK.
5. Wait one minute, and then proceed.

► To verify that the domain is synchronized

Finally, you verify that synchronization has occurred by logging on as UserA-4, which you were unsuccessful in doing earlier. If you are successful now, the user account has been replicated to the backup domain controller, and the domain controllers are synchronized.

Important Complete this procedure from the backup domain controller of Domain-A.

---

1. Attempt to log on as UserA-4.
2. Were you able to log on? Why or why not?

3. Log off as UserA-4, and then log on as Administrator.

► **To verify synchronization using the Event Log**

For additional verification, you view the Event Log to see the events recorded as a result of domain synchronization.

Important Complete this procedure logged on as Administrator at both domain controllers of Domain-A.

---

1. Start Event Viewer.
2. Verify that the System Log appears. If it does not, from the Log menu choose System.

   The System Event Log appears.
3. From the View menu, choose Filter Events.

   The Filter dialog box appears.
4. In the Source box, select NetLogon and then choose OK.

   The System Log appears, displaying only NetLogon events.
5. From the View menu, choose Detail.
6. Read the event details, choosing Next, until you find confirmation of synchronization.
7. Close Event Viewer.

Domain Synchronization Over a Slow WAN Link

Windows NT Server has a new parameter that can be used to increase performance of replication across slow links. It is called the ReplicationGovernor.

A BDC uses the ReplicationGovernor Registry value to increase the performance of domain synchronization over a slow WAN link.

Important The ReplicationGovernor parameter is supported on only Windows NT Server 3.5.

The ReplicationGovernor defines both the size of the data transferred on each call to the PDC and the frequency of those calls. Adjusting the ReplicationGovernor parameter works in two ways. First, it reduces the size of the buffer used on each call from the BDC to the PDC, ensuring that a single call does not occupy the WAN link for too long a time. Second, it causes NetLogon essentially to "sleep" between calls, allowing other applications to access the WAN link between calls to the PDC.

The ReplicationGovernor parameter can be added to the Registry of a BDC under the following key:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon
\Parameters
```

To add this parameter, assign a type of REG_DWORD and a value from zero to 100 (the default is 100). This value defines a percentage for both the amount of the data transferred on each call to the PDC and the frequency of those calls. For instance, setting the ReplicationGovernor value to 50 percent will use a 64 KB buffer rather than the default 128 KB buffer. In addition, the BDC will have an outstanding synchronization call on the net for only a maximum of 50 percent of the time.

Caution Care must be taken in setting this value: if the ReplicationGovernor is set too low, synchronization might never complete. A value of zero will cause NetLogon never to synchronize, and the user account database can become completely out of sync.

Important This parameter must be set individually on each BDC and should only be used when the PDC is a computer running Windows NT Server 3.5.

User Account Database Replication

If the domain controllers are all running Windows NT Server, a full synchronization of the user account database is not necessary when the account database of the domain changes. The reason for this is that the PDC keeps track of the synchronization level of each BDC, which allows the PDC to control the rate of partial synchronizations. The PDC sends a message announcing the change in the user account database only to the domain's BDCs that need the changes, instead of to all BDCs.

These messages are sent to a subset of your domain's domain controllers in each pulse (the subset is defined by the PulseConcurrency parameter), which prevents all the BDCs from responding simultaneously. This helps to reduce network traffic and also ensures that the PDC is not overloaded by having all the BDCs making synchronization requests simultaneously.

The following table describes the values that can be added to the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \Netlogon\Parameters Registry key to control synchronization.

Value name	Description
Pulse	The Pulse defines the pulse frequency, in seconds. All changes made to the user account database since the last pulse are collected together. Then, after the Pulse time has expired, a pulse is sent to each BDC needing the changes; however, no pulse is sent to a BDC that is up-to-date. Default value: 300 (5 minutes); Value range: 60 (1 minute)–3600 (1 hour)
PulseConcurrency	The PulseConcurrency defines the maximum number of simultaneous pulses the PDC will send to BDCs in the domain. The NetLogon service sends pulses to individual BDCs, which causes the BDCs to respond by requesting any database changes. To control the maximum load these responses place on the PDC, the PDC will have only the number of pulses specified under PulseConcurrency "pending" at one time. Increasing PulseConcurrency will increase the load on the PDC. Decreasing PulseConcurrency will increase the time it takes for a domain with a large number of BDCs to send a change to all of the BDCs. Default value: 20; value range: 1–500
PulseMaximum	This defines the maximum pulse frequency in seconds. Every BDC will be sent at least one pulse at this frequency, regardless of whether its user account database is up-to-date. Default value: 7200 (2 hours); value range: 60 (1 minute)–86400 (1 day)
PulseTimeout1	PulseTimeout1 defines how long, in seconds, the PDC will wait for a non-responsive BDC. When a BDC is sent a pulse, it must respond within this time period. If the BDC does not respond, it is considered to be non-responsive. A non-responsive BDC is not counted against the PulseConcurrency limit, thereby allowing the PDC to send a pulse to another BDC in the domain. If this number is too large, a domain with a large number of non-responsive BDCs will take a long time to complete a partial synchronization. If this number is too small, a slow BDC might be falsely accused of being non-responsive. When the BDC finally does respond it will receive a partial synchronization from the PDC, which can increase the load on the PDC. Default value: 5 (5 seconds); value range: 1 (1 second)–120 (2 minutes)

(continued)

Value name	Description
PulseTimeout2	PulseTimeout2 defines how long, in seconds, a PDC will wait for a BDC to complete partial synchronization. Even though a BDC initially responds to a pulse (as described for PulseTimeout1), it must continue making synchronization progress, or the BDC will be considered non-responsive. Each time the BDC calls the PDC, the BDC is given another PulseTimeout2 seconds to be considered responsive. If this number is too large, a slow BDC (or one that has its ReplicationGovernor rate artificially governed) will consume one of the PulseConcurrency slots. If this number is too small, the load on the PDC could be unduly increased because of the large number of BDCs doing a partial sync. Default value: 300 (5 minutes); value range: 60 (1 minute)–3600 (1 hour)
Randomize	Randomize specifies the BDC backoff period, in seconds. When the BDC receives a pulse, it will back off between zero and the Randomize seconds before calling the PDC. Randomize should always be smaller than the PulseTimeout1. Consider that the time to synchronize a change to all the BDCs in a domain will be greater than: ((Randomize/2)*NumberOfBdcsInDomain)/ PulseConcurrency Default value: 1 (1 second); value range: 0–120 (2 minutes)

Important The PulseTimeout2 parameter affects only cases in which a BDC cannot retrieve all the changes to the user account database in a single RPC call. This happens only if a large number of changes are made to the database before a synchronization.

Controlling the Rate of Automatic Synchronization

To change the speed of the synchronization process, you edit the Registry and change the value of the Pulse parameter on the primary domain controller. You then use Server Manager remotely to stop and restart the NetLogon service of the PDC for the change to take effect.

► To edit the pulse parameter in the Registry

In this procedure, you add the pulse parameter to the PDC to notify the BDC every minute there are account database changes.

Important Complete this procedure logged on as Administrator at the primary domain controller of Domain-A.

---

1. Start the Registry Editor (run REGEDT32.EXE).
2. Maximize the HKEY_LOCAL_MACHINE window.
3. Open the SYSTEM\CurrentControlSet\Services\Netlogon\Parameters folder.

   You will now add the Pulse parameter, overriding the default value of 300 seconds.
4. From the Edit Menu, choose Add Value.

   The Add Value dialog box appears.
5. In the Value Name box, type **pulse**
6. In the Data Type box, select REG_DWORD, and then choose OK.

   The DWORD Editor dialog box appears.
7. In the Radix box, select Decimal.
8. In the Data box, type **60** and then choose OK.

   The screen refreshes and the Pulse value appears in the Parameters folder using hexadecimal notation (0x3c).
9. Exit the Registry Editor.

► To administer remotely the NetLogon service of the PDC from the BDC

After the Registry has been updated, the appropriate service generally must be restarted for the change to take effect. In this case, the NetLogon services must be restarted. Now that you have a backup domain controller, the BDC can be used to control services of the PDC.

Important Complete this procedure logged on as Administrator at the backup domain controller of Domain-A.

---

1. Start Server Manager, and then select PDC-A.
2. From the Computer menu, choose Services.

   The Services on PDC-A dialog box appears.
3. Under Service, select NetLogon, and then choose Stop.

   A Server Manager message box appears, asking whether you are sure you want to stop the Net Logon service.

4. Choose Yes.

   The Service Control box appears while the NetLogon service is being stopped.

   When the NetLogon service has been stopped, you are returned to the Services on PDC-A dialog box.

5. With the NetLogon service selected, choose Start.

   The Service Control box appears while the NetLogon service is being started.

   When the NetLogon service has been started, you are returned to the Services on PDC-A dialog box.

6. Choose Close to return to Server Manager.
7. Exit Server Manager.

▶ To test the pulse parameter

In this procedure, you delete UserA-4 from the domain account database, and then wait to see how long it takes to update the BDC.

Important Complete this procedure logged on as Administrator at the backup domain controller of Domain-A.

---

1. Start User Manager for Domains, and then select UserA-4.
2. From the User menu, choose Delete.

   A User Manager for Domains message box appears, indicating that user accounts are associated with unique identifiers, and warning of the consequences of deleting the account.

3. Choose OK

   A User Manager for Domains message box appears, prompting for confirmation of the Delete request.

4. Choose Yes.

   UserA-4 has been removed from the user list for the domain.

5. Exit User Manager for Domains.
6. Start Event Viewer.

   There should be a recent event added with a Source of NetLogon, indicating the synchronization. If not, wait one minute and then refresh the list.

7. From the View menu, choose Detail.
8. What database was synchronized, and with how many updates?

9. Close the Event Details dialog box, and then exit Event Viewer.

Promoting a Backup Domain Controller to a Primary Domain Controller

There is only one primary domain controller (PDC) in a domain. It maintains the master copy of the domain's account and security database, which is automatically replicated to the backup domain controllers (BDCs) in the domain. The need can arise to promote a BDC to a PDC—for example, when the PDC must be shut down for routine maintenance. If the PDC is taken off the network without having had a BDC promoted to take its place, no user account or security policy changes can be implemented, although users can continue to log on to the domain and be validated.

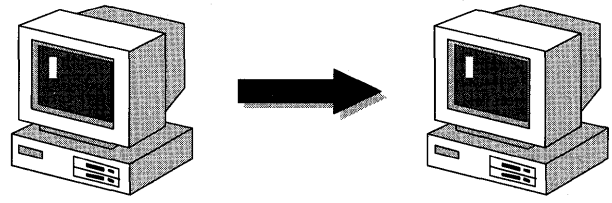


Figure 48: Promoting BDC to PDC

If the PDC is online, it is possible for it to swap roles with a BDC. Promoting a BDC to a PDC will demote the existing PDC to a BDC.

If the PDC is offline, a BDC can still be promoted to PDC, but any recent changes could be lost. When the original PDC is brought back online, one of the two PDCs will have to be demoted to a BDC.

You use Server Manager to promote the backup domain controller to the role of primary domain controller.

► To verify server information

In this procedure, you verify that the BDC and PDC are using the same set of domain members from Server Manager.

Important Complete this procedure logged on as Administrator on both computers.

1. Use Server Manager to complete the following information about the servers in your domain. The icon column refers to the type of icon, such as cube, cube with monitor, or workstation.

Icon	Computer	Type

2. Does this information match the information on the other domain controller in your domain? Why or why not?

► To promote a BDC to a PDC

In this procedure, you promote BDC-A to the role of primary domain controller for DOMAIN-A.

Important Complete this procedure from the primary domain controller (PDC-A) of Domain-A.

1. From Server Manager, select BDC-A.
2. From the Computer menu, choose Promote to Primary Domain Controller.

   A Server Manager message box appears.
3. What warning message appears?

4. How does this affect your network if you are remotely running Server Manager over a RAS connection?

5. Choose Yes to make the change.

   The Server Manager status box appears.
6. What actions are occurring during the promotion? Watch the messages in the status dialog box and record them below.

► To refresh a Server Manager window

Important Complete this procedure from the new primary domain controller (BDC-A) of Domain-A.

1. Press F5 to refresh the Server Manager window.
2. After the refresh, proceed to the next procedure.

► To verify server information

In this procedure, you verify that the BDC and the PDC are using the same set of domain members from Server Manager.

Important Complete this procedure logged on as Administrator on both computers of Domain-A.

1. Use Server Manager to complete the following information about the servers in your domain.

Icon	Computer	Type

2. Does this information match the information on the other controller in your domain? Why or why not?

3. How does this information compare to the information in the first procedure?

► To reverse the roles back to original

In this procedure, you return BDC-A to the role of backup domain controller for DOMAIN-A by promoting PDC-A back to primary domain controller. This is done to have consistency in the remaining procedures.

Important Complete this procedure logged on as Administrator from the primary domain controller (BDC-A) of Domain-A.

1. From Server Manager, select PDC-A.
2. From the Computer menu, choose Promote to Primary Domain Controller.

   A Server Manager message box appears, prompting for verification to complete the promotion and demotion.

3. Choose Yes.
4. Verify that the roles have changed by viewing the computer type in Server Manager.

► **To refresh a Server Manager window**

Important Complete this procedure logged on as Administrator from the new primary domain controller (PDC-A) of Domain-A.

5. Press F5 to refresh the Server Manager window.

Lesson Summary

Managing a domain requires you to make sure that all domain controllers are using precisely the same copy of the domain's user accounts database. This includes any computers added to or removed from the domain, as well as user account or security policy changes. Server Manager provides the capabilities to maintain the domain to ensure proper operation of all of the domain's controllers.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You have installed a domain with a single domain controller. After conferring with other network administrators, you realize that this is not the best policy and decide to add two backup domain controllers to the domain. How can this be accomplished now that the domain has already been created?

2. You have a domain that has a remote site connected over a slow link. What can you do to make sure that when domain synchronizations occur, the synchronization process does not use the entire bandwidth of the WAN link?

For more information on	See
Adding computers to domains	Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide.*
Synchronizing domain controllers	Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide.*
Promoting domain controllers	Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide.*
Using Event Viewer	Chapter 17, "Event Viewer," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Adding computers to a domain	Server Manager Help, Manage a Domain, Adding a Computer to the Domain
	Server Manager Help, Computer Menu Commands, Add to Domain
Synchronizing domain controllers	Server Manager Help, Manage a Domain, Synchronizing a Backup Domain Controller with the Primary Domain Controller, or Synchronizing all Servers of the Domain
	Server Manager Help, Computer Menu Commands, Synchronize with Primary Domain Controller, or Synchronize Entire Domain
Promoting domain controllers	Server Manager Help, Manage a Domain, Promoting a Backup Domain Controller to Primary Domain Controller, or Demoting a Primary Domain Controller to Backup Domain Controller
	Server Manager Help, Computer Menu Commands, Promote to Primary Domain Controller, or Demote to Backup Domain Controller
Using Event Viewer	Event Viewer Help, View Event Logs
	Event Viewer Help, View Menu Commands, Filter Events
	Event Viewer help, View Menu Commands, Detail

Lesson 3: Replication

When managing a domain, not only is it necessary to ensure that all domain controllers are using the same copy of the domain's user accounts database, but it is also important to make sure that any domain controller can provide the user with any configured logon scripts or server profiles. If the user accounts database has been synchronized throughout the domain, yet the logon scripts and/or server-based user profiles have not been copied to all domain controllers, users can be validated properly, but their desktop environment might not be as expected.

Server Manager can be used to manage the process of replicating information between computers on the network.

After this lesson you will be able to:

- Describe common uses for replication.
- Describe the components used in replication.
- Set up replication on an export server and import computer.
- Configure the export server.
- Configure the import computer.
- Adjust the timing of directory export notices.
- Manage various aspects of replication on an export server and import computer.

Estimated Completion Time: 60 minutes

Introduction to Replication

Directory replication is a Microsoft Windows NT Server feature that allows you to set up and automatically maintain identical directory trees on multiple servers and workstations. Updates made to the files or directories on one server are periodically copied, or replicated, to other servers and workstations.

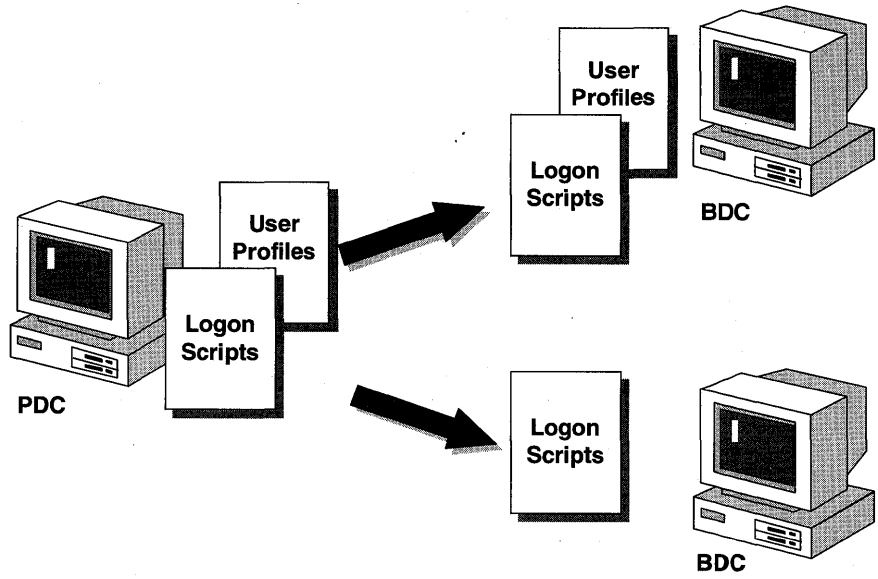


Figure 49: Examples of data replicated from PDC to BDCs

Replication is useful in a variety of situations. For example, if many users must periodically access a file, the computer storing the file could become overburdened. Replication can make the same file available at multiple servers for user access.

Replication is best used for read-only information. This is because any open file will not be replicated. Also, directories that receive copies of the files (*import directories*) are overwritten each time replication occurs. Any changes that users make to files in import directories will be lost during the next replication. For this reason, replication is recommended for files such as the following:

- Logon scripts—When there is more than one Windows NT Server controller in a domain, logon scripts should be replicated to all domain controllers. This allows each domain controller that participates in authenticating logons to have a copy of all user logon scripts. By using replication, only one copy of each script needs to be maintained.
- Mandatory user profiles—Mandatory user profiles can be replicated to all domain controllers. This allows a mandatory profile to be made available for a user no matter where that user logs on (a computer running Windows NT Workstation or Windows NT Server). By using replication, only one copy of the profile needs to be maintained.
- Distribution of read-only files—If many users need to access a file such as a phone list, replicate the file to several computers. Different groups of users should access the file from different computers to balance the load.

Replication Components

There are three main components used in replication. The export server, import computer, and export and import directories.

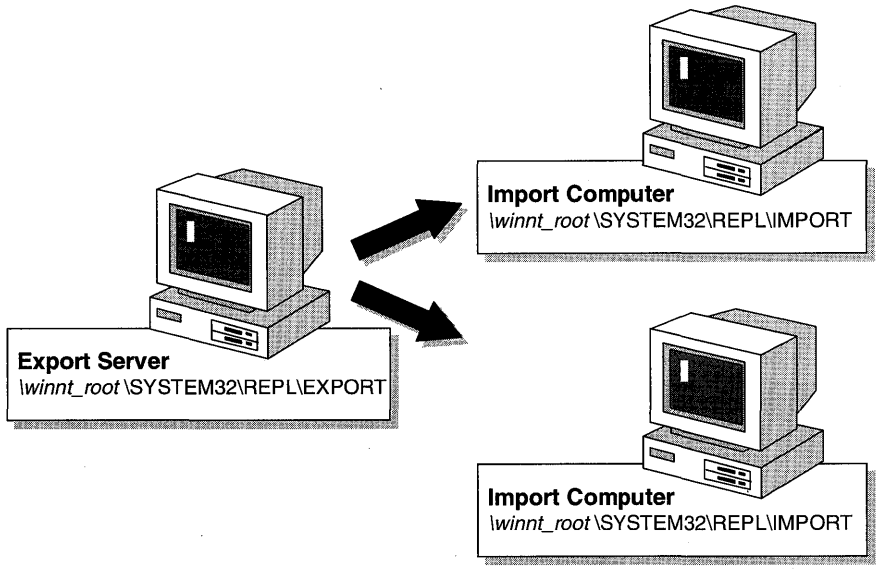


Figure 50: Replication components

The Export Server

The computer that provides the files and directories to be replicated is called the *export server*. Files and directories can be replicated from the export server to specified computers or domains. Only computers running Windows NT Server can be export servers. They do not, however, have to be domain controllers.

The Import Computer

Computers that receive replicated files and directories (sometimes called updates) from the export server are called *import computers*. Updates can be received from specified computers or domains. The following can be import computers:

- Microsoft Windows NT Server domain controllers and servers
- Microsoft Windows NT Workstations
- Microsoft Windows NT 3.1 Advanced Server computers
- Microsoft Windows NT 3.1 computers
- Microsoft LAN Manager OS/2 Servers and OS/2 peer servers

Export and Import Directories

The export server keeps the directories to be replicated in an *export directory*. By default, this is the \<*winnt_root*>\SYSTEM32\REPL\EXPORT directory. This directory is shared as REPL$ when you start the Directory Replicator service for exporting. You create subdirectories under this directory for each group of files you want replicated.

Each import server has an *import directory* that corresponds to the export server's export directory. By default, the import directory is \<*winnt_root*>\SYSTEM32\REPL\IMPORT. The Directory Replicator service automatically creates the subdirectories under this directory.

To provide for replication of logon scripts, a computer running Windows NT 3.5 Server exports logon scripts from the \<*winnt_root*>\SYSTEM32\REPL\EXPORT\SCRIPTS directory. Logon scripts are imported to the \<*winnt_root*>\SYSTEM32\REPL\IMPORT\SCRIPTS directory on import computers. By replicating the logon scripts, all domain controllers will be able not only to validate a user's logon request but also to supply the logon script to the user. The user's connected network resources will be present whenever the user logs on to the domain.

Preparing the Export Server

To set up replication on an export server, you must first create a user account for the Directory Replicator service to use. This account should be an account that a normal user would not use for logging on to the domain. The account should be set so that the password never expires, log on is possible during all hours, and the account has membership in both the Replicator and Backup Operators groups.

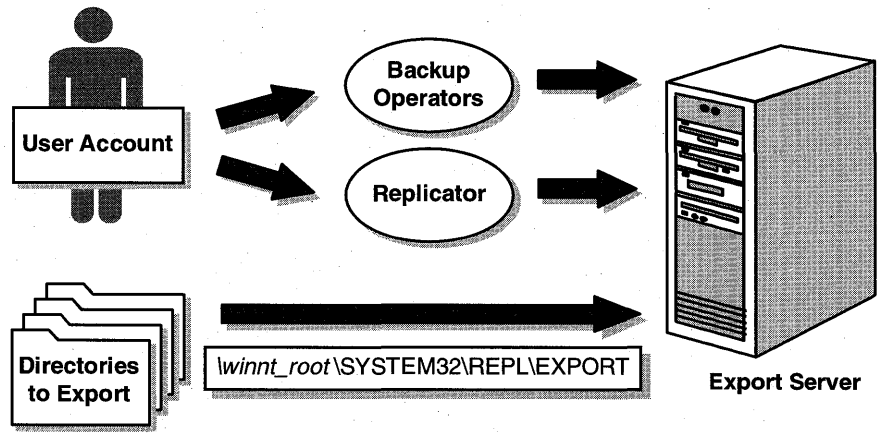


Figure 51: Export server preparations

When configuring the Directory Replicator service to start automatically, designate this account for the service to log on as, and specify the password.

The following steps are necessary for setting up replication on an export server:

- Using the default export directory structure, create directories to export.
- Configure the Directory Replicator service (including creating the user account for directory replication).
- Start replication.

► To prepare the export server

In this procedure, you prepare the PDC to be an export server to replicate logon scripts and server-based user profiles to the BDC.

Important Complete this procedure logged on as Administrator on the PDC of Domain-A.

---

1. Use User Manager for Domains to create a domain user account with the following properties:
   - Account name of replicate
   - Password is password
   - The User Must Change Password At Next Logon check box is cleared.
   - The Password Never Expires check box is selected.
   - All logon hours are allowed.
   - The account is a member of the domain's Backup Operators and Replicator groups.

2. Use File Manager to move the files from \<*winnt_root*>\SYSTEM32\REPL\IMPORT\SCRIPTS to \<*winnt_root*>\SYSTEM32\REPL\EXPORT\SCRIPTS.

   This places the logon script and the server-based user profile in the proper location for replicating. The Directory Replicator service will replicate the files into the proper location for logon script and profile use.

► To control the timing of directory export notices

In this procedure, you set how often an export server checks the replicated directories for changes. The default is to check every five minutes for files that need to be replicated. You will shorten this interval to one minute (to speed the directory replication process for this procedure). In a normal environment, the default of five minutes is standard.

Important Complete this procedure logged on as Administrator from the primary domain controller of Domain-A.

- Use REGEDT32.EXE to add the following values to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Replicator\Parameters:

Value Name	Data Type	Data
Interval	REG_DWORD	1 (decimal)
GuardTime	REG_DWORD	0 (decimal)

► To configure the Directory Replicator service

In this procedure, you configure the Directory Replicator service to start automatically when the Microsoft Windows NT Server computer starts and to use the Directory Replicator service account you just created.

Important If the export directory is on an NTFS partition, the Replicator group on the export server should be granted Full Control to the export directory tree.

Complete this procedure logged on as Administrator from the primary domain controller of Domain-A.

---

1. Using Server Manager, select PDC-A.
2. From the Computer menu, choose Services.

   The Services on PDC-A dialog box appears.
3. Under Service, select Directory Replicator and then choose Startup.

   The Directory Replicator service dialog box appears.
4. Under Startup Type, select Automatic.
5. Under Log On As, select This Account.
6. In the This Account box, type **replicate**

7. In the Password and Confirm Password boxes, type **password**, and then choose OK.

   A Server Manager message box appears, indicating that the account replicate has been granted the Log On As A Service right.

8. Choose OK.

   The Services on PDC-A dialog box appears.

9. Choose Close.

► To start the Directory Replicator service

In the following procedure, you designate to which BDCs to export and then start the Directory Replicator service on the PDC.

Important Complete this procedure logged on as Administrator from the primary domain controller of Domain-A.

---

1. Using Server Manager, select PDC-A.
2. From the Computer menu, choose Properties.

   The Properties on PDC-A dialog box appears.

3. Choose Replication.

   The Directory Replication dialog box appears.

4. Select Export Directories.
5. Under Export Directories choose Add.

   The Select Domain dialog box appears.

6. Under Select Domain, select DOMAIN-A, and then choose OK.
7. If the To List box is left empty, which import servers will receive the exported files?

8. In the Directory Replication on PDC-A dialog box, choose Import Directories.

   Choosing Import Directories allows the PDC to replicate logon scripts and profiles to itself, placing them in the correct directory for user access.

9. Under Import Directories choose Add.

   The Select Domain dialog box appears.

10. Under Select Domain, select DOMAIN-A, and then choose OK.

11. Choose OK to close the Directory Replication dialog box.

    Notice the Service Control status box starting the Directory Replicator service.

12. Choose OK to close the Properties dialog box.

Important If you still have the Alerter service running, an Alerter message appears, notifying you that files have been replicated. Choose OK to clear the message.

Preparing the Import Server

To set up replication on an import server, you must first create a replication user, if the import computer is not already part of the export server's domain or trusting domain.

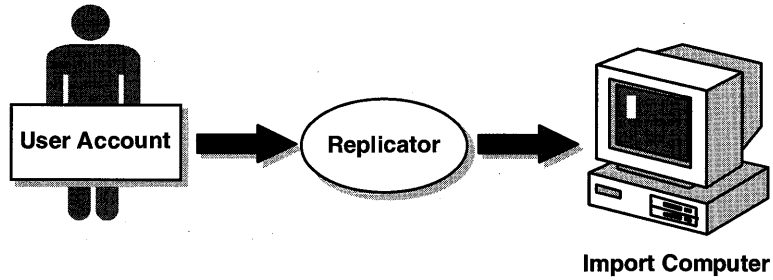


Figure 52: Import server preparations

The following steps are necessary for setting up replication on an import computer:

1. If the import computer is not part of the export server's domain or a trusting domain, create a replication user account. This account must have permission to access the export server's REPL$ share.

   If the import computer is part of the export server's domain or a trusting domain, use the domain's replicator user account.

2. Grant the replicator user account membership in the local Replicator group.
3. Configure the Directory Replicator service to start automatically and to log on under the directory replicator user account created on the export server. This causes the replication service to start whenever the server starts. This allows for any scripts and the like to be implemented at startup.
4. Using Server Manager, configure the import computer to receive files from other servers or domains.

► To configure the Directory Replicator service

In this procedure, you configure the Directory Replicator service to start automatically when Windows NT Server starts using the Directory Replicator service account.

Important Complete this procedure logged on as Administrator from the backup domain controller of Domain-A.

---

1. Using Server Manager, select BDC-A.
2. From the Computer menu, choose Services.

   The Services on BDC-A dialog box appears.
3. Under Services, select Directory Replicator, and then choose Startup.

   The Directory Replicator Service dialog box appears.
4. Under Startup Type, select Automatic.
5. Under Log On As, select This Account.
6. In the This Account box, type **replicate**
7. In the Password and Confirm Password boxes, type **password**, and then choose OK.
8. Choose Close to return to Server Manager.

► To start the Directory Replicator service

In this procedure, you start the Directory Replicator service on the BDC to import from the PDC.

Important Complete this procedure logged on as Administrator from the BDC of Domain-A.

---

1. Using Server Manager, select BDC-A.
2. From the Computer menu, choose Properties.

   The Properties on BDC-A dialog box appears.
3. Choose Replication.

   The Directory Replication dialog box appears.
4. Select Import Directories.
5. Under Import Directories, choose Add.

   The Select Domain dialog box appears.
6. Under Select Domain, select DOMAIN-A and then choose OK.

7. Choose OK to close the Directory Replication dialog box.

   Notice the Service Control message box starting the Directory Replicator service.

8. Choose OK to close the Properties dialog box.

► **To verify that directory replication has occurred**

In this procedure, you verify that directory replication has occurred by viewing the import directory structure to see whether the logon script and user profile have been replicated.

Important Complete this procedure logged on as Administrator from both domain controllers of Domain-A.

- Use File Manager to check the import path, \<*winnt_root*>\SYSTEM32\REPL\IMPORT\SCRIPTS, to verify that DAILY.TXT, NETLOGON.BAT and USERS.MAN have been replicated.

  The files should have been replicated. If DAILY.TXT, NETLOGON.BAT and DAILY.TXT were not replicated, check the Application Event log for entries made by the Replication Service. Also, verify that only one instance of Server Manager is running on each controller.

Managing Replication for the Export Server

After directory replication has been configured, managing the replication process allows you to control what directories in the export tree can be replicated and what directories are imported into the import tree.

Server Manager is used to manage the directories on the export server.

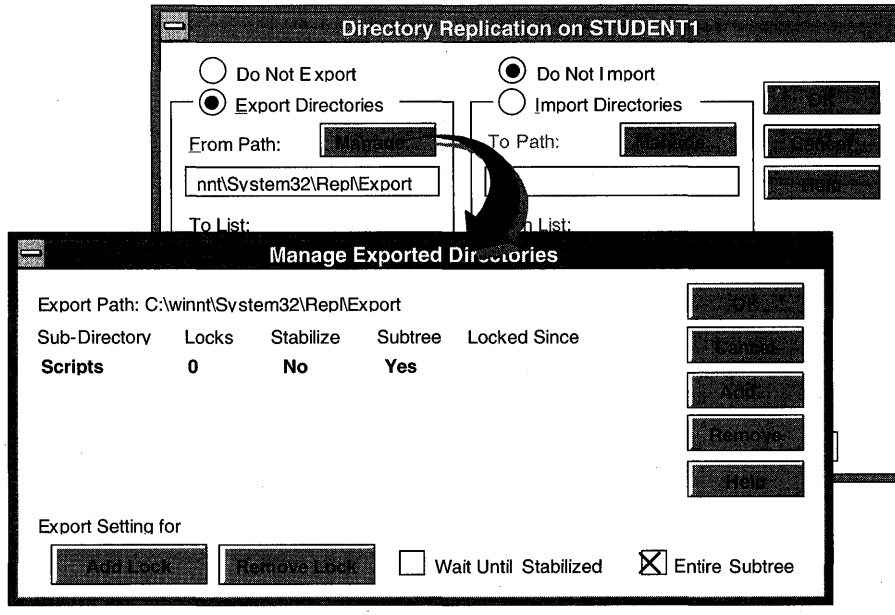


Figure 53: Export server management

With Server Manager, you can manage the following aspects of replication at the export server:

- Export Path—Path from which directories are exported.
- Locks—Prevents a directory from being exported. This is useful when you are working on files in a directory and do not want the directory replicated until all the work is completed.
- Stabilize—Indicates whether files in the export directory wait two minutes or more after changes before being exported. This helps prevent the premature replication of a directory that is being actively changed and might not contain complete data.
- Subtree—Indicates whether the entire subtree will be exported.
- Locked Since—Date and time a lock was placed on a directory.

The Registry contains entries that control various aspects of replication. These are located in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \Replicator\Parameters.

For More Information See the *Microsoft Windows NT Resource Kit.*

Managing Replication for the Import Computer

Server Manager also allows you to manage replication on the import server.

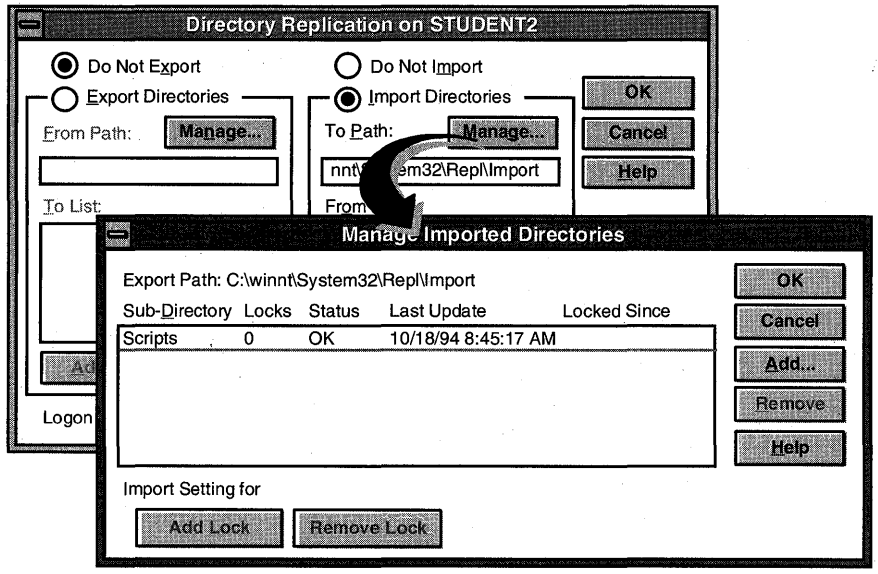


Figure 54: Import server management

With Server Manager, you can manage the following aspects of replication at the import computers:

- Import Path—Path in which replicated directories are stored.
- Locks—Prevents a directory from being imported.
- Status—Indicates the status on receiving updates from the export server:
  - OK—The directory is receiving regular updates from the export server and the imported data is identical to the data exported.
  - No Master—The directory is not receiving updates from the export server. The export server might not be running or might have stopped exporting updates.

- No Sync—Indicates that the directory has received updates, but 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 to the export server, or an export server malfunction.
- [blank]—Replication has never occurred for the directory. Replication might not be properly configured for this import computer, for the export server, or both.

▪ Last Update—Date and time the last update was made to a file in the import directory.

► To manage directory replication at the export server

Important Complete this procedure logged on as Administrator from the PDC of Domain-A.

1. Using Server Manager, select PDC-A.
2. From the Computer menu, choose Properties.

   The Properties on PDC-A dialog box appears.
3. Choose Replication.

   The Directory Replication dialog box appears.
4. Under Export Directories, choose Manage.

   The Manage Exported Directories dialog box appears.
5. Choose Add.

   The Add Sub-Directory dialog box appears.
6. In the Sub-Directory Name box, type **Profiles** and then choose OK.

   The Manage Exported Directories dialog box appears with Profiles added.
7. Under Sub-Directory, select Profiles and choose Add Lock.
8. Choose OK to return to the Directory Replication on PDC-A dialog box.
9. Choose OK to return to the Properties for PDC-A dialog box.
10. Use File Manager to create \<*winnt_root*>\SYSTEM32\REPL\EXPORT\PROFILES and then copy USERS.MAN into the new directory.

► To manage directory replication at the import server

In this procedure, you verify that the locked directory was not replicated.

Important Complete this procedure logged on as Administrator from both domain controllers of Domain-A.

---

1. In User Manager for Domains, access the Properties dialog box for your controller, and then choose Replication.

   The Directory Replication dialog box appears.
2. Under Import Directories, choose Manage.

   The Manage Imported Directories dialog box appears.
3. View the status of imported directories. What is the status of the Profiles directory? Why?

4. Choose OK.
5. When would you place a lock on a directory on the export server?

6. When would you place a lock on a directory on the import server?

► To remove the export directory lock

In this procedure, you remove the lock on the Profiles directory on the export server and verify that the unlocked directory was replicated.

Important Complete this procedure logged on as Administrator from the PDC of Domain-A.

---

1. Use Server Manager to remove the lock from the Profiles directory.

Important Complete this procedure logged on as Administrator from both domain controllers of Domain-A.

---

2. Use File Manager and Server Manager to verify that the Profiles directory was replicated when the lock was removed.
3. After the Profiles directory has been replicated, exit Server Manager.

Lesson Summary

To ensure that all domain controllers can offer a consistent user environment, as defined in a logon script or mandatory user profile, the Directory Replicator service can be used to copy updated files automatically from export servers to import computers.

For directory replication to occur, a number of steps are necessary to prepare the export and import computers. The export and import directory structures must be created, the directory replication service must be configured, and the directory replicator service must be started.

Managing the directory replication process involves determining which directories should be replicated and received at the export and import computers.

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Your company has decided to use logon scripts to support the MS-DOS–based network clients on your network. However, you have more than one domain controller in the domain. How can you make sure that the logon script is available to a user being validated by any domain controller?

2. Give an example of how replication can be used.

3. For replication to work, which computers have to be running the Directory Replicator service?

4. What is the default export directory path?

5. What is necessary to set up replication on an import computer that is part of the export server's domain?

For more information on	See
Using Directory Replicator service	Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide.*
	Chapter 4, "Managing the User Environment," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
	Chapter 5, "Managing Network Files," in the *Microsoft Windows NT Server Concepts and Planning Guide..*
Setting up an export server	Chapter 4, "Managing User Environments," in the *Microsoft Windows NT Server Network Operations Quick Reference Guide.*
Setting up an import server	Chapter 4, "Managing User Environments" in the *Microsoft Windows NT Server Network Operations Quick Reference Guide.*
Creating a Directory Replicator Service Account	Chapter 15, "Server Manager," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Enabling a service to start automatically	Server Manager Help, Manage Services, Configuring Service Startup
	Server Manager Help, Manage Services, Assigning a Logon Account to the Directory Replicator Service
Preparing an Export Server	Server Manager Help, *computer* Properties, Replication help
Preparing an Import Server	Server Manager Help, *computer* Properties, Replication help

CHAPTER 5

Establishing Trust Relationships

Before You Begin

Before you begin this chapter, you must have completed chapters 1-4. These chapters prepare your network for the advanced feature of trust relationships. In addition, it is recommended that you review the "Trust Relationships" segment of the video included in your kit.

At this point you should have two computers set up in DOMAIN-A, one as a PDC and the other as a BDC. In this chapter, either you configure the BDC computer to dual-boot and install a second domain PDC, or you reinstall and create a new domain PDC.

Important All lessons in this chapter are dependent on each other. Please complete them in order.

Lesson 1: Introduction to Trust Relationships

In this lesson you learn what trust relationships are and how they are implemented to make managing a large network more efficient. You also explore the advantages that trust relationships provide for administrators and for users.

To implement trust relationships later in this chapter, you set up one computer to dual-boot and create a second domain. Two domains are necessary to implement trust relationships.

After this lesson you will be able to:

- Define a trust relationship.
- Describe the key advantages of trust relationships for both administrators and users.
- Explain how trusts are based on a one-way relationship.
- Contrast a trusted (account) domain with a trusting (resource) domain in a trust relationship.
- Prepare your network for trust relationships.
- Use the BOOT.INI file to setup a dual-boot computer.

Estimated Completion Time: 30 minutes

What Is a Trust Relationship?

A trust relationship is a link between two domains This link allows one domain to recognize the user accounts of another domain, trusting the other domain to authenticate the logons of those users. When trust relationships are properly established between domains, they allow a user to have only one user account, and still be able to access the entire network. Trust relationships can also be thought of as a method of account administration.

Advantages for Administrators

There are two key advantages that trust relationships offer administrators:

- Trust relationships simplify administration by linking two domains into a single administrative unit. You use trust relationships to centralize user account administration into one domain instead of administering each domain separately.
- A trust relationship between the two domains enables user accounts and global groups to be used in domains other than the domain where those accounts are located.

Advantages for Users

There are two key advantages that trust relationships offer users:

- Trust relationships make it possible for users from one domain to be permitted to use resources in another domain, even if they do not have a user account in the domain where the resource is located. For example, if you have an account only in DOMAIN-A, but you need to use a resource in DOMAIN-B, a properly configured trust between DOMAIN-A and DOMAIN-B allows your account to be granted rights and permissions to perform tasks or use resources in DOMAIN-B.
- All the Windows NT computers on a network can recognize the user account. A user has to log on and provide a password only once to access any shared resources on the network for which the user account has been granted permissions.

Trust Relationships Between Domains

All trusts are established from a one-way perspective. A two-way trust is the sum of establishing two one-way trusts.

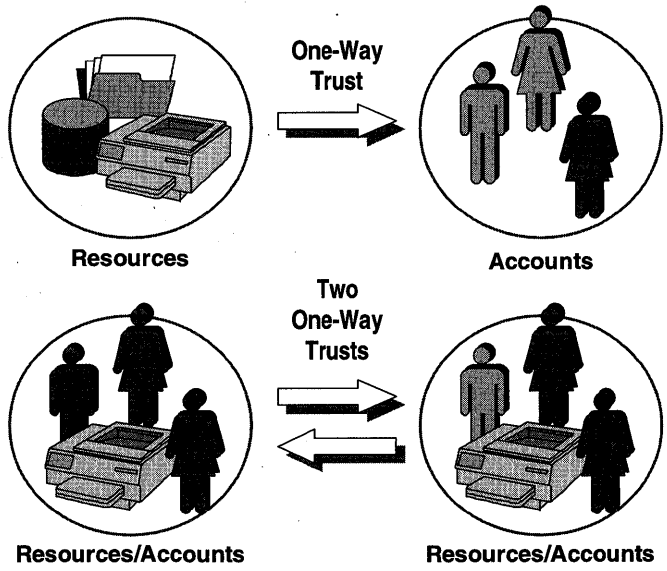


Figure 55: One-way and two-way trust relationships

The previous figure shows a trust relationship going one way, in which the Accounts domain is trusted by the Resources domain, and a trust relationship going two ways, in which both domains contain resources and accounts and they trust each other.

Trusting vs. Trusted Domains

In all trust relationships, one domain is always the *trusted* domain, while the other is the *trusting* domain.

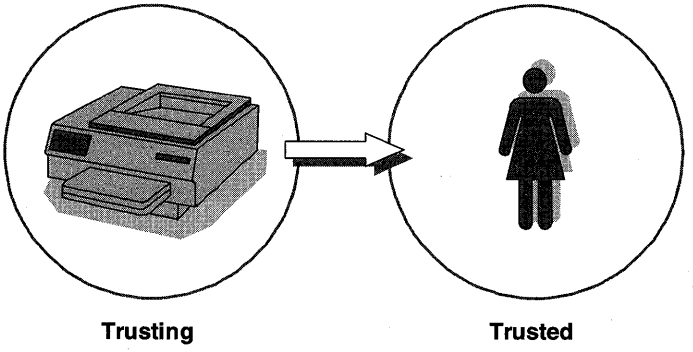


Figure 56: Relationship of users to resources

The previous figure illustrates that the printer is a resource, and the domain in which it is located is referred to as a Resource (trusting) domain. The person using the printer has a user account in the Account (trusted) domain.

- Trusted Domain—Accounts are kept in the *trusted*, or account domain. The arrows in all trust diagrams point to the domain where the accounts are kept. The key to understanding all trust relationships lies in the phrase, "Arrows point to people you can trust."
- Trusting Domain— Resources are usually located in a *trusting* domain, which is also known as a resource domain. The arrows point away from the trusting domain.

The concepts of trusted versus trusting can be thought of in terms of resources. The domain with the resources is trusting users from a different domain and allowing them to use the resources, if the proper trust relationship has been established and permissions are assigned.

For example, if your neighbor wanted to use your car, you would give your neighbor your car, and your neighbor could then drive it. You have set up a one-way trust relationship with your neighbor, in which you trust your neighbor with your car.

Your neighbor represents the trusted domain. You represent the trusting domain with the car (resource). In a diagram of this arrangement, the arrow would point from you to your neighbor.

Preparing to Set Up a Trust Relationship

Setting up trust relationships properly requires knowledge and planning. Review the following considerations and planning issues before determining your trust relationship configuration.

Considerations

- Trust relationships can be established only between Microsoft Windows NT Server domains (not workgroups or LAN Manager domains).
- Accounts and global groups in trusted domains can be given permissions in trusting domains.
- You can be physically located in a trusting (resource) domain and log on to a trusted domain.

Planning Issues

- Determine which domain(s) will be the trusted domain by identifying where the accounts are located.
- Determine which domain(s) will be the trusting domain by identifying where the resources are located.
- Do you want trusted domains to be trusting domains also and vice versa?

You will now create a second domain to prepare your network environment for implementing trust relationships.

► To create a second domain

At this point you have two computers configured with Windows NT Server in DOMAIN-A:

- PDC-A
- BDC-A

You will now set up the BDC-A computer to dual-boot between Windows NT Server installations. You install a primary domain controller in a second domain called DOMAIN-B. You need your Configuration Table for this procedure.

Important Complete this procedure from the BDC of DOMAIN-A only.

---

1. Start File Manager and select the drive containing the Windows NT Server CD-ROM.
2. Change to the appropriate platform subdirectory, such as I386, and then start WINNT32.EXE.

   A Windows NT 3.5 Upgrade/Installation dialog box appears, prompting for the path to the Windows NT 3.5 files.
3. Verify that the path is correct and choose Continue.

   A Windows NT 3.5 Server Installation/Upgrade message box appears, indicating that you need three blank high density disks, and tells you how to label them.
4. When prompted, insert the appropriate disks in drive A, and then choose OK.

   The Windows NT 3.5 Server Installation/Upgrade status box appears, indicating the progress of the file copy process.

   A Windows NT 3.5 Server Installation/Upgrade message box appears, indicating that the computer needs to be restarted with Windows NT Server Setup boot disk in drive A.
5. Choose Restart Computer.
6. Do *not* upgrade the existing installation. Install a new copy of Windows NT Server as the primary domain controller (PDC-B) for DOMAIN-B, using information from your Configuration Table

---

Note For detailed steps on installing Windows NT Server, see Chapter 1, "Installing Windows NT Server," in this book.

You now have a primary domain controller in a second domain. To complete configuring this computer, you must complete the following procedures.

► To change the attributes of BOOT.INI

In this procedure, you modify BOOT.INI so that you can easily dual-boot between the BDC of DOMAIN-A and the PDC of DOMAIN-B. These entries appear on the operating system selection screen.

Important Complete this procedure from the PDC of DOMAIN-B.

---

1. Log on to DOMAIN-B as Administrator.
2. Start File Manager and select drive C.
3. From the View menu, choose By File Type.
4. Select Show Hidden/System Files, and then choose OK.

   You are returned to the File Manager window.

5. Select C:\BOOT.INI.
6. From the File menu, select Properties.

   The Properties for BOOT.INI dialog box appears.
7. Under Attributes, clear Read Only, and then choose OK.

   You are returned to the File Manager window.

► **To modify BOOT.INI**

1. From the File menu, choose Open.

   Notepad starts, and then loads BOOT.INI.

   The default boot loader selection is the Windows NT Server that you installed earlier in this lesson.
2. In the [Operating Systems] section of BOOT.INI, find the two entries that match the default boot loader selection.
3. Edit these two entries, changing Windows NT Server Version 3.5 to **Windows NT 3.5 PDC-B**
4. Edit the other two Windows NT Server entries, changing Windows NT Server Version 3.5 to **Windows NT 3.5 BDC-A**
5. Exit Notepad and save the changes to BOOT.INI.
6. Reset the attributes of BOOT.INI to include Read Only and System.
7. Exit File Manager.

► **To test modifications to BOOT.INI**

1. Shut down and restart your computer.
2. When the Operating System Selection screen appears, notice that the choices for starting the computer now include:
   - Windows NT Server 3.5 PDC-B
   - Windows NT Server 3.5 PDC-B VGA
   - Windows NT Server 3.5 BDC-A
   - Windows NT Server 3.5 BDC-A VGA
   - MS-DOS (depends on initial installation)
3. Select Windows NT 3.5 PDC-B.
4. Your computer initializes as a primary domain controller for DOMAIN-B.
5. Log on as Administrator.

When your computer boots, you can now easily select which Windows NT Server domain controller role to use.

► **To allow Everyone to log on locally**

In this procedure, you allow the group Everyone to log on locally at the domain controller of Domain-B. This is required for future procedures in this and subsequent chapters.

Important Complete this procedure logged on as Administrator from the PDC of DOMAIN-B.

---

1. Start User Manager for Domains.
2. From the Policy menu, choose User Rights.
3. In the Right box, select Log on locally.
4. Choose Add.
5. Under Names, select Everyone, and then choose Add.
6. Choose OK to return to the User Rights Policies dialog box.
7. Choose OK to return to User Manager for Domains.
8. Exit User Manager for Domains.

Now that you have a second domain configured and can dual-boot between BDC-A and PDC-B, you are ready to implement trust relationships in the following lessons.

Lesson Summary

To maintain user accounts in a central location yet allow for resource access in a different location, trust relationships can be established between Windows NT Server domains. Trust relationships consist of a trusted domain (containing the user and group accounts) and a trusting domain (containing the resources that users in the trusted domain need to access). Before implementing trust relationships, careful thought and planning is necessary to ensure that the trust relationship works as intended.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Define a trust relationship.

2. List two key advantages that trust relationships offer administrators and users.

3. Why are all trusts based on a one-way relationship?

4. Differentiate between a trusted domain and a trusting domain in a trust relationship.

5. List three planning considerations when preparing to establish trust relationships.

For more information on	See
Trust Relationships	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*

Lesson 2: Creating the Master Domain Model

In Chapter 1, "Installing Microsoft Windows NT Server," you created a single domain consisting of one primary domain controller. You later added a backup domain controller. A single domain is sufficient for a small number of groups and users, but if your organization is large, you might consider moving into one of the other domain models. For companies in which the network does have to be split into multiple domains for organizational purposes, although the network has a small number of users and groups, the master domain model could be the best choice. In this lesson, you explore the master domain model and implement the necessary trust relationships.

After this lesson you will be able to:

- Define what a master domain is and why a trust relationship is necessary.
- Identify and use the correct tool to establish trust relationships.
- List the recommended sequence for establishing trust relationships.
- Explain how passwords are used to increase security on the network.
- Establish one-way trust relationships to create a master domain model.

Estimated Completion Time: 20 minutes

What Is the Master Domain Model ?

The master domain model consists of at least two domains, each of which has its own domain controllers and defined roles within the master domain model. All user and global group account information is kept in one domain, called the *master domain*. The other domains, called *resource domains*, maintain the file, directory, and printer resources. The resource domains do not have to maintain users and global groups; they use the accounts from the master domain to assign user and group access to local resources.

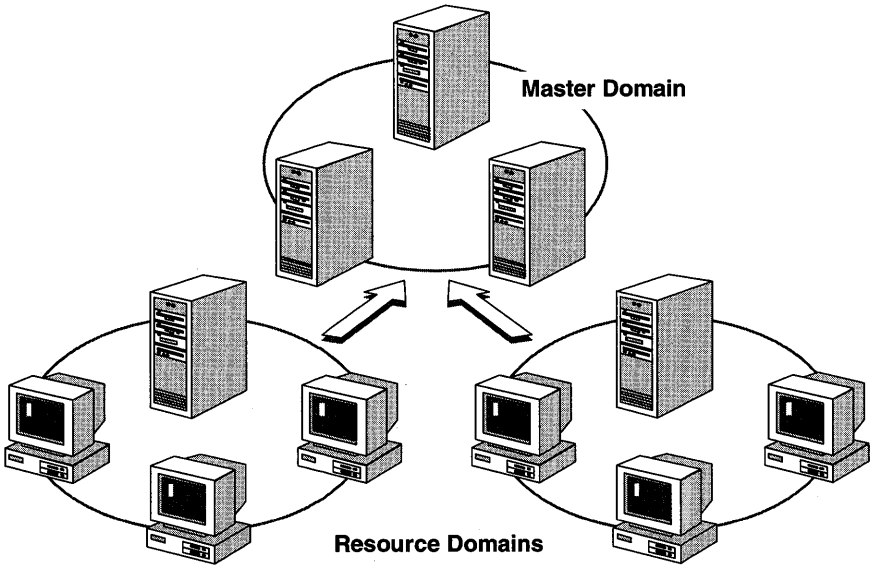


Figure 57: The master domain model

The master domain model offers the benefits of both multiple domains and centralized account administration. The master domain model would be appropriate in the following situations:

- A company has developed a complex assortment of divisions and departments, each wanting its own separate resource management.
- The company seeks to maintain a centralized user accounts database, but still allow access to resources throughout the entire enterprise.
- The network has not yet reached 15,000 users and groups.

The following table gives an overview of the advantages and disadvantages of the master domain model.

Advantages	Disadvantages
The best choice for companies that do not have many users and must have shared resources split into groups	Poor performance if the domain has too many users and groups
User accounts can be centrally managed.	Local groups must be defined in each domain in which they will be used.

(continued)

Advantages	Disadvantages
Resources are grouped logically.	
Department domains can have their own administrators, who manage the resources in the department.	
Global groups need to be defined only once (in the master domain).	

Trust Relationships in a Master Domain Model

The master domain is a trusted domain. All other domains are trusting domains linked to the master domain by one-way trust relationships.

The master domain model splits the network into two different areas of administration:

- User accounts—Located and maintained in the master domain, or trusted domain
- Resources—Located and maintained in the trusting domains

Only the domain controllers in the master domain have copies of the master domain's account database. In addition to the primary domain controller, there should be at least one backup domain controller, in case the primary domain controller fails.

With domains, the goal is to maintain only one account for each user on the entire network. This permits easy administration of the user accounts, and prevents password problems that might result from having to maintain a single user account in multiple domains.

In the master domain model, all accounts should be located in the master domain. No user accounts are needed in the resource domains. By implementing proper trust relationships, a user can log on from any domain and still be validated, because pass-through authentication, discussed in the next lesson, sends the request to the master domain where the user is verified.

Establishing Trust Relationships

Trusts are primarily for managing accounts. Therefore, the first thing to do when you set up a trust is to identify which domain will be the *trusted* domain.

Trust relationships are established using User Manager for Domains. To set up a one-way trust relationship, you start User Manager for Domains, and then choose Trust Relationships from the Policies menu. There are two sections in the Trust Relationships dialog box:

- The Permitted to Trust this Domain box is completed by the trusted domain. It specifies the names of the trusting domains.
- The Trusted Domains box is completed by the trusting domain. This section specifies the names of the trusted domains.

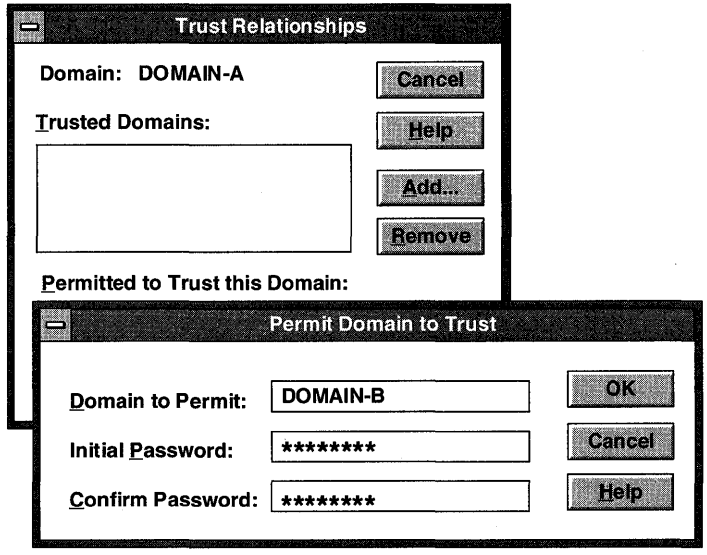


Figure 58: The Trust Relationships and Permit Domain to Trust dialog boxes

The order in which you establish trust is not critical. However, it is better to establish the Permitted to Trust this Domain relationship first, and then establish the Trusted Domain relationship. In this way, the new trust relationship takes effect immediately and can be verified immediately.

The recommended sequence for establishing a trust relationship between two domains is as follows:

1. The administrator in a trusted (account) domain initiates a trust by adding the name of a trusting (resource) domain in the Permitted to Trust this Domain box. A password can also be part of implementing the trust to control which domains are allowed to participate in trust relationships.
2. The administrator in the trusting domain completes the trust by adding the name of the trusted (account) domain in the Trusted Domains box. This administrator must enter the password created at the trusted domain when it is time for the trusting domain to complete the trust. This is the only time that the trusting domain administrator needs to enter the password.

Permit Domain to Trust

Because trust relationships are primarily an administration tool for managing user accounts, you should first identify the trusted domain where the accounts will reside.

When an account domain has been identified, that domain specifies the other domains which it will permit to trust it. The trust can be initiated from either domain. This is done through the Policies menu in User Manager for Domains.

Prepare to Trust

The following figure illustrates the master domain model configuration you implement in this lesson.

DOMAIN-A keeps the accounts (the trusted domain), and DOMAIN-B has the resources (the trusting domain). This configuration allows a user sitting at a Windows NT computer in a trusting domain (DOMAIN-B) to log on using an account that exists in the trusted domain (DOMAIN-A).

If you are not using the suggested domain names, refer to your Configuration Table to fill in your domain names. Use this figure for reference throughout this lesson.

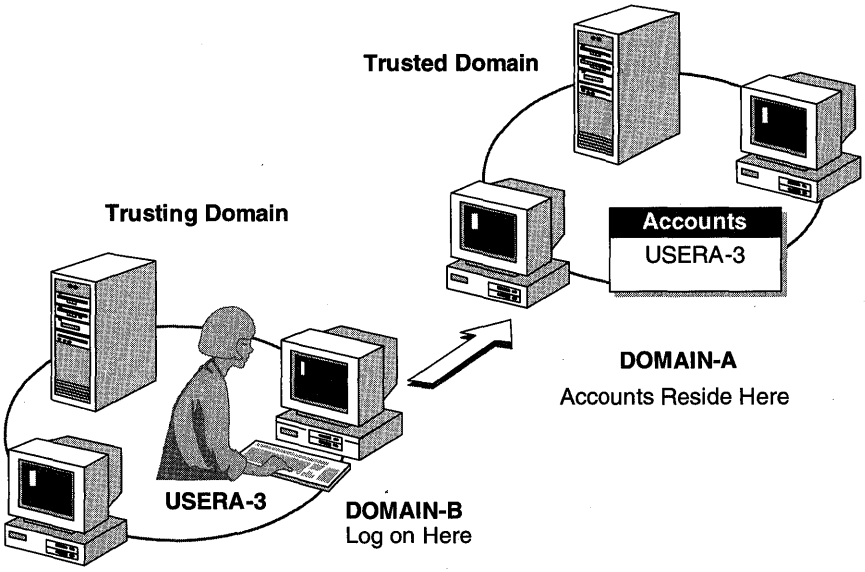


Figure 59: The master domain model that you will implement

► To permit DOMAIN-B to trust DOMAIN-A

At this point you should have two computers set up with Windows NT Server. One computer is the PDC for DOMAIN-A, the other is the PDC for DOMAIN-B. You need your Configuration Table in this procedure.

Important Complete this procedure logged on as Administrator from the PDC of DOMAIN-A.

---

1. Open User Manager for Domains.
2. From the Policies menu, choose Trust Relationships.

   The Trust Relationships dialog box appears.
3. To the right of the Permitted to Trust this Domain list, choose Add.

   The Permit Domain to Trust dialog box appears.
4. In the Domain to Permit box, type **domain-b** (the name of the trusting domain).
5. Do not use a password. Leave Initial Password and Confirm Password blank.
6. Choose OK.

   The name of DOMAIN-B appears in the Permitted to Trust this Domain list.
7. Choose Close.

You have completed the first stage of implementing a one-way trust relationship between domains. You have permitted DOMAIN-B (the trusting domain) to trust DOMAIN-A (the trusted domain).

Important The trust relationship will not be complete until both domains have done their part to establish the trust relationship.

Trusting Domain Completes Trust

To complete the trust, the trusting domain (or resource domain) must add the trusted domain to its list of trusted domains. After this is done, the trusting domain can allow users from the trusted domain to be granted permissions to use resources in the trusting domain.

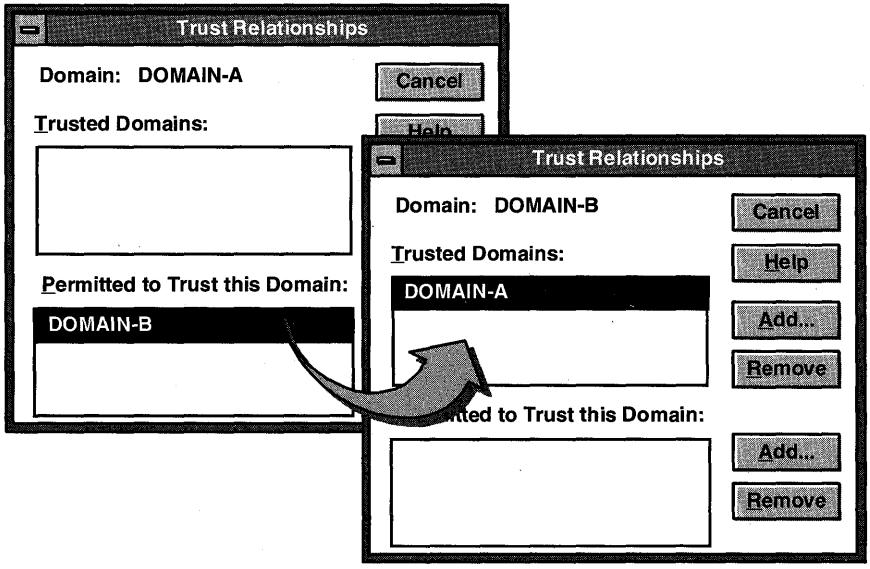


Figure 60: The Trust Relationships dialog box

The previous figure shows the Trust Relationships dialog box, with DOMAIN-B as the trusting domain and DOMAIN-A as the trusted domain.

► To complete the one-way trust relationship

At this point, you have completed the first part of establishing a trust relationship by permitting DOMAIN-B to trust DOMAIN-A. You will now complete the trust relationship by configuring DOMAIN-A to be a trusted domain of DOMAIN-B.

Important Complete this procedure logged on as Administrator from the PDC of DOMAIN-B.

---

1. Open User Manager for Domains.
2. From the Policies menu, choose Trust Relationships.

   The Trust Relationships dialog box appears.
3. To the right of the Trusted Domains list, choose Add.

   The Add Trusted Domain dialog box appears.
4. In the Domain box, type **domain-a** (the domain you are going to trust).
5. Do not use a password. Leave Password blank because the trusted domain did not assign a password to your domain.
6. Choose OK.

   A User Manager for Domains message box appears, indicating that the trust relationship was successfully established.
7. If you do not receive this message, what message did you receive? Take corrective action as indicated in the message. (Write the message below.)

8. Choose OK.

   The name of DOMAIN-A appears in the Trusted Domains list box.
9. Choose Close.

DOMAIN-B now trusts DOMAIN-A. This means that any user account in DOMAIN-A can log on to DOMAIN-A from a computer that is physically located in DOMAIN-B.

Lesson Summary

To establish a trust relationship, the domain with the accounts should first permit the domain with the resources to trust it. The trusting domain then adds the trusted domain to its list of trusted domains. When this has been completed properly, the trust relationship is active, and accounts in the trusted domain are available for use in the trusting domain.

For more information on	See
The Master Domain Model	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide*.
Establishing Trust Relationships	Chapter 2, "Managing Domains and Trust Relationships," in the *Microsoft Windows NT Server Network Operations Quick Reference*.

For online information about	From the Help menu, choose Contents and then
Establishing Trust Relationships	User Manager for Domains Trust Relationships Help

Lesson 3: Access Across Trusts

Two user access issues are solved as soon as trust relationships are established properly. First, a user can log on at a computer in a domain in which the user has no user account. Second, a user account defined in a trusted domain can be assigned resource permissions or given user rights in any trusting domain. In this lesson you test your domain configuration.

After this lesson you will be able to:

- Describe how pass-through authentication makes it possible for users to log on at domains in which they have no account.
- Assign permissions to resources and grant users rights across domains.

Estimated Completion Time: 30 minutes

Pass-Through Authentication

With pass-through authentication, a user needs an account in only one domain and can still access the entire network—including all domains that trust the user's account domain. After being logged on, the user is known throughout the network as DomainName\Username, where DomainName is the domain that contains the user's account and authenticates the logon request, and Username is the actual account name used for the logon process.

For example, in a large network consisting of several domains tied together by trust relationships, a user can log on at a computer in DOMAIN-B and be verified by the user accounts database in DOMAIN-A.

Pass-through authentication occurs in one of two circumstances:

- At initial logon from a workstation in a trusting domain, when a user is logging on to a trusted domain.
- When the user is connecting to a resource in a trusting domain from a computer in the trusted domain.

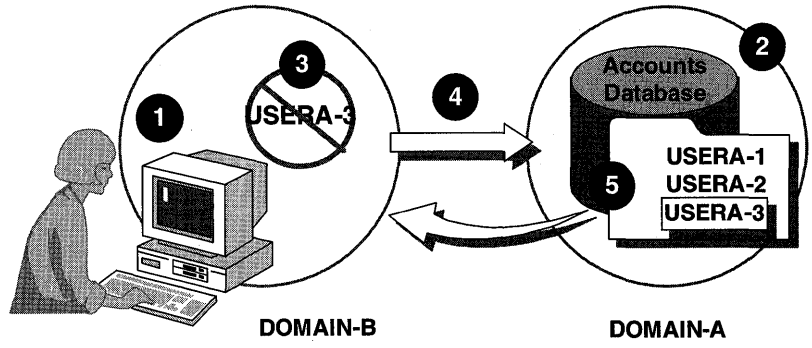


Figure 61: Pass-through authentication

In the previous figure, the logon process using a trusted domain is accomplished by this sequence of events:

1. When a Windows NT computer starts, it locates a Windows NT Server domain controller in its domain (DOMAIN-B).
2. USERA-3 attempts to log on at a computer in DOMAIN-B with a user account from DOMAIN-A.

   This is done by selecting DOMAIN-A in the From box of the Welcome dialog box.
3. The Windows NT Server domain controller in DOMAIN-B is not able to authenticate the request because the request is for a DOMAIN-A user account.
4. The authentication request is passed through the trust to a Windows NT Server domain controller in DOMAIN-A. This Windows NT Server domain controller checks DOMAIN-A's account database for the existence of USERA-3's account and for correct password information.
5. The domain controller in DOMAIN-A authenticates USERA-3's request and passes SID and group information about USERA-3 back to the domain controller in DOMAIN-B. The domain controller in DOMAIN-B then passes the information to USERA-3's Windows NT computer.

Logging On Through the Trust

In this procedure, you use a user account in the trusted domain. You then test the trust by logging on to the trusted domain from a computer in a trusting domain.

► **To prepare to test the trust**

At this point, you have established a one-way trust relationship with DOMAIN-A and DOMAIN-B. User accounts created in Chapter 2 are used in this procedure.

Important Complete this procedure logged on as Administrator from the PDC of DOMAIN-A.

---

1. Confirm that USERA-3 has the following properties:
   - USERA-3 should be a member of the default group Domain Users.
   - USERA-3 should not have to change the password at next logon.
   - USERA-3 should not exist in DOMAIN-B.

   Note For more information on checking properties of a user account, see the Help files associated with User Manager for Domains.

► **To identify the domains trusted by DOMAIN-A**

Important Complete this procedure from the PDC of DOMAIN-A.

---

1. Log off.
2. Press CTRL+ALT+DEL to access the Welcome dialog box.
3. In the From box, display the available domains.
4. Which names appear in the From box of a trusted domain?

5. Log on as Administrator.

► **To identify the domains trusted by DOMAIN-B**

Important Complete this procedure from the PDC of DOMAIN-B.

---

1. Log off.
2. Press CTRL+ALT+DEL to access the Welcome dialog box.

3. In the From box, display the available domains.
4. Which names appear in the From box of a trusting domain?

► **To complete the logon process**

Important Complete this procedure from the PDC of DOMAIN-B.

1. Attempt to log on to DOMAIN-B as the user named USERA-3. (DOMAIN-B should appear in the From box.)
2. Were you able to log on? Why or why not?

3. Attempt to log on to DOMAIN-A as the user named USERA-3. (DOMAIN-A should appear in the From box to indicate that you want to be validated by the user accounts database of DOMAIN-A.)
4. Were you able to log on? Why or why not?

5. Log off.

   By logging on to DOMAIN-A while your computer is a member of DOMAIN-B, you have verified that a trust relationship exists.

Granting Permissions Across Trusts

After a trust has been established, you can grant permissions across the trust.

The List Names From box in the Add Users and Groups dialog box, shown in the following figure, allows you to display accounts and groups located in the local domain and other trusted domains. This allows the local administrator to access user and global group accounts from any trusted domains when assigning access permissions to resources or when adding user rights policies.

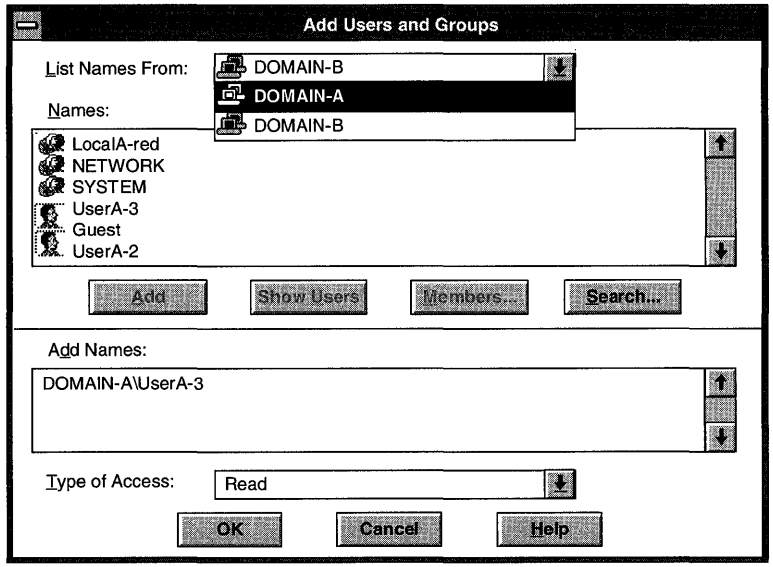


Figure 62: The Add Users and Groups dialog box

► To create and share a resource

At this point you have established a trust relationship between DOMAIN-A (trusted) and DOMAIN-B (trusting). In this procedure, you create and share a resource in the trusting domain, assigning permissions to an account defined in the trusted domain. You then log on and access the resource from the trusted domain. You need your Configuration Table for the second domain PDC drive/partition.

Note For this procedure, you must know how to share a directory and assign permissions to it, and how to use Notepad.

Important Complete this procedure logged on as DOMAIN-B\Administrator from the PDC of DOMAIN-B.

---

1. Use File Manager to share a directory on the PDC of DOMAIN-B, using the following information:
   - Directory: <*second domain PDC drive/partition*>:\users\default
   - Sharename: SHARE-B
   - Permissions:
     DOMAIN-B\Administrators have FULL CONTROL
     DOMAIN-A\USERA-3 has FULL CONTROL
     There are no other permissions assigned.

Important To assign permissions to DOMAIN-A\USERA-3, make sure that DOMAIN-A is selected in the List Names From box.

► **To log on and access the share from DOMAIN-A**

Important Complete this procedure from the PDC of DOMAIN-A.

1. Log off, and then log on to DOMAIN-A as USERA-3.
2. Use File Manager to connect to \\PDC-B\SHARE-B.
3. Verify that you have full access to the resource by using Notepad to create and save a file in SHARE-B.
4. Disconnect from \\PDC-B\SHARE-B.
5. Close File Manager.
6. Log off.

► **To log on and access the share from DOMAIN-B**

Important Complete this procedure from the PDC of DOMAIN-B.

1. Log off, and then log on to DOMAIN-A as USERA-3.
2. Use File Manager to connect to \\PDC-B\SHARE-B.
3. Verify that you have full access to the resource by using Notepad to create and save a file in SHARE-B.
4. Disconnect from \\PDC-B\SHARE-B.
5. Close File Manager.
6. Log off.

By using accounts in the trusted domain (DOMAIN-A), you can log on at any trusting domain (DOMAIN-B). You can also use resources in any trusting domain.

Lesson Summary

Implementing trust relationships between domains solves three common problems that face most network administrators: centralized account management, domain logons, and entire network resource access. This lesson introduced the benefits of trust relationships and tested the trust relationship by showing how pass-through authentication allows users to log on to a trusted domain from a trusting domain.

For more information on	See
Pass-Through Authentication	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
Logging On	Chapter 1, "Knowing the Basics," in the *Microsoft Windows NT Server Network Operations Quick Reference.*
Access Permissions	Chapter 3, "Managing Users, Groups, and Security Policy," in the *Microsoft Windows NT Server Network Operations Quick Reference.*

For online information about	From the Help menu, choose Contents and then
Logging On	Welcome dialog box, choose Help
Access Permissions	File Manager Help, Sharing a Directory, Setting Permissions Through Shared Directories

Lesson 4: The Multiple Master Domain Model

For larger companies that want centralized administration, the multiple master domain model could prove to be the best choice because it is the most scalable. As the name implies, multiple master domains and trust relationships are required to create this model.

After this lesson you will be able to:

- Establish a two-way trust relationship.

Estimated Completion Time: 30 minutes

Trust Relationships in a Multiple Master Domain

In this model, there are several master domains. Each master domain serves as an account domain, and each network user account is created in one of these master domains. Other domains in the network are resource domains, which are typically created at the department level.

The following table summarizes the advantages and disadvantages of the multiple master domain model.

Advantages	Disadvantages
The best choice for companies with many users and a centralized MIS department.	Both local and global groups might have to be defined multiple times.
Scalable to networks with any number of users.	More trust relationships to manage.
Resources are grouped logically.	Not all user accounts are located in one domain.
Department domains can have their own administrators, who manage the resources in the department.	

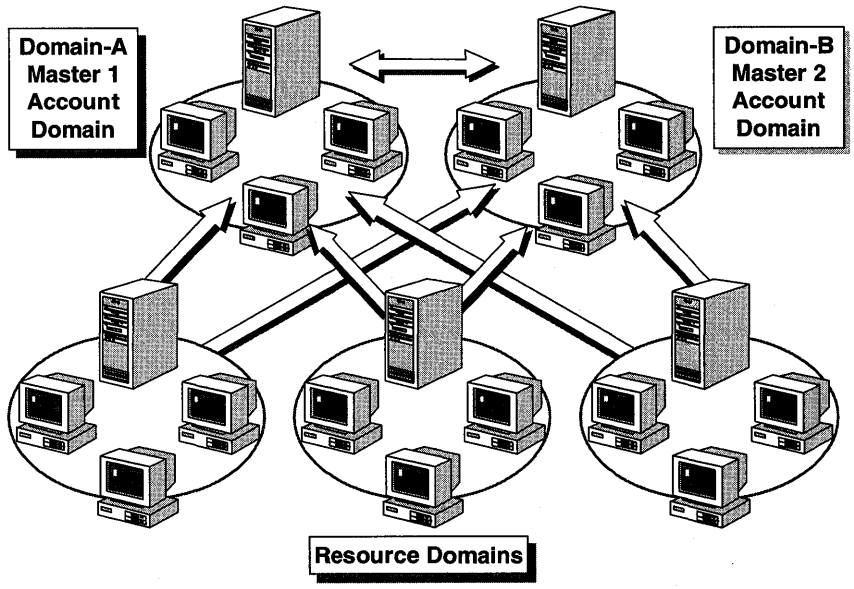


Figure 63: Trust relationships in a multiple master domain

The following trust relationships are required in a multiple master domain model:

- Each master domain is linked to every other master domain by two-way trusts. (Each master domain trusts every other master domain.) In the previous figure, DOMAIN-A trusts DOMAIN-B, and DOMAIN-B trusts DOMAIN-A.
- All of the resource domains trust each of the master domains, but they do not have to trust other resource domains. (There are one-way trusts between resource domains and master domains.) In the previous figure, each resource domain establishes a one-way trust with DOMAIN-A and a one-way trust with DOMAIN-B.

Each user account is defined only once. Because every user account in the company exists in one of the master domains and all domains in the company trust every master domain, every user account in the company is available to all domains. In the previous figure, any user in the network can log on from any computer in any domain.

Establishing and Testing a Two-Way Trust Relationship

When creating a multiple master domain, the master domains must trust one another. This is accomplished by creating a two-way trust, which is the sum of two one-way trusts. As you can see in the following figure, DOMAIN-A must trust DOMAIN-B, and DOMAIN-B must trust DOMAIN-A.

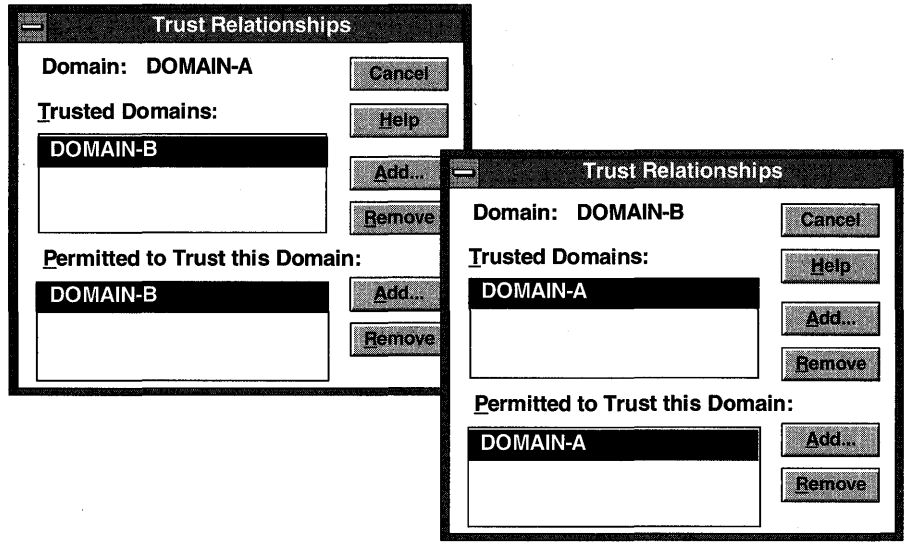


Figure 64: Two-way trusts in Trust Relationships dialog boxes

The following figure illustrates the configuration that you implement in this lesson. Notice that you have already created half of this two-way trust relationship: DOMAIN-B trusts DOMAIN-A user accounts to use DOMAIN-B resources.

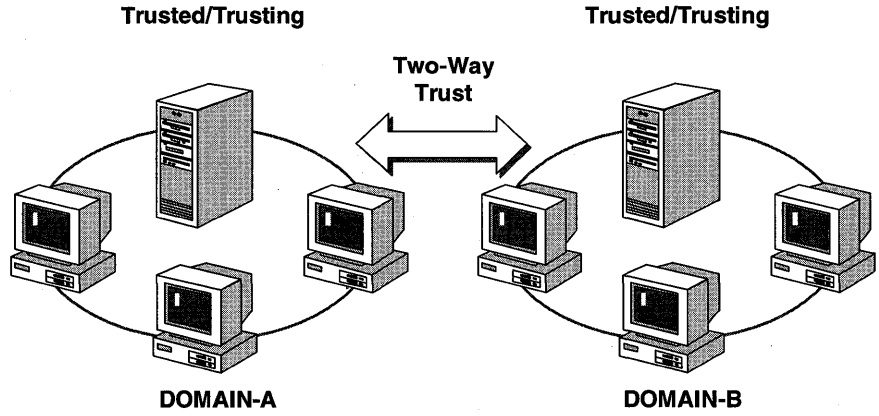


Figure 65: A two-way trust

► **To establish a two-way trust by permitting DOMAIN-A to trust DOMAIN-B**

In this procedure, you implement a two-way trust relationship with another domain. You have already established a one-way trust relationship. Using the same two domains, you now complete a two-way trust relationship.

Important Complete this procedure logged on as DOMAIN-B\Administrator from the PDC of DOMAIN-B.

- Use User Manager for Domains to permit Domain-A to trust Domain-B.

► **To complete the trust relationship from DOMAIN-A**

Important Complete this procedure logged on as Administrator from the PDC of DOMAIN-A.

- Use User Manager for Domains to make Domain-B a trusted domain.

You have now implemented the two-way trust relationship necessary between master domains in the multiplemaster domain model.

In the following procedures, you create a user on DOMAIN-B to verify the trust relationship. You assign permissions to this user, log on through the trust, and access the shared resource. You then assign permissions to a resource on DOMAIN-A, and access the resource while logged on with an account from DOMAIN-B.

► **To create a user and assign permissions in DOMAIN-B**

Important Complete this procedure logged on as DOMAIN-B\Administrator from the PDC of DOMAIN-B.

---

1. Create USERB-4 in DOMAIN-B with the following properties:
   - USERB-4 should be a member only of the default group Domain Users.
   - USERB-4 should not have to change the password at next logon.
   - USERB-4 should not exist in DOMAIN-A.
2. Use File Manager to add Full Control permissions for UserB-4 to Share-B.

Important Leave existing permissions assigned to DOMAIN-A\UserA-3.

► **To log on and access the share from DOMAIN-A**

Important Complete this procedure from the PDC of DOMAIN-A.

1. Log off and then log on to DOMAIN-B as UserB-4.
2. Use File Manager to connect to \\PDC-B\SHARE-B.
3. Verify that you have full access to the resource by using Notepad to create and save a file on SHARE-B.
4. Disconnect from \\PDC-B\SHARE-B.
5. Close File Manager.

► **To share a resource on DOMAIN-A**

Important Complete this procedure from the PDC of DOMAIN-A.

1. Log off and then log on to DOMAIN-A as Administrator.
2. Use File Manager to add Full Control permissions for DOMAIN-B\UserB-4 to Share-A.

   Important Leave the existing permissions for Administrators and LocalA-green.

3. Log off.

► **To log on and access the DOMAIN-A share from DOMAIN-B**

Important Complete this procedure from the PDC of DOMAIN-B.

1. Log off and then log on to DOMAIN-B as USERB-4.
2. Use File Manager to connect to \\PDC-A\Share-A.
3. Verify that you have full access to the resource by using Notepad to create and save a file in SHARE-A.
4. Disconnect from \\PDC-A\SHARE-A.
5. Close File Manager.
6. Log off.

Variations of the Multiple Master Domain Model

The multiple master domain model is an extension of the master domain model. In Lesson 2, you configured a master domain model. In it, DOMAIN-A was the master domain, and DOMAIN-B trusted DOMAIN-A. In Lesson 3, you logged on and accessed resources across the trust relationship. You had one master domain and one resource domain.

In this lesson, you configured a two-way trust relationship between two domains. In terms of the multiple master domain model, these two domains function as multiple masters.

If you had more than two domains in your environment, you could implement the multiple master domain model by configuring your additional domains as resource domains. To do this, you configure each of your additional domains to trust both DOMAIN-A and DOMAIN-B. You would then be able to sit at any computer in any of these domains, log on to the master domain that contained your user account, and access any resource in any of the domains to which your account has been given permissions.

Lesson Summary

For companies with a large user base, a master domain model might not allow enough flexibility in the management of user accounts. In such a situation, a multiple master domain model might be better suited. A multiple master domain model is very similar to the master domain model; the major difference is the existence of multiple account domains, which have two-way trust relationships established between them. The network resources are still maintained in resource domains, which have one-way trusts with each master domain in the model.

For more information on	See
Multiple Master Domain Model	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
Establishing a two-way trust relationship	Chapter 13, " User Manager for Domains," in the *Microsoft Windows NT Server System Guide.*

Lesson 5: The Complete Trust Domain Model

If you want the management of users and domains to be distributed among different departments rather than centralized, you might want to use the complete trust model. With this model, every domain on the network trusts every other domain.

In this lesson you explore the criteria for the complete trust domain model.

After this lesson you will be able to:

- Implement the complete trust domain model.
- Determine the number of trusts needed in a complete trust.

Estimated Completion Time: 15 minutes

Trust Relationships in a Complete Trust Model

The complete trust domain model consists of several domains, and each domain performs its own administration. No single domain exerts any control over the others. The complete trust domain model distributes the administration of users, groups, and domains among different departments rather than centralizing it. This model is ideal for companies that want individual departments or groups to manage their own network environments.

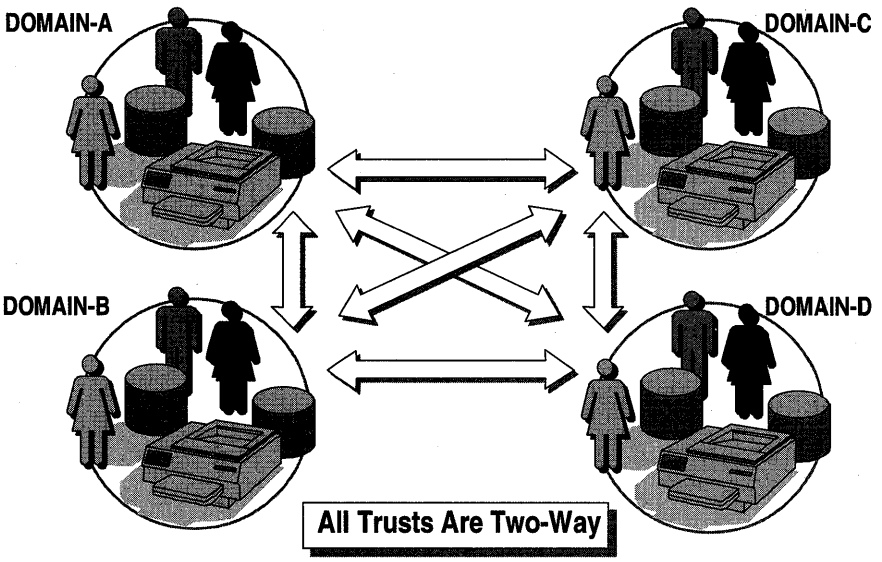


Figure 66: The complete trust domain model

The following table summarizes the advantages and disadvantages of using a complete trust model.

Advantages	Disadvantages
Best for companies with no central MIS group.	Because there is no central management of users, this model is impractical for companies with central MIS departments.
Scalable to networks with any number of users.	Very large number of trust relationships to manage.
Each department has full control over its user accounts and resources.	Each department must trust that the other departments will not put inappropriate users into global groups.
Both resources and user accounts are grouped into departmental units.	

In the complete trust model, every domain on the network trusts every other domain. Each department manages its own domain and defines its own users and global groups. These users and global groups can be used on all domains in the complete trust model.

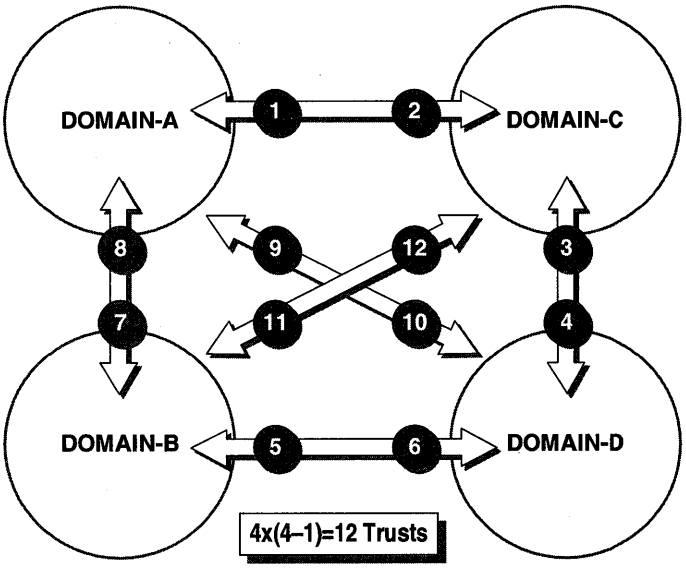


Figure 67: Trust relationships in a complete trust domain

Determining the Number of Trusts

The number of trust relationships required for a company with *n* domains is:

$$n * (n-1)$$

For example, 4 domains require 12 trust relationships (4 x [4 – 1]), and 10 domains require 90 trust relationships. Adding a new domain to an existing network of 10 domains requires establishing 20 new trust relationships.

Security

Because there is no central administration in the complete trust model, users from other domains with access to resources could pose a security risk.

This model requires a high degree of confidence in global groups from other trusted domains. When you give permissions to a global group from another domain (or place that global group in a local group in your domain), you are trusting the administrator of the other domain not to add any unauthorized or inappropriate users to that global group.

Implementing a Complete Trust Model

The complete trust model is an extension of a two-way trust relationship between two domains. In Lesson 4, you created a two-way trust relationship between DOMAIN-A and DOMAIN-B.

If you had more than two domains, you would be able to implement the complete trust model fully by configuring your additional domains. To do this, you would:

- Create a two-way trust relationship between each of your additional domains and DOMAIN-A.
- Create a two-way trust relationship between each of your additional domains and DOMAIN-B.
- Create two-way trust relationships between each of your additional domains.

You would then be able to sit at any computer, in any of these domains, log on to the domain that contained your user account, and access any resource in any of the domains to which your account has been given permissions.

Lesson Summary

The complete trust model allows decentralized account and resource management while allowing users to access any resource in the model to which they have been given permissions. In this model, the management of trust relationships is critical.

For more information on	See
Complete Trust Model	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide*.

Lesson 6: Group Strategies Across Domains

Using local and global groups across domains is one way to make your network easier to administer and maintain. In Chapter 2, we presented a strategy for using global and local groups in a single domain. In this lesson you review some of the group strategy concepts that you learned in Chapter 2, and then apply them to a multiple master domain.

At this point your network configuration should be a multiple master domain using trust relationships. Keep in mind that your group strategy can be the same regardless of the domain model you implement.

After this lesson you will be able to:

- Plan a group strategy for any domain model.
- Describe the role of trust relationships when planning group strategies.

Estimated Completion Time: 15 minutes

Planning a Group Strategy

In a multiple domain environment with trust relationships, keep in mind the following guidelines when implementing groups:

1. Determine what you need to accomplish. Is it one of the following?
   - A network responsibility (assigning administrative tasks, creating users)
   - Assigning permissions to resources
2. Use built-in global and local groups where possible. Determine whether there is an existing group that can perform the task.
3. At the primary domain controller of any trusted domains, create any new user accounts and global groups that are necessary.
4. At the primary domain controller of any trusted domains, assign the appropriate users to existing or newly created global groups for domain-wide and multi-domain access.
5. At your domain or trusting domains, create any new local groups where needed.
6. At your domain or trusting domains, add global groups from trusted domains to the appropriate local groups.
7. At your domain or trusting domains, assign the local group to user rights and resource permissions.

After you have a group strategy, you are ready to implement it.

The Role of Trusts

As suggested in the previous strategy, when there are trust relationships between domains, global groups in a trusted domain can become members of a local group in a trusting domain. The trusting domain local group can then be assigned permissions to resources, or administrative tasks, in the trusting domain. The effect of this strategy is that the members of the global group from the trusted domain have the permissions that are granted to the local group in the trusting domain.

After you understand the relationship between local and global groups, and trust relationships, you can plan a group strategy that improves the efficiency of your network administration. The key is knowing that global groups from a trusted domain join a local group in a trusting domain.

▶ To administer domains across trusts

In these procedures, you allow a user to administer both the trusted and the trusting domains. Given a scenario, you design and implement group membership to allow administration of multiple domains across a trust relationship.

Scenario

User Admin-A is a member of DOMAIN-A's Domain Admins group. Admin-A has just been promoted from Domain Administrator to Network Administrator. Admin-A now needs to administer both DOMAIN-A and DOMAIN-B. In addition, all of the DOMAIN-A administrators need to administer DOMAIN-B. DOMAIN-B trusts DOMAIN-A.

▶ To design group membership

1. Why is Admin-A currently able to administer DOMAIN-A?

2. Write the steps you would use to allow all administrators of DOMAIN-A to administer DOMAIN-B.

▶ To implement a group membership

Important Complete this procedure logged on as DOMAIN-B\Administrator from the PDC of DOMAIN-B.

- Use User Manager for Domains to add the DOMAIN-A\DOMAIN ADMINS global group to the DOMAIN-B\ADMINISTRATORS local group.

► To test the administration capability

In this procedure you test Admin-A's ability to administer DOMAIN-B. You use Server Manager to view shared resources. Only members of Administrators and Server Operators can view shared resources.

Important Complete this procedure from the PDC of DOMAIN-B.

1. Log off, and then log on to DOMAIN-A as Admin-A.
2. Open Server Manager.

   Notice that the title bar of Server Manager indicates DOMAIN-A.
3. Select PDC-A.
4. From the Computer menu, select Shared Directories.
5. Were you successful in viewing the shared directories? Why or why not?

6. Choose Close.

   You now select the trusting domain to administer in Server Manager.
7. From the Computer menu, choose Select Domain.

   The Select Domain dialog box appears.
8. Under Select Domain, select DOMAIN-B, and then choose OK.

   Notice that the title bar of Server Manager now indicates DOMAIN-B.
9. From the Computer menu, select Shared Directories.
10. Were you successful in viewing the shared directories? Why or why not?

11. Choose Close.

Lesson Summary

In a multiple domain environment with trust relationships, group strategies are similar to what we saw in Chapter 2. We still suggest putting Users into Global Groups, Global Groups into Local Groups. However, across trust relationships, the global groups are defined on the trusted domains and the local groups exist in all domains. The appropriate use of trust relationships, and global and local groups, can easily centralize administration in a multiple domain environment.

For more information on	See
Group strategies	Chapter 3, "How Network Security Works" in the *Microsoft Windows NT Concepts and Planning Guide.*

For online information about	From the Help menu, choose Contents and then
Managing local groups	User Manager for Domains Help, Manage Local Groups
Managing global groups	User Manager for Domains Help, Manage Global Groups
Manage shared directories	Server Manager Help, Manage Shared Directories

Lesson 7: Trust Relationship Issues

Various problems can arise while creating and maintaining trust relationships. This lesson gives you an overview of some of the most common issues and how to solve them.

After this lesson you will be able to:

- Identify common problems and issues related to establishing and maintaining trust relationships.

Estimated Completion Time: 10 minutes

The following is a list of common trust relationship issues and possible solutions:

Issue	Possible solution
Cannot establish a trust relationship.	Verify that the primary domain controllers in each domain are running.
	Verify that no session exists with the primary domain controller.
	Verify that the correct password was supplied.
Cannot verify the trust relationship.	To receive verification, the trusted domain must permit the trusting domain before the trusting domain can attempt to establish the trust relationship.
A trust relationship is broken.	If a trust relationship is broken, trusted accounts will no longer be available for use. Reestablish the trust relationship.
Cannot reestablish a broken trust.	Microsoft Windows NT Server will automatically change the initially assigned password after the trust relationship has been established. You must break the trust from both domains, and then reestablish it as if it were a new relationship.
Cannot use trusted accounts.	The trust relationship might have been established in the wrong direction. Break the existing relationship, and have the trusted domain permit the trusting domain, and the trusting domain to trust the trusted domain.
	Possible broken trust. Reestablish.

(continued)

Issue	Possible solution
Cannot administer another domain.	Verify that the trusted domain's Domain Admins group has been added to the local Administrators group.
Access is denied when using a trusted account.	Check to see whether the same account name exists in both domains. In a trust relationship, each account should appear in only one domain, the trusted domain or the local domain, not in both.
Can access other domain resources when using a local account.	Check to see whether the same account name exists in both domains. In a trust relationship, each account should appear in only one domain, the trusted domain or the local domain, not in both.

Lesson Summary

In this lesson you reviewed some of the common issues that can arise when establishing trust relationships. In most of the cases presented here, the issues involved using incorrect names or passwords, or establishing trust relationships in the wrong sequence.

For more information on	See
Trust Relationships	Chapter 3, "How Network Security Works," in the *Microsoft Windows NT Server Concepts and Planning Guide*.

CHAPTER 6

Protecting Server Data

Before You Begin

Before starting this chapter, you must have completed Chapter 1. In addition, to complete the procedures in this chapter you must have:

- A minimum of two hard disks to do disk mirroring; the second hard disk must have an area of unpartitioned disk space equal to the size of drive C.
- A minimum of three hard disks to do striping with parity; each disk must have a minimum of 5 MB unpartitioned disk space.

If you do not have the appropriate equipment to complete the exercises in this chapter, you can still learn the concepts and procedures presented.

Lesson 1: Introduction to Fault Tolerance

In this lesson you learn about the tool for protecting data that is provided with Windows NT Server, the Disk Administrator program in the Administrative Tools group.

The Windows NT Server version of Disk Administrator includes the common organizational tools (volume sets and stripe sets) and then adds the data protection tools (mirror sets and stripe sets with parity). Additionally, Windows NT Server provides an automatic data protection service, which fixes sector failures (sector sparing).

After this lesson you will be able to:

- Compare features of the various fault tolerance options.
- Identify which levels of Redundant Arrays of Inexpensive Disks (RAID) are supported by Windows NT Server.
- Select the option best suited for your needs.

Estimated Completion Time: 35 minutes

Fault Tolerance Features of Windows NT Server

In the event of a system failure, the downtime spent recovering data can result in lost business opportunities and severe financial losses. Windows NT Server provides tools to protect data so that failure of a hard drive will not lead to system failure. These data protection tools are known as fault tolerance options.

Fault tolerance options protect data by duplicating data or placing data in different physical sources, such as different partitions or different disks within an array (a grouping of disk drives used to create fault tolerance options). Data redundancy allows access to data even if part of your data system fails. This redundancy is a prominent feature common to most fault tolerance options.

Windows NT Server offers three types of software-based fault tolerance options:

- Disk mirroring
- Disk striping with parity
- Sector sparing

These three features are covered in detail in this lesson. There are two additional options (not covered here):

- UPS service
- Integrated tape backup utility

Note For additional information on these last two options, see the *Support Fundamentals for Windows NT 3.5: Self-Paced Training* book.

Redundant Arrays of Inexpensive Disks (RAID) Levels

Fault tolerance options are standardized and categorized into six levels. These levels, level 0 through level 5, are known as Redundant Arrays of Inexpensive Disks (RAID). The levels offer various combinations of performance, reliability, and cost.

Raid Level	Supported by Windows NT Server	Description
Level 0	**Yes**	**Disk striping**
Level 1	Yes	Disk mirroring
Level 2	No	Disk striping with error correction code (ECC)
Level 3	No	Disk striping with ECC stored as parity
Level 4	No	Disk striping large blocks; parity stored on one drive
Level 5	Yes	Disk striping with parity distributed across multiple drives

RAID Software Solutions

Microsoft's Windows NT Server RAID solutions are software-based. Windows NT Server supports RAID levels 0,1, and 5. (Microsoft chose to support the redundant disk striping level 5, as opposed to levels 2, 3, and 4, because it evolved from levels 2, 3, and 4 and is therefore a later, more current version of redundant level disk striping.)

RAID Hardware Solutions

Many computer hardware vendors have built various levels of RAID directly into the computer hardware itself. One way to do this is with disk array controller cards. Whether you decide to implement a hardware or software solution of RAID will depend on your particular requirements and the results wanted. Advantages and disadvantages of hardware implementations of RAID follow.

Hardware RAID Advantages

Some advantages are as follows:

- Because these methods are vendor-specific and bypass the Windows NT Server software drivers, they can offer performance improvements.
- Some hardware implementations allow you to replace a failed drive without shutting down the system.

Hardware RAID Disadvantages

Some disadvantages are as follows:

- It can be very expensive.
- It can lock you into a single-vendor solution.

Let's take a look now at the three levels of RAID that are supported by Windows NT Server.

Level 0—Disk Striping

In RAID level 0, disk striping divides data into 64K blocks and spreads it equally, in a fixed rate and order, among all disks in an array. The entire configuration of data spread across all the disks in the array is called a *stripe set*. Disk striping does not provide any fault tolerance because there is no data redundancy.

Note To implement disk striping, you need a minimum of two hard disks. As many as 32 hard disks can be supported.

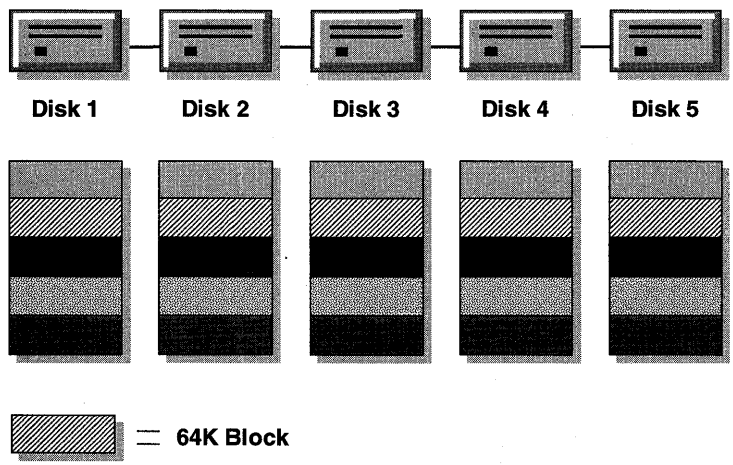


Figure 68: Disk striping across disks in an array

Be aware that, if any disk in the stripe set fails, all data is lost. This is an obvious drawback to Level 0.

Though Level 0 disk striping does not offer data protection, there are several good reasons for using it:

- It allows you to take a number of small partitions and make one large partition for better utilization of hard disk space.
- By adding multiple disk controllers you can achieve improved performance.
- You might need to use this method of distributing data because of your system requirements. For example, if you have only two partitions of 50 MB each, and you need to install an application that requires 100 MB, you can create a stripe set and utilize all 100 MB as a single partition.

Level 1—Disk Mirroring

Disk mirroring is an actual duplication of a partition. Disk mirroring can be considered a form of *continual backup* because it maintains a *fully redundant* copy of a partition on another disk. Any partition, including the boot and system partitions, can be mirrored.

Note To implement disk mirroring, you need a minimum of two hard disks.

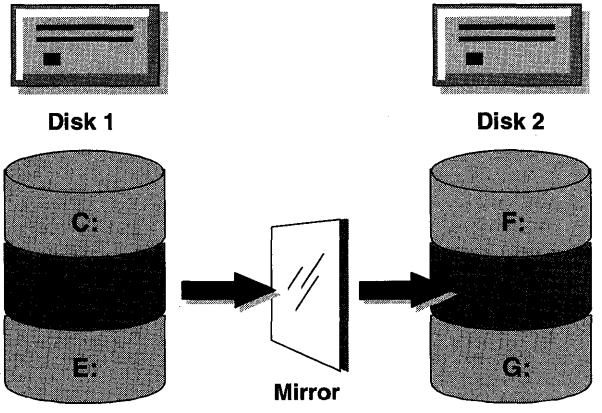


Figure 69: Disk mirroring

There are advantages and disadvantages to disk mirroring:

- This strategy is the simplest way of protecting a single disk against failure. It is simplest because it requires only two hard disks and it is easy to set up. (From Disk Administrator, select first partition, select free space, and then choose Establish Mirror.)
- Since it provides protection from the downtime involved in recovering lost data and restoring data from a backup storage facility, it can save on expenses.
- For peer-to-peer and small- to medium-sized server-based LANs, disk mirroring usually has a lower entry cost because it requires only two disks.
- However, in terms of dollars per megabyte, disk mirroring is more expensive than other forms of fault tolerance, because disk space utilization in disk mirroring is only 50 percent.

Disk Duplexing

Disk duplexing takes a mirrored pair of disks and adds an *additional* disk controller for the second drive.

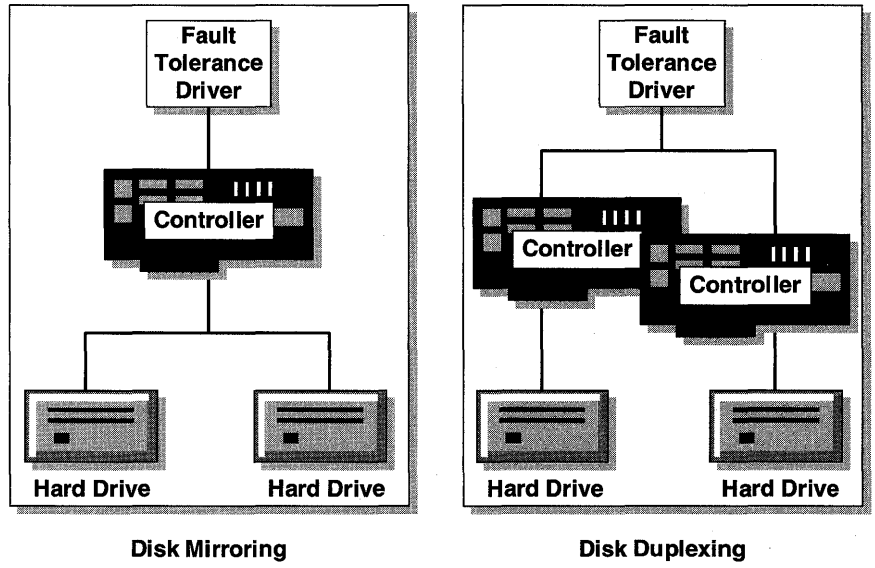


Figure 70: Disk duplexing, showing the addition of a second controller

Disk duplexing adds additional benefits to disk mirroring:

- By having redundant controllers, duplexing protects against controller failures as well as media failures.
- When performing read or write operations, having two controllers reduces channel traffic, which can result in significantly improved performance.

No additional configuration is needed to implement disk duplexing. When you establish a mirror set, if the disks you select have different controllers, disk duplexing will be automatically implemented.

Level 5—Striping with Parity

Striping with parity is currently the most popular approach to fault tolerance design. It differs from other levels by writing parity information across *all* disks in an array (the entire stripe set). The data and parity information are arranged so that the two are always on different disks.

Note In a stripe set with parity, a minimum of three to a maximum of 32 drives are supported.

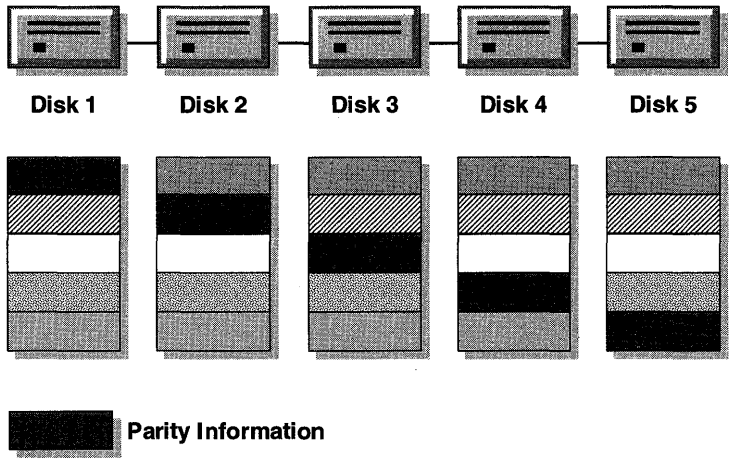


Figure 71: Striping with parity, showing parity information stored on each disk

A parity stripe block exists for each stripe (row) across the disk. The parity stripe block is used to reconstruct data for a failed physical disk.

If a single disk fails, enough information is spread across the remaining disks to allow the data to be completely reconstructed. For example, in Figure 4, if Disk 3 fails and needs to be replaced, data for the new disk can be regenerated using the data and parity information in each stripe on the remaining four disks.

All partitions, except the boot or system partition, can be part of a stripe set with parity.

Advantages and disadvantages of striping with parity

- Stripe sets with parity offer the best performance for read operations.
- However, when a disk has failed, the read performance is degraded by the need to regenerate the data using the parity information.
- Also, all normal *write* operations require three times as much memory due to the parity calculation.

Disk Mirroring vs. Striping with Parity

As you can see, there is no one perfect fault tolerance option. There are tradeoffs depending on the level of protection you want. Compare the two methods in the following table.

Disk mirroring	Striping with parity
Supports FAT, HPFS, and NTFS	Supports FAT, HPFS, and NTFS
Can mirror system and/or boot partition	Cannot stripe system or boot partition
Requires two hard disks	Requires three hard disks
Higher cost per megabyte (50% utilization)	Lower cost per megabyte
Good read and write performance	Moderate write performance
Uses less system memory	Excellent read performance
	Requires more system memory
	Supports up to 32 hard disks

The major differences between disk mirroring and striping with parity are performance and cost. Let's take a closer look.

Disk Mirroring

- Overall, disk mirroring offers better I/O performance on writes.
- It also has the advantage of being able to mirror either boot or system partitions.
- However, because mirroring utilizes only 50 percent of available disk space, it tends to be more expensive in cost per megabyte. As hard disk prices decrease, these costs will become less significant.

Disk Striping with Parity

- Disk striping with parity offers better read performance than does mirroring. This is especially true of multiple controllers, because data is split among multiple drives and can be read simultaneously from all of the drives.
- However, the need to calculate parity information requires more system memory, and this can slow down *write* performance considerably.
- The cost per megabyte will be lower with striping because disk use is much greater. For example, if there are four disks in a stripe set with parity, the overhead in terms of disk space is 25%, as opposed to 50% with mirroring.

Note For more information, see Chapter 7, "Managing Fault Tolerance and UPS," in the *Windows NT Server Concepts and Planning Guide.*

Sector Sparing

In addition to supporting the fault tolerance options in RAID, Windows NT Server adds another fault tolerance service. Sector sparing, commonly known as "hot fixing," automatically adds sector-recovery capabilities to the file system during operation.

Note It is possible for Small Computer System Interface (SCSI) devices to perform sector sparing, but IBM® PC/AT® devices (ESDI and IDE) cannot do this.

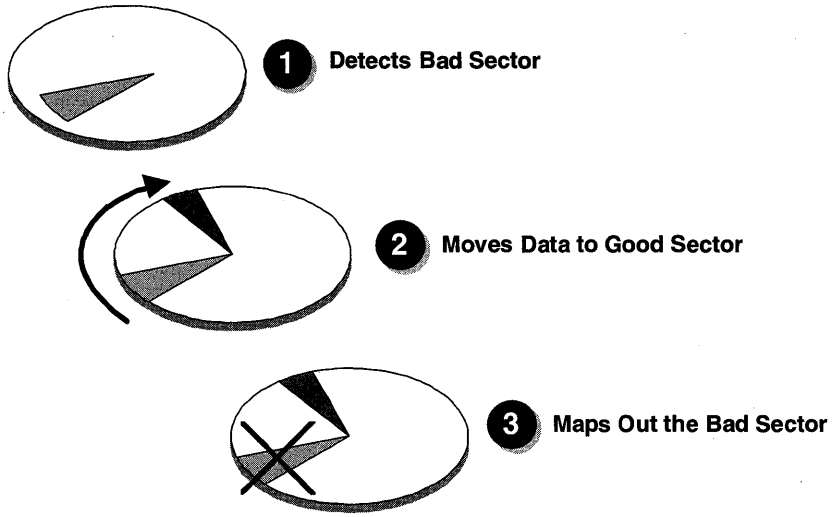


Figure 72: Sector sparing ("hot fixing") steps

Whenever a volume is formatted, the file system will verify the sectors in the partition and spare any bad sectors from use. The Windows NT Server fault-tolerant services go beyond this level of sector sparing to implement sector sparing whenever data is read from or written to a sector.

How Sector Sparing Works

In a fault-tolerant system with redundant copies of data, all read/write operations to the hard disk are verified. If a sector failure is detected, the following steps occur.

1. The Windows NT Server Fault Tolerance driver removes the data from the bad sector and places it in a good sector.
2. The driver maps out the bad sector. If the mapping is successful, the file system is not alerted of the problem.
3. Additionally, the fault tolerance driver asks the device driver to obtain the data from the new sector (where the data was written).

As administrator, you are notified through the Event Viewer program of:

- All sector failures handled by the Windows NT Fault Tolerance driver.
- The potential for data loss if the redundant copy also fails.

In the next lesson, you learn how to implement fault tolerance options.

Lesson Summary

To assist in protecting valuable hard disk data, Windows NT Server provides disk mirroring, striping with parity, and sector sparing.

Review Questions

The following review questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You are planning to implement disk striping with parity after installing Windows NT Server. With this in mind, why would you possibly not want to place application data on one large partition with the Windows NT system files?

2. You have heard that Windows NT Server supports RAID and wonder which fault-tolerant options you can implement with your server installation.

3. Which partitions cannot be included in a stripe set?

4. List three differences between striping with parity and mirroring.

For more information on	See
RAID levels	Chapter 7, "Managing Fault Tolerance and UPS," in the Microsoft Windows NT Server Concepts and Planning Guide.
Windows NT fault-tolerant options	Chapter 8,"Managing Hard Disks, Fault Tolerance, and UPS," in the Microsoft Windows NT Network Operations Quick Reference.

Lesson 2: Implementing Fault Tolerance

Now that you know the different kinds of fault tolerance options, you are ready to configure them for your disks using Disk Administrator.

Disk Administrator is the tool that manages the hard disk(s) by creating, deleting, and formatting partitions; creating, extending and deleting volume sets; creating and deleting stripe sets; and implementing the fault tolerance features of Windows NT Server.

To use Disk Administrator you must be logged on as a user account with administrative privileges.

After this lesson you will be able to:

- Identify the hard disk management capabilities of Disk Administrator.
- Implement disk mirroring.
- Implement disk striping with parity.

Estimated Completion Time: 25 minutes

Disk Administrator

The Disk Administrator program is the primary tool used to configure Windows NT Server fault tolerance. The graphical interface of Disk Administrator makes it easy to configure and manage disk partitioning and fault tolerance options.

A typical Disk Administrator screen looks like this:

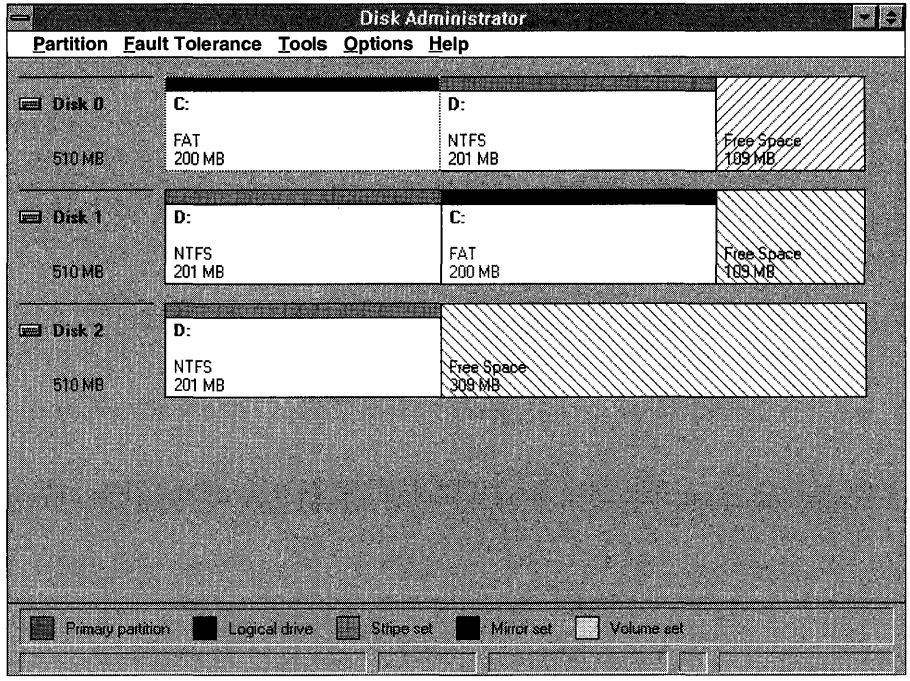


Figure 73: Disk Administrator dialog box

Note In the previous figure, drive D is a stripe set with parity, and drive C is mirrored.

Disk drives can have various configurations, including:

- Volume sets which accumulate multiple disk areas into one large partition, filling the areas in sequence.
- Stripe sets which accumulate multiple disk areas into one large partition, distributing data storage across all drives simultaneously.
- Stripe sets with parity which accumulate multiple disk areas into one large partition, distributing data storage across all drives simultaneously, adding fault tolerance parity information.
- Mirror sets which make an exact duplicate of one partition and place it onto a separate physical disk.

Note For more information on volume sets and stripe sets, see the *Support Fundamentals for Windows NT 3.5: Self-Paced Training* book.

Common Disk Administrator Procedure

When using Disk Administrator, there is a common procedure for creating volume sets, stripe sets, stripe sets with parity, and mirror sets. The options you choose to implement can differ, but knowing this common procedure makes implementation of other features easy.

1. Select the first area of disk space. For mirroring, this is an existing partition. For volume and stripe sets, this is free disk space. Free disk space is defined as disk space that is not partitioned or formatted.
2. While pressing the CTRL key, select other area(s) of free disk space to be used in the set.
3. From the Partition (volume set or stripe set) or Fault Tolerance (mirror set or stripe set with parity) menu, choose the appropriate option.
4. Complete the configuration by supplying any additional information, such as total size of partition.

After these steps are completed, you must shut down and restart Windows NT Server to use the new feature.

Implementing Fault Tolerance Options

To implement fault tolerance, your computer must meet certain system requirements.

Implementing Disk Mirroring

To use the disk mirroring feature of Windows NT Server, you need a computer with a minimum of two hard disks. The second hard disk must have free disk space (an unpartitioned area) at least as large as the partition to be mirrored on the first disk. For example, if you want to mirror drive D on the first physical disk drive, which is 100 MB in size, then the second physical disk drive must have an area of free disk space that is at least 100 MB in size.

The system and boot partition(s) can be mirrored with Windows NT Server. Both hard disks can be of different types, such as SCSI, ESDI, or IDE. Any file system (FAT, HPFS, or NTFS) can be mirrored.

► To configure disk mirroring

Important Complete this procedure logged on as Administrator on the computer that has a minimum of two hard disks with available space for configuring the mirror set.

1. From the Administrative Tools group, start Disk Administrator.

   The Disk Administrator window appears.
2. On Disk 0, select the C: partition.
3. Hold down the CTRL key, and then click an area of free space on another disk. The area must be equal to or greater than the partition selected in the preceding step.
4. From the Fault Tolerance menu, choose Establish Mirror.

   A Disk Administrator message box appears, indicating that you are mirroring the system boot partition.
5. Choose OK.

   The partitions should now have the same drive letter and be highlighted in purple. This indicates that they are part of a mirror set.
6. From the Partition menu, choose Exit.

   A Confirm message box appears, prompting you to save the changes.
7. Choose Yes to keep the mirror set. If you do not want to keep the mirror set, choose No, and then skip the remaining steps in this procedure.

   A Confirm message box appears, indicating that you must restart the computer.
8. Choose Yes.

   A Disk Administrator message box appears, indicating that you should update the Emergency Repair disk to reflect the new disk configuration.
9. Choose OK.

   A Disk Administrator message box appears, indicating that you must restart the computer.
10. Choose OK to initiate shutdown and restart.
11. Log on as Administrator.
12. Start Disk Administrator.

    Notice that the text in the mirror of drive C is red, indicating that the mirror is currently being generated.

13. Select the mirror of drive C. Notice the status at the bottom left of the display. It is labeled Mirror set #x (INITIALIZING), where x is the number of your mirror set. When the mirror is completed, the INITIALIZING will change to HEALTHY, and the text in the mirror of drive C will change from red to black.
14. Close Disk Administrator.

Implementing Striping with Parity

To use the striping with parity feature of Windows NT Server, you need a computer with a minimum of three hard disks. Each hard drive must have free (unpartitioned) disk space available. For example, when using three hard disks to create a stripe set with parity that is a minimum of 120 MB of usable disk space, you must have a minimum of 60 MB free disk space on each hard disk. If the partitions are not of equal size, Disk Administrator will create the stripe set with parity using equal-sized partitions that are a multiple of the smallest partition in the set.

The system and boot partition(s) cannot be part of a stripe set with parity with Windows NT Server. Each hard disk can be one of different types, such as SCSI, ESDI, or IDE. A stripe set with parity can be formatted with any file system (FAT, HPFS, or NTFS).

► To configure disk striping with parity

Important Complete this procedure logged on as Administrator on the computer which has a minimum of three hard disks and available space for configuring the stripe set with parity. Each area of free disk space must be a minimum of 5 MB.

1. From the Administrative Tools group, start Disk Administrator.
2. Select an area of free space on the first disk to be used for creating a stripe set with parity.
3. Hold down the CTRL key, and then select a minimum of two additional areas of free space located on at least two other disks.
4. From the Fault Tolerance menu, choose Create Stripe Set With Parity.

   The Create Stripe Set With Parity dialog box appears. The default size is three times the size of the smallest area of selected free space.
5. Select the size of the stripe set, and then choose OK.

   The partitions now have the same drive letter and are highlighted in green. This indicates that they are part of a stripe set with parity.
6. From the Partition menu, choose Exit.

   A Confirm message box appears, prompting you to save the changes.

7. Choose Yes to save the stripe set with parity. If you do not want to save the stripe set with parity, choose No, and then skip the remaining steps in this procedure.

   A Disk Administrator message box appears, indicating that you should update the Emergency Repair disk to reflect the new disk configuration.

8. Choose OK.

   A Disk Administrator message box appears, indicating that you must restart the computer.

9. Choose OK to initiate shutdown and restart.
10. Log on as Administrator.
11. Format the stripe set as a FAT, HPFS, or NTFS partition using Disk Administrator or the command prompt.

Lesson Summary

Windows NT Server allows the administrator to implement striping with parity or disk mirroring to provide redundant data for protection against data loss. Both can be implemented using Disk Administrator from the Administrative Tools group of Program Manager.

Review Question

The following review question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- You want a user to create a mirror set on her Windows NT Server computer to protect it from data loss. What must you do so that the user is able to implement the mirror set?

For online information about	From the Help menu, choose Contents and then
Creating a mirror set	Disk Administrator Help, Establish and Break Mirror Sets
	Disk Administrator Help, Fault Tolerance Commands, Establish Mirror
Creating a stripe set with parity	Disk Administrator Help, Create and Delete Stripe Sets with Parity
	Disk Administrator Help, Fault Tolerance Commands, Create Stripe Set with Parity

Lesson 3: Recovering Data

The process you use to recover data depends on which fault tolerance option you have configured, and on whether the loss is due to failure of a *member* of a partition or due to failure of the *system* partition.

After this lesson you will be able to:

- List the steps in fixing a mirror set.
- Describe the process of regenerating a stripe set with parity.
- Describe ARC naming conventions.
- List the four steps in creating a fault tolerance boot disk.

Estimated Completion Time: 20 minutes

Partition Failures: Member of a Mirror Set or of a Stripe Set with Parity

A *member* of a mirror set or stripe set with parity is one of the physical disk partitions that make up the set. When a member of a mirror set or a stripe set with parity fails (as in a disk crash), the Fault Tolerance driver directs all I/O to the remaining members of the fault-tolerant volume. This ensures continuous service at least until the system is restarted.

Fixing a Mirror Set

When a member of a mirror set fails, you must:

1. Break the mirror set relationship to expose the remaining partition as a separate volume.
2. Then, if it is not done automatically, assign to the exposed *working* member of the mirror set the drive letter that was previously assigned to the complete mirror set.
3. Assign to the *failed* partition the next available letter or any available drive letter.

   You can then use free space on another disk to create a new mirror set relationship.

   When the computer is restarted, the data from the good partition is copied to the new member of the mirror set.

► To break a mirror set

Important To complete this procedure, you need a disk mirror set on your computer. Complete this procedure logged on as Administrator.

1. Start Disk Administrator.
2. Select drive C (the mirror set), and then from the Fault Tolerance menu, choose Break Mirror.

   A Confirm message box appears, prompting you for confirmation.
3. Choose Yes.

   Notice that the "mirrored" partition receives the next available drive letter.
4. From the Partition menu, choose Commit Changes Now.

   A Confirm message box appears, prompting you to save the changes.
5. Choose Yes.

   A Disk Administrator message box appears, indicating you should update the Emergency Repair disk.
6. Choose OK.
7. From the Partition menu, choose Exit.
8. Start File Manager, and then select the "new" drive (the drive that was created from breaking the mirror set).

   Notice that it is an exact duplicate of drive C. You have broken the mirror set.
9. Exit File Manager.

Regenerating a Stripe Set with Parity

When a member of a stripe set with parity fails, you can continue to use the computer and access all data. However, you will be regenerating data in RAM, as it is needed, and system performance could degenerate.

To return the computer to its normal state after a member of a stripe set with parity has failed, you can regenerate the data for the failed member from the *remaining* members:

1. Using Disk Administrator, select the stripe set with parity; and then select a new area of free space (on a different hard disk) that is the same size as, or larger than, the other members of the stripe set with parity.
2. Choose the Regenerate command from the Fault Tolerance menu.

When you restart the computer, the fault tolerance driver reads the information from the stripes on the other member disks. It then recreates the data of the missing member and writes the recreated data to the new member.

Partition Failures: System Partitions

If the failure involves the *system partition* on the primary physical drive, a fault tolerance boot disk is required to restart the system. Creating this boot disk involves using certain naming conventions.

Understanding ARC Names

To set up the boot information for recovery of a boot or system disk, you have to understand how Advanced RISC Computing (ARC) names are constructed. ARC naming conventions are a generic method for identifying devices on *x86* and RISC-based computers. In the following example, you see components of an ARC name.

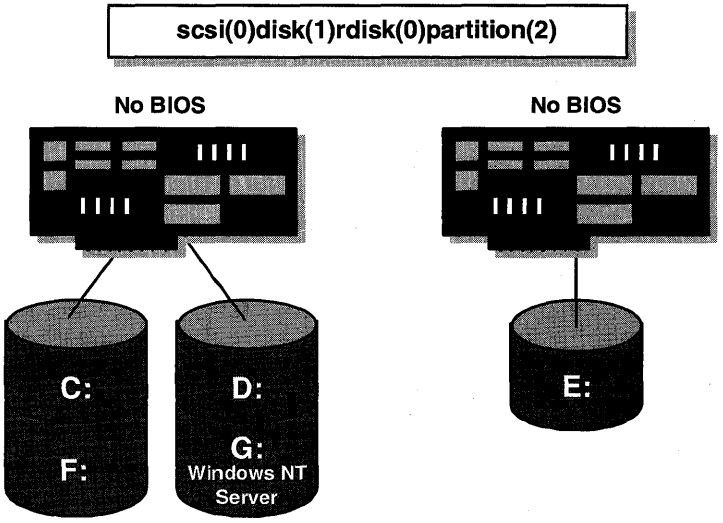


Figure 74: An ARC name

Type of Disk Controller

The first part of the ARC name identifies the hardware adapter/disk controller.

scsi(0)disk(1)rdisk(0)partition(2)

The two valid options are *SCSI* and *multi.* In this example, it is *SCSI. SCSI* indicates a SCSI disk on which SCSI BIOS is not enabled; *multi* indicates a disk other than SCSI or a SCSI accessed by the SCSI BIOS. For Windows NT Server, this could be a disk supported by the Atdisk driver, or one supported by Abiosdsk or Cpqarray.

Ordinal Number of the Hardware Adapter

Following the disk controller identifier is the ordinal number for the hardware adapter. This refers to the physical controller in the computer.

scsi(**0**)disk(1)rdisk(0)partition(2)

In this example, the ordinal number is 0, indicating the first SCSI controller. SCSI() always starts with 0.

Disk Parameters

Next are the disk parameters.

scsi(0)**disk(1)rdisk(0)**partition(2)

The designation **disk()** refers to the hard drive of the controller you are using. SCSI notation varies the disk() parameter for successive disks on one controller; the disk number is always zero if it is multi. For example, disk(0) indicates the disk with a SCSI target ID of 0.

The designation **rdisk()** refers to the ordinal number of the disk you are using. Multi format varies the rdisk() parameter, while rdisk is ignored for SCSI controllers.

Both the disk() and rdisk() parameters start at 0.

Partition Number

Finally, the *partition()* parameter of the ARC name refers to the partition number. Partition numbers are assigned starting with *partition(1). Partition(0)* is special and refers to the entire disk.

scsi(0)rdisk(1)disk(0)**partition(2)**

All *primary* partitions are first assigned numbers. (Primary partitions are partitions that are designated to hold operating systems and possibly to start the computer.) Then, all logical drives in *extended* partitions are assigned numbers. (An extended partition cannot be used to start the computer, but it can be subdivided into multiple smaller components referred to as logical drives. A drive can contain four partitions, only one of which can be extended.)

To return to the original graphic, this is what the ARC name looks like with all corresponding components identified:

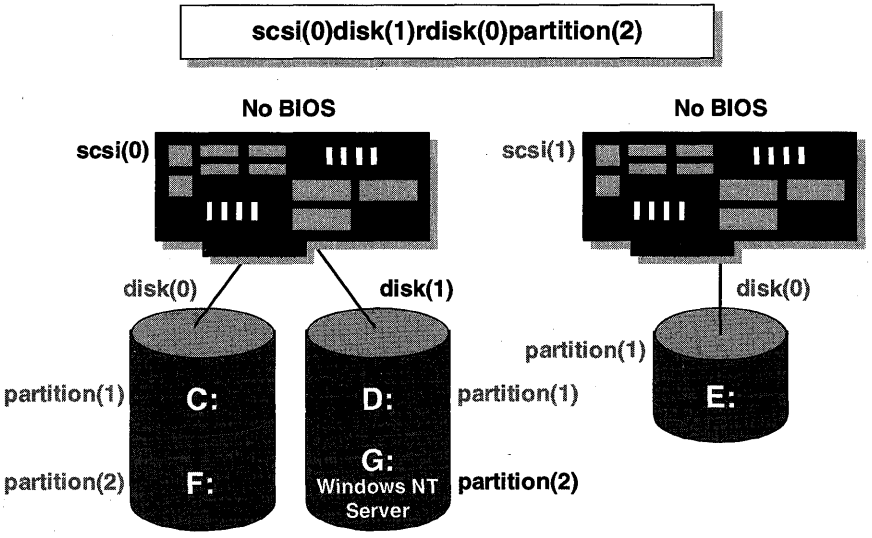


Figure 75: An ARC name with all components identified

Creating a Fault Tolerance Boot Disk

A fault tolerance boot disk is the key to recovery in case of a physical disk failure. You should create this boot disk whenever you are mirroring the boot partition of a computer running Windows NT Server. This disk can be created any time when the computer is online.

The steps to create this boot disk are as follows:

1. Format a floppy disk using Windows NT Server. This writes information to the boot track of the floppy disk so that it will look for the appropriate loader file when the system is started.

2. Copy the necessary files, in the following list, from the primary partition of your Windows NT Server computer to the boot disk. Several of the files are normally hidden in the root directory. File Manager or the ATTRIB command will show the files.

x86-based computers	RISC-based computers
NTLDR	OSLOADER.EXE
NTDETECT.COM	HAL.DLL
NTBOOTDD.SYS (for SCSI disks not using SCSI BIOS)	
BOOT.INI	

Note The NTBOOTDD.SYS file appears only on SCSI systems in which the SCSI BIOS is not used.

3. Modify BOOT.INI so that it points to the mirrored copy of the boot partition. Whenever partition information is changed, it is important to update the BOOT.INI file. Knowledge of ARC names is essential in this situation.
4. Test the boot disk to ensure that it works and will boot using data from the mirrored copy of the boot partition.

Note For more information see Chapter 7, "Managing Fault Tolerance and UPS," in the *Windows NT Server Concepts and Planning Guide*.

Recovering a Mirror Set

If the *system* partition in a mirror set fails, the mirror set is no longer bootable. However, the data is not lost; it can be recovered because the *boot* partition, where you store the system files, is still accessible. Recovering a mirror set is accomplished by following these steps:

1. Replace the bad drive.
2. Boot the system with a Windows NT boot disk that loads Windows NT Server from the mirrored partition.
3. Break the existing mirror.

4. Reestablish the mirror to the new drive.
5. Reboot the system without the floppy disk.

Note The Windows NT boot disk cannot be created while the system is down. It must be created before failure occurs. It can be created on another computer running Windows NT Server with an identical configuration.

Lesson Summary

The ability to protect data on a hard disk is important, especially for a network file server. It is also important to be able to recover data in the event that the failed hard disk happens to be the boot drive. This lesson presented methods for recovering data. One of the best ways to ensure that your server can be restarted quickly is to create a Windows NT boot disk. To do so, it is important to understand the ARC naming conventions covered in this lesson.

Review Questions

The following review questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You have decided to establish a mirror set with the system partition of your hard disk, which also contains the Windows NT Server system files. How can you protect yourself in the event that the boot drive becomes inaccessible?

2. Here is an example of an ARC name:

   multi(1)disk(0)rdisk(1)partition(3)

   Draw a picture of what the configuration looks like.

For more information on	See
Recovering data from fault-tolerant systems	Chapter 8, "Managing Fault Tolerance and UPS," in the Microsoft Windows NT Server Concepts and Planning Guide.
	Chapter 18, "Disk Administrator," in the Microsoft Windows NT Server System Guide.
Breaking a mirror set	Chapter 18, "Disk Administrator," in the Microsoft Windows NT Server System Guide.
Understanding ARC names	Chapter 18, "Disk Administrator," in the Microsoft Windows NT Server System Guide.

For online information about	From the Help menu, choose Contents and then
Breaking a mirror set	Disk Administrator Help, Establish and Break Mirror Sets
	Disk Administrator Help, Fault Tolerance Menu Commands, Break Mirror
Regenerating a stripe set with parity	Disk Administrator Help, Regenerate Stripe Set with Parity
	Disk Administrator Help, Fault Tolerance Menu Commands, Regenerate

CHAPTER 7

Installing and Configuring Microsoft TCP/IP on Windows NT Server

Before You Begin

The information in this chapter is intended as an introduction to installing, configuring, and testing Microsoft TCP/IP on Windows NT Server. Detailed information on TCP/IP implementation issues is available in the "Inter-Networking Microsoft TCP/IP on Microsoft Windows NT 3.5" course.

This chapter requires that you have completed Chapters 1–5. Your computers are booted as the primary domain controller of DOMAIN-A (PDC-A) and the primary domain controller of DOMAIN-B (PDC-B).

Lesson 1: Introduction to Microsoft TCP/IP

A significant difference between the Microsoft Windows NT Server operating system and other operating systems is that networking capabilities are built into Windows NT Server.

Because most modern operating systems (including Windows NT) support TCP/IP protocols, an internetwork with mixed system types can share information using simple networking applications and utilities. With TCP/IP as a connectivity protocol, Windows NT can communicate with many non-Microsoft systems.

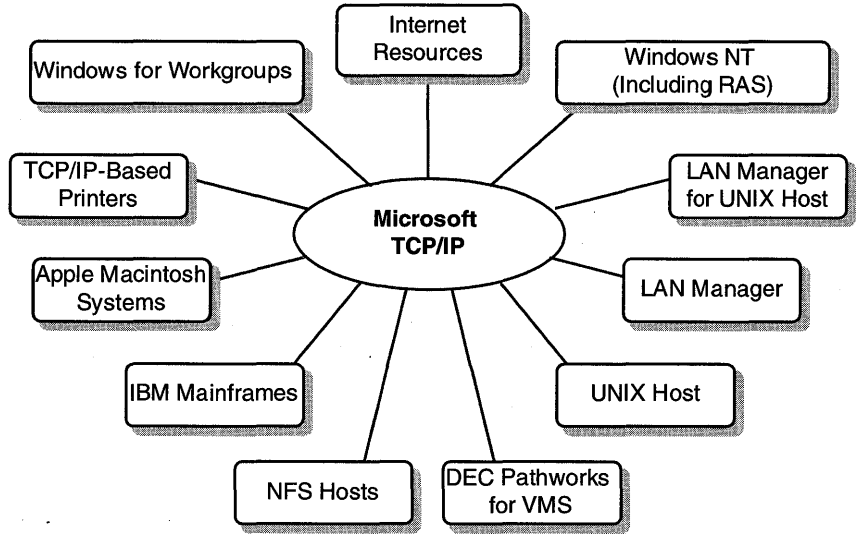


Figure 76: Microsoft TCP/IP connectivity

After this lesson you will be able to:

- Describe the advantages of TCP/IP on Windows NT.

Estimated Completion Time: 5 minutes

What Is TCP/IP on Windows NT?

The Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols designed for wide area networks (WANs). TCP/IP was developed in 1969, by the U.S. Department of Defense Advanced Research Projects Agency, as the result of a research sharing experiment called ARPANET. The purpose of TCP/IP was to provide high-speed communication network links. Since 1969, ARPANET has grown into a worldwide community of networks known as the Internet.

Microsoft TCP/IP on Windows NT enables enterprise networking and connectivity on Windows NT–based computers. Adding TCP/IP to a Windows NT configuration offers the following advantages:

- A standard, routable enterprise networking protocol that is the most complete and accepted protocol available. All modern operating systems offer TCP/IP support, and most large networks rely on TCP/IP for much of their network traffic.
- A technology for connecting dissimilar systems. Many standard connectivity utilities are available to access and transfer data between dissimilar systems, including File Transfer Protocol (FTP) and Terminal Emulation Protocol (Telnet). Several of these standard utilities are included with Windows NT Server.
- A method of gaining access to the Internet. The Internet consists of thousands of networks worldwide connecting research facilities, universities, libraries, and private companies.
- A robust, scalable, cross-platform client-server framework. Microsoft TCP/IP offers the Windows Sockets interface, which is ideal for developing client-server applications that can run on Windows Sockets–compliant stacks from other vendors. Windows Sockets applications can also take advantage of other networking protocols such as Microsoft NWLink, the Microsoft implementation of the IPX, SPX, and NetBIOS protocols used in Novell NetWare networks.

Lesson Summary

TCP/IP is an industry standard suite of protocols used for wide area networking. Installing Microsoft TCP/IP on Windows NT provides the ability to connect to a variety of non-Microsoft systems, access the worldwide Internet, and connect multiple physical LANs and route between them.

For more information on	See
Microsoft TCP/IP Protocols, Utilities, and Services	Chapter 1, "Overview of Microsoft TCP/IP for Windows NT," in the *Microsoft Windows NT Server TCP/IP* documentation.

Lesson 2: Installing and Configuring Microsoft TCP/IP

In this lesson, you learn how to install Microsoft TCP/IP on a computer running Windows NT Server, and then you manually configure an IP address, subnet mask, and default gateway.

After this lesson you will be able to:

- Identify and describe the configuration parameters required to install Microsoft TCP/IP.
- Install Microsoft TCP/IP on a computer running Windows NT Server.
- Configure the IP address, subnet mask, and default gateway parameters manually.

Estimated Completion Time: 20 minutes

TCP/IP Configuration Parameters

Before you install Microsoft TCP/IP, it is important to know the required configuration parameters. If you are installing Windows NT Server in a routed network environment, there are three parameters required for each computer running TCP/IP: IP address, subnet mask, and default gateway.

IP Address

Every host interface on a TCP/IP network is identified by a unique IP address. This address is used to identify a host on a network; it also specifies routing information in an internetwork. An IP address consists of 32 bits divided into four octets, or fields. An address is usually represented in dotted decimal notation, which depicts each octet in its decimal value and separates each octet with a period.

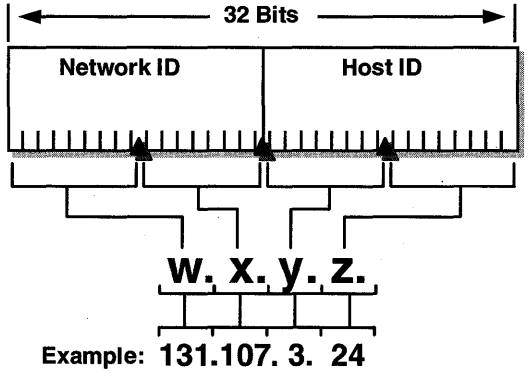


Figure 77: IP Address in dotted decimal notation

The octets are divided into two pairs—the network ID and the host ID (as illustrated in the previous figure). The network ID identifies the physical network. The host ID uniquely identifies a host on a network. When combined, the IP address is used to determine an exact TCP/IP host on a specific IP network.

Because IP addresses identify hosts on an interconnected network, each host on the internetwork must be assigned a unique IP address, valid for its particular network.

If you plan on connecting your network to the worldwide Internet, you must obtain the network ID portion of the IP address from InterNIC to guarantee IP network ID uniqueness. The InterNIC can be contacted through electronic email at info@internic.net (for the United States, 1-800-444-4345 or, for Canada and overseas, 619-455-4600).

If you do not plan on connecting to the worldwide Internet, you can use any valid network ID, which is determined by its address class.

Address Classes

The Internet community has defined multiple address classes to accommodate networks of varying sizes. Windows NT Server supports class A, B, and C networks. The class of address defines the possible number of networks and the number of hosts on a network.

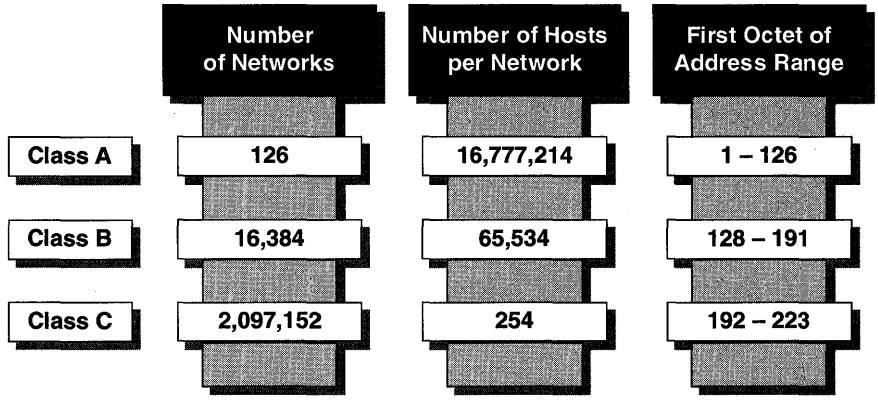


Figure 78: Internet address classes

As illustrated in the previous figure, class A addresses are used for very large networks, class B addresses are used for large networks, and class C addresses are used for small networks. The class of address can be determined by the number in the first octet. For example, an IP address that begins with a decimal value of 150 is a class B address. The host ID can have a decimal value in the range of 0–255.

Note The address 127 is not a valid network ID because it is reserved for loopback testing and interprocess communication on the local computer.

Default Subnet Masks

A subnet mask is used to "mask" a portion of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts communicate, the subnet mask is used to determine whether a host is located on a local or a remote network.

A default subnet mask is used for TCP/IP networks that are not interconnected or that do not use a network ID assigned by the InterNIC. Windows NT Server has a default subnet mask for each address class:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

For example, if your IP address is 131.107.126.88, and your network is a local area network, you use the default subnet mask for a class B address of 255.255.0.0.

Custom Subnet Masks

A custom subnet mask is often required when you have only one network ID. For example, if the InterNIC assigns your company one network ID, and you have a wide area network consisting of multiple sites, you would define a custom subnet mask for your network ID that is based on the number of subnets and the number of hosts required on each subnet. Custom subnet masks allow you to use the single network ID for all subnets.

Note For more information on custom subnet masks, see the "Internetworking Microsoft TCP/IP on Microsoft Windows NT 3.5" course.

Default Gateway (Router)

For communication with a host on another network, an IP address must be configured for a router with a route to the destination network. If no route is found to the destination network, the default gateway is used. If you do not specify a default gateway, communications are limited to the local network.

Whenever IP prepares to send a packet, it first determines whether the destination host is on a different network. If it is, the request is sent to a router that can communicate with the destination network. If no route to the destination network is found on the local host, the request is sent to the default gateway. A default gateway is simply the router to use for all remote requests when no other path to that network can be found.

Installing Microsoft TCP/IP

The TCP/IP protocol is fully integrated into Windows NT Server. This means that no additional software is required for installation. Installing TCP/IP on Windows NT Server is similar to adding any other network component.

► To install Microsoft TCP/IP

In this procedure you install TCP/IP as a protocol on both the PDC of DOMAIN-A and the PDC of DOMAIN-B. This procedure assumes that you do not yet have TCP/IP installed on your primary domain controllers. If TCP/IP is already installed, skip the procedures in this lesson. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from both primary domain controllers in DOMAIN-A and DOMAIN-B.

---

1. From Control Panel, start Network.

   The Network Settings dialog box appears.

2. Choose Add Software.

   The Network Software dialog box appears.

3. In the Network Software box, select TCP/IP Protocol and Related Components, and then choose Continue.

   The Windows NT TCP/IP Installation Options dialog box appears.

4. Choose Continue to install the default configuration options. The default configuration includes TCP/IP Internetworking and Connectivity Utilities.

   TCP/IP Internetworking is the actual TCP/IP protocol stack for basic communications with other Microsoft TCP/IP computers. This is a required component.

   Connectivity Utilities include the utilities to communicate with other TCP/IP hosts, using FTP, Telnet, and so on. This is selected by default, but can be cleared if there are no requirements for communicating using standard TCP/IP utilities.

   A Windows NT Setup dialog box appears, and prompts you for a path to the Windows NT distribution files.

5. Type the path to the *location of Windows NT Server distribution files*, and then choose Continue.

   The TCP/IP software is installed on the local computer, and the Network Settings dialog box reappears.

6. Choose OK.

   The TCP/IP Configuration dialog box appears.

7. Repeat this procedure on the primary domain controller of the other domain.

Manually Configuring TCP/IP

TCP/IP parameters can be configured in two ways—manually by the user, or dynamically using a Dynamic Host Configuration Protocol (DHCP) server. Configuring TCP/IP manually presents the possibility of having multiple computers configured with the same IP address. Duplicate IP addresses cause IP communications to fail. Configuring TCP/IP dynamically with DHCP reduces the chance of having duplicate IP addresses.

Implementing DHCP is covered in more detail later in this chapter.

► To configure TCP/IP manually

In this procedure you manually configure TCP/IP. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from both primary domain controllers of DOMAIN-A and DOMAIN-B.

---

1. From the TCP/IP Configuration dialog box, configure the IP address and default subnet mask as follows (you do not need to configure the default gateway for this procedure).

Computer name	IP address	Subnet mask
PDC-A	131.107.2.150	255.255.0.0
PDC-B	131.107.2.155	255.255.0.0

Important If you are installing TCP/IP on your company network, you should check with your network administrator to determine the correct IP address and subnet mask to use.

---

2. Choose OK.

   A Windows NT message appears, indicating that at least one adapter card has an empty WINS address. This means that there is no primary Windows Internet Name Service (WINS) server address supplied for the configured TCP/IP interface.

   Important If you do have a WINS server installed, you should supply the IP address of the WINS server to resolve NetBIOS names in an internetwork environment. This address can also be supplied by the DHCP server if you have one. For the present procedure, supplying the IP address of the WINS server is not necessary.

3. Choose Yes.

   A Network Settings Change message appears and prompts you to shut down and restart your computer. This is required to implement the configuration.

4. Choose Restart Now.

   Your computer is shut down and restarted. The Welcome box appears.

5. Log on to your domain as Administrator.

   If you did not receive an error message stating that the system detected an IP address conflict, the IP address you configured was unique.

6. Repeat this procedure on the primary domain controller of the other domain.

Lesson Summary

Installing TCP/IP in a routed network environment requires the configuration of three parameters—IP Address, subnet mask, and default gateway.

For more information on	See
Installing and configuring Microsoft TCP/IP	Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP," in the *Microsoft Windows NT TCP/IP* documentation.
IP addresses, subnet masks, and default gateway parameters	Chapter 3, "Network Concepts for TCP/IP," in the *Microsoft Windows NT TCP/IP* documentation.

For online information about	From the Help menu, choose Contents and then
Installing TCP/IP	Control Panel Network, Add Software, TCP/IP and Related Components, Help.
Configuring the IP Address	Control Panel Network, TCP/IP Protocol, Help, IP Address.
Configuring the Subnet Mask	Control Panel Network, TCP/IP Protocol, Help, Subnet Mask.

Lesson 3: Testing TCP/IP with PING

Installing TCP/IP requires careful configuration of an IP address, subnet mask, and default gateway. An error in typing the IP address, subnet mask, or default gateway can lead to problems. Problems can range from trouble communicating by means of TCP/IP if the default gateway or subnet mask is wrong, to network problems with a duplicate IP address. After you shut down and restart your computer, it is always a good idea to test the configuration and any connections to other TCP/IP hosts and networks to verify that these problems do not exist.

In this lesson, you learn how to use Packet InterNet Groper (PING) to verify that TCP/IP is installed and configured correctly.

After this lesson you will be able to:

- Test a TCP/IP configuration and IP connection with the PING utility.

Estimated Completion Time: 10 minutes

The PING Utility

The PING (Packet InterNet Groper) utility is a diagnostic tool used to test TCP/IP configurations and to diagnose connection failures. PING uses ICMP *echo request* and *echo reply* messages to determine whether a particular TCP/IP host is available and functional.

The command syntax is:

ping IP_address

If PING is successful, it responds with the following message:

Pinging *IP_address* with 32 bytes of data:
Reply from *IP_address*: bytes=32 time<10ms TTL=32
Reply from *IP_address*: bytes=32 time<10ms TTL=32
Reply from *IP_address*: bytes=32 time<10ms TTL=32
Reply from *IP_address*: bytes=32 time<10ms TTL=32

Guidelines for Testing a TCP/IP Configuration

The following steps outline the procedures for verifying a computer's configuration and for testing router connections.

Tip If you start with step 4 and can ping successfully, then steps 1–3 are successful by default.

1. Ping the loopback address (127.0.0.1) to verify that TCP/IP is installed and loaded correctly.

   If this step is unsuccessful, verify that the computer was restarted after TCP/IP was installed and configured.

   Also, check the Event Viewer's System Log for any error messages from system startup.

2. Ping the IP address of your computer to verify that it was added correctly and to check for possible duplicate IP addresses.

   If this step fails, verify that the IP address you used with the PING command matches the IP address that was configured.

   Additionally, you can use IPCONFIG from a command prompt to display the current TCP/IP configuration.

   Also, check the Event Viewer's System Log for any Tcpip error messages from system startup.

3. Ping the IP address of the default gateway to verify that the default gateway is up and running and that you can communicate with the local network.

   If this step fails, verify that the IP address you used with the PING command matches the default gateway's IP address that was configured.

   Attempt to ping another local IP host.

4. Ping the IP address of a remote host to verify that you can communicate through a router.

   If this step fails, verify that the IP address of the default gateway is correct and that the IP router and remote host are functional.

► To test a configuration using PING

In the following procedure, you verify that TCP/IP has initialized properly, and that you can communicate with another host on the local network. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. Go to a command prompt.
2. Type **ping 127.0.0.1** and then press ENTER to ping the local loopback address for testing TCP/IP initialization.

   You should receive four messages stating "Reply from 127.0.0.1" with a packet size and time information.
3. Type **ping 131.107.2.150** and then press ENTER to ping the local IP address for verifying unique addressing.

   You should receive four messages stating "Reply from 131.107.2.150" with a packet size and time information.
4. Type **ping 131.107.2.155** and then press ENTER to ping a host on the local network to test TCP/IP communications.

   You should receive four messages stating "Reply from 131.107.2.155" with a packet size and time information.
5. Type **ping 131.107.2.255** and then press ENTER to attempt to ping a host on the local network that does not exist.

   You should receive four messages stating "Request timed out." This indicates that your computer was unsuccessful in communicating with a host at that address.

Important You can perform the same procedure from the primary domain controller of DOMAIN-B, switching the IP addresses used in steps 3 and 4.

In the previous lesson, you saw how to configure IP addressing information manually. The PING test indicates that you were successful in this configuration. Now you learn what happens when IP addressing information is not unique to a computer. This is a common problem resulting from manually configuring TCP/IP.

► To configure a duplicate IP address

In this procedure, you cause a duplicate IP address to exist on the network by changing the IP address of PDC-A to match that of PDC-B. Duplicate IP addresses are a common problem when manually configuring TCP/IP. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A only.

---

1. From Control Panel, start Network.

   The Network Settings dialog box appears.

2. Under Installed Network Software, select TCP/IP Protocol, and then choose Configure.

   The TCP/IP Configuration dialog box appears.

3. In the IP Address box, type **131.107.2.155** and then choose OK.

   Important If you used a different IP address for PDC-B, use it in place of 131.107.2.155.

   A Windows NT message appears, stating that at least one adapter has an empty Primary WINS address.

4. Choose Yes.

   The Network Settings dialog box appears, and TCP/IP attempts to initialize using the new IP addressing information, but fails.

► To verify the effects of a duplicate IP address

In this procedure, you verify the duplicate IP address problem.

Important Complete this procedure logged on as Administrator from both primary domain controllers of DOMAIN-A and DOMAIN-B.

When the computer initialized TCP/IP using the new IP address, a System Process – System Error message appeared on both Windows NT Server computers displaying the following message:

> "The system has detected an IP address conflict with another system on the network. The local interface has been disabled. More details are available in the system event log. Consult your network administrator to resolve the conflict."

1. Choose OK to close the message on each computer.
2. Switch to Program Manager, and then from the Administrative Tools group, start Event Viewer.

   The Event Viewer window appears. Verify that it is displaying the System Log. If it is not, from the Log menu, choose System.
3. Find the event listed as Tcpip and view the event details.

   The Event Details dialog box appears, displaying the IP and hardware addresses of the other host using the locally assigned IP address.
4. Close the Event Details dialog box.
5. Close Event Viewer.

► **To correct the duplicate address problem**

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A only.

---

1. Switch to Control Panel, and then choose Configure to correct the IP address.

   The TCP/IP Configuration dialog box appears.
2. In the IP Address box, type **131.107.2.150** and then choose OK.

   A Windows NT message appears, stating that at least one adapter has an empty Primary WINS address.
3. Choose Yes.

   The Network Settings dialog box appears, and TCP/IP initializes successfully using the new IP address information.
4. Choose OK to exit the Control Panel Network application.

Lesson Summary

After TCP/IP has been installed and configured, you should verify that communications can take place. The PING utility is an effective way to test TCP/IP communications between hosts. You should start by verifying that your host is configured properly, then verify communications with a local host, and finally verify communications with remote hosts. If communications cannot be established, you can look in the Windows NT Event Viewer for detailed information on initialization problems.

For more information on	See
The PING utility	Chapter 11, " Utilities Reference," in the *Microsoft Windows NT TCP/IP* documentation.
Configuring IP parameters	Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP," in the *Microsoft Windows NT Server TCP/IP* documentation.
Using Event Viewer	Chapter 17, "Event Viewer," in the *Microsoft Windows NT Server System Guide*.

For online information about	From the Help menu, choose Contents and then
Using PING	Windows NT Help, Command Reference Help, PING.
Using IPCONFIG	Windows NT Help, Command Reference Help, IPCONFIG.
Using Event Viewer	Event Viewer Help, View Event Logs. Viewing Event Logs.

Lesson 4: Implementing the Dynamic Host Configuration Protocol (DHCP)

Implementing DHCP eliminates some of the configuration problems associated with manually configuring TCP/IP. DHCP centralizes TCP/IP configurations and manages the allocation of TCP/IP configuration information by automatically assigning IP addresses to computers configured to use DHCP. In this lesson, you learn how to install and configure a DHCP server and a DHCP client to solve problems associated with manually configuring TCP/IP.

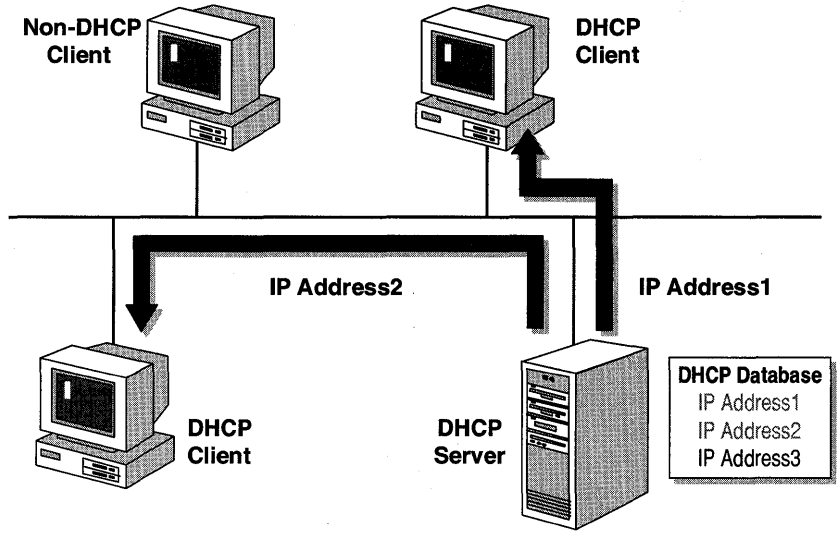


Figure 79: DHCP communications between DHCP servers and clients

After this lesson you will be able to:

- Explain how DHCP automates the TCP/IP configuration process.
- Configure Windows NT Server with DHCP to allocate TCP/IP configuration information to clients.
- Configure a client to use DHCP to obtain TCP/IP configuration information.

Estimated Completion Time: 25 minutes

Why Use DHCP?

Using DHCP to configure IP addressing information automatically means that:

- Users no longer have to get IP addressing information from an administrator to configure TCP/IP properly. When a DHCP client is started, it automatically receives, or leases, IP addressing information from a DHCP server.
- The DHCP server supplies all the necessary configuration information to all the DHCP clients and servers. As long as the DHCP server has the correct configuration information, none of the clients or servers will be configured incorrectly.
- The difficult-to-trace network problems that result from incorrectly configured clients and servers will be completely eliminated.

DHCP Requirements

Because DHCP is a client-server system, software is required on both the client and the server.

A DHCP server requires:

- The DHCP server service configured on at least one computer within the TCP/IP internetwork running Windows NT Server, as long as your IP routers support Request for Comment (RFC) 1542. Otherwise, you will need a DHCP server on each subnet.
- A DHCP scope created on the DHCP server. A DHCP scope consists of a pool of IP addresses, such as 131.107.3.51 through 131.107.3.200, which the DHCP server can assign, or lease, to DHCP clients.

A DHCP client requires:

- A computer running a DHCP-supported operating system. The following operating systems are capable of being a DHCP client:
  - Windows NT Server 3.5
  - Windows NT Workstation 3.5
  - Windows for Workgroups 3.11 with the Microsoft 32-bit TCP/IP VxD installed (provided on the Windows NT Server 3.5 CD)
  - Microsoft Network Client 3.0 for MS-DOS with the real mode TCP/IP driver included on the Windows NT Server 3.5 CD
  - LAN Manager 2.2c included on the Windows NT Server 3.5 CD
  - DHCP enabled at the client

Non-DHCP Clients

Other clients that are not DHCP-enabled can access DHCP clients using TCP/IP utilities and Windows networking. The DHCP administrator should know the IP addresses assigned to these clients to exclude them from the DHCP server scope configuration. If this is not done, it is possible for the DHCP server to assign an IP address to a client that has already been assigned manually to another IP host.

For example, if a client computer has a manually configured IP address of 131.107.3.117, and the pool of addresses in the DHCP scope ranges from 131.107.3.51 through 131.107.3.200, you should make sure to exclude 131.107.3.117 from the pool of addresses in the scope.

How DHCP Works

Each time the DHCP client restarts, it requests IP addressing information from a DHCP server.

When the DHCP server receives the request, it selects an unleased IP address from its pool of IP addresses and offers it to the DHCP client. In most cases, the DHCP server also returns additional TCP/IP configuration information, such as the subnet mask and default gateway.

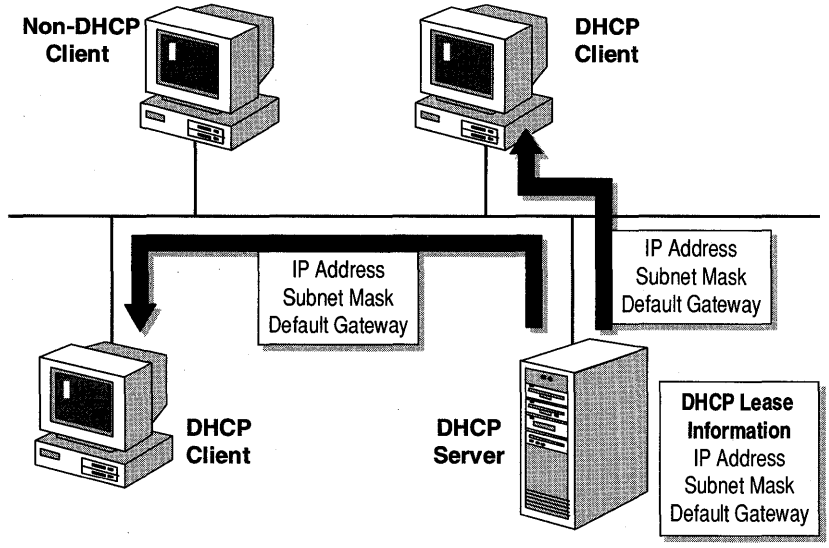


Figure 80: How DHCP works

If there is no available IP addressing information in the pool to lease to a client, the client is unable to bind TCP/IP. IP addressing information is leased to a client until the client manually releases it, or until the DHCP server cancels the lease and makes it available to other clients.

Installing the DHCP Server

You install a DHCP server as part of the process of installing Microsoft TCP/IP. It is important to note that even though the process might be somewhat familiar to you, it is usually done after carefully planning and developing a strategy for implementing DHCP in a TCP/IP internetwork.

These instructions assume that you have already installed TCP/IP.

► To install DHCP on the server

In this procedure you install a DHCP server on PDC-A. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A only.

---

1. Start the Control Panel Network application, and then choose Add Software.

   The Add Network Software dialog box appears.

2. In the Network Software box, select TCP/IP Protocol and Related Components, and then choose Continue.

   The Windows NT TCP/IP Installation Options dialog box appears, displaying the TCP/IP components available to be installed.

3. Select DHCP Server Service, and then choose Continue.

   The Windows NT Setup box appears, prompting you for the full path of the Windows NT distribution files.

4. Type the path to the *location of Windows NT Server distribution files*, and then choose Continue.

   The appropriate files are copied to your server, and then the Network Settings dialog box appears.

5. Choose OK.

   A Network Settings Change dialog box appears, indicating that the system must be restarted to initialize the new configuration.

6. Choose Restart Now to restart Windows NT Server.

7. Log on as Administrator.

Configuring a DHCP Scope

After the DHCP Server service has been installed and initialized on Windows NT Server, you must create a range of addresses before the server can assign addresses to requesting clients. The scope must be configured to supply a client computer with the following information:

- A range or pool of addresses from which the DHCP server can draw to lease to clients
- A subnet mask to be assigned to clients

Optionally, the DHCP server can provide additional TCP/IP configuration parameters to the client, such as the following:

- Default gateway address
- Domain Name Service (DNS) server address(es)
- WINS server address(es)
- NetBIOS name resolution type

► To configure a DHCP scope

In this procedure you configure a DHCP scope for your DHCP server. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A only.

---

1. From the Network Administration group, start DHCP Manager.

   The DHCP Manager window appears.

2. Under DHCP Servers, select *Local Machine*.

   Local Machine indicates that you are configuring the local DHCP server, and not a remote DHCP server.

3. From the Scope menu, choose Create.

   The Create Scope dialog box appears.

4. Complete the scope configuration using the following information:

In this box...	You type this...
IP Address Pool Start Address	**131.107.2.160**
IP Address Pool End Address	**131.107.2.169**
Subnet Mask	**255.255.0.0**

This pool of IP addresses allows for ten DHCP clients to receive address leases from the DHCP server. This is sufficient for this exercise, but if you need more, you can create either a larger pool or an additional pool of addresses on the server.

Important If you use different IP addresses for your computers, the range should not include the addresses used for PDC-A and PDC-B.

---

5. Choose OK when done.

   A DHCP Manager message appears, indicating that the scope was successfully created and must be activated.

6. Choose Yes to activate the scope.

   The DHCP Manager window appears with the new scope added. Notice the yellow light bulb next to the IP address. This indicates an active scope.

7. Close DHCP Manager.

Enabling DHCP At the Client

You enable a client to use DHCP as part of the process of installing Microsoft TCP/IP. If you installed and configured TCP/IP manually, you can modify the TCP/IP configuration to take advantage of DHCP by using the following procedure.

► **To configure TCP/IP automatically using DHCP**

In this procedure, you configure the Windows NT Server domain controller to use DHCP for assigning IP addressing information. This solves the problem of configuring duplicate IP addresses.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B only.

---

1. From Control Panel, start Network.

   The Network Setup dialog box appears.

2. Under Installed Network Software, select TCP/IP Protocol, and then choose Configure.

   The TCP/IP Configuration dialog box appears.

3. Select Enable Automatic DHCP Configuration.

   A Microsoft TCP/IP message appears, indicating that the DHCP protocol will attempt to configure the server automatically during system initialization.

4. Choose Yes.

   The Microsoft TCP/IP Configuration dialog box appears, displaying current TCP/IP configuration parameters.

   Notice that the IP Address and Subnet Mask boxes have been grayed out, and that the manually configured values are no longer displayed.

5. Choose OK to return to the Network Settings dialog box.
6. Choose OK to exit Network.
7. Shut down and restart the computer.
8. Log on to the domain as Administrator.

► To verify the DHCP configuration

In this procedure, you verify the configuration information provided by the DHCP server. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B only.

---

1. Go to a command prompt.
2. To test TCP/IP connectivity with the domain controller for DOMAIN-A computer, type **ping 131.107.2.150** and then press ENTER.

   Four "Reply from 131.107.2.150" messages appear. These indicate proper TCP/IP communications to the host at that IP address.

   Note If you did not receive four successful messages, attempt to ping the local loopback address (127.0.0.1), followed by the IP address of your local computer. If these are successful, attempt to ping another IP host on the network (if another IP host exists).

   ---

3. To verify the DHCP-assigned TCP/IP parameters, type **ipconfig /all** and then press ENTER.

   The TCP/IP configuration appears.

4. What is the DHCP-assigned IP Address of the domain controller?

5. What is the address of the DHCP Server?

You have successfully used a DHCP server to provide an IP address to your PDC of DOMAIN-B.

▶ To reconfigure TCP/IP manually

In this procedure, you reconfigure the primary domain controller of DOMAIN-B to use the manually assigned IP address. This is necessary for successful completion of other chapters in this course, because your current DHCP server (PDC-A) might not always be online. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

---

1. From a command prompt, type **ipconfig/release** to release the IP address assigned form the DHCP server.
2. From Control Panel, start Network.

   The Network Settings dialog box appears.
3. Under Installed Network Software, select TCP/IP Protocol, and then choose Configure.

   The TCP/IP Configuration dialog box appears.
4. Clear the Enable Automatic DHCP Configuration check box.
5. In the IP Address box, type **131.107.2.155**
6. In the Subnet Mask box, type **255.255.0.0**

   Important If you used a different IP address and Subnet Mask for PDC-B, use it instead of 131.107.2.155 and 255.255.0.0.

7. Choose OK.

   A Windows NT message appears, stating that at least one adapter has an empty Primary WINS address.
8. Choose Yes.
9. Choose OK to exit the Control Panel Network application.

Lesson Summary

Administering IP addresses on TCP/IP hosts can be a time-consuming task for network administrators. To assist with this, Windows NT Server computers can be configured as DHCP servers, which can automatically assign and maintain IP addressing information for clients that support DHCP. This allows administration to be controlled from a central location, and prevents users from supplying invalid or incorrect IP addressing information on their local computers.

For more information on	See
Dynamic Host Configuration Protocol (DHCP)	Chapter 3, "Network Concepts for TCP/IP," in the *Microsoft Windows NT TCP/IP* documentation.
	Chapter 4, "Installing and Configuring DHCP Servers," in the *Microsoft Windows NT TCP/IP* documentation.
	Appendix F, in the "*Microsoft Windows NT Server 3.5 Dynamic Host Configuration Protocol and Windows Internet Naming Service.*"
Enabling DHCP at a client computer	Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP," in the *Microsoft Windows NT TCP/IP* documentation.
Using IPCONFIG	Chapter 11, "Utilities Reference," in the *Microsoft Windows NT TCP/IP* documentation.

For online information about	From the Help menu, choose Contents and then
Installing the DHCP Server Service	Control Panel Network, Add Software, TCP/IP and Related Components, Help.
Creating a DHCP Scope	DHCP Manager Help, Defining DHCP Scopes, Introduction to DHCP Scopes.
	DHCP Manager Help, Defining DHCP Scopes, Creating DHCP Scopes.
Enabling DHCP at a client computer	Control Panel Network, TCP/IP Configuration Help, Enable Automatic DHCP Configuration..
Using the IPCONFIG command	Windows NT Help, Command Reference Help, IPCONFIG.

CHAPTER 8

Browsing for Wide Area Network Resources

Before You Begin

This chapter assumes that you understand the basic TCP/IP concepts covered in Chapter 7, "Installing and Configuring Microsoft TCP/IP on Windows NT Server."

The procedures in this chapter are paper-based and do not require the use of a computer.

Lesson 1: Introduction to Browsing in a Wide Area Network

The Microsoft Windows NT Computer Browser service builds a list of the domains and servers that are available on the network. Users view this list to see which computers they can access. For example, when a user issues a net view request from a command prompt or chooses Connect Network Drive from File Manager, the Browser service generates the list of domains and servers that are active and available on the network. These lists are generated from Browser servers.

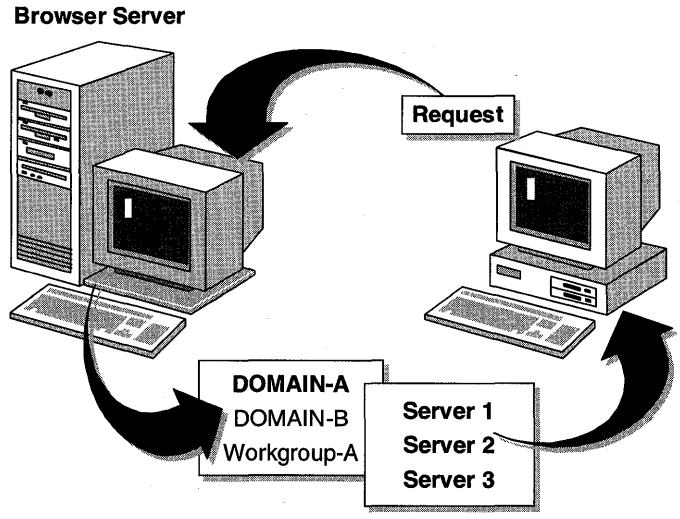


Figure 81: Browsing network resources

In this lesson, you learn the different type of browser computers, how browsing works in multiple workgroup and domain networks, and how browsing works in a wide area network environment.

After this lesson you will be able to:

- Describe the different types of browsers and their roles.
- Explain how browsing works across domains and workgroups.
- Explain how browsing works in a wide area network.

Estimated Completion Time: 10 minutes

Types of Browsers

Both Microsoft Windows NT Workstation and Microsoft Windows NT Server computers can be browsers. There are four types of browsers, and each type performs a different role: Domain Master Browser, Backup Browser, Master Browser, and Preferred Master Browser.

Domain Master Browser

The *Domain Master Browser* is responsible for collecting announcements for the entire domain (including any subnets) and providing a list of domain resources to *Backup Browsers*. An announcement is a message sent by a server to notify computers that it is available on the network. The Domain Master Browser is always the primary domain controller for the domain. It also collects announcements from other domains to build a list of available domains.

Backup Browser

The *Backup Browser* maintains a copy of the browse list and distributes the list to computers in the domain upon request. All Windows NT Server domain controllers are automatically configured as Backup Browsers. Windows NT Workstation and Windows NT Server (non-domain controller) computers have the potential to be Backup Browsers if there are not already at least three Windows NT Server computers performing Master and Backup Browser functions for the workgroup or domain.

Master Browser

The *Master Browser* receives announcements from computers within the workgroup or domain and provides a list of domain resources to the Backup Browsers. In a TCP/IP internetwork, there is a Master Browser on each subnet; in a LAN, the Master Browser is the Domain Master Browser.

The Master Browser is chosen from a domain's servers through an election algorithm. The criteria for electing a Master Browser are evaluated in the following order:

- If the local computer's election criteria are greater than the initiator of the election process's criteria, the local computer wins. For example, a Windows NT computer will win over a Windows for Workgroups computer.
- If the computer has been powered on longer than the initiator, the computer wins.
- The server with the lower alphabetical name wins. For example, a server named *A* will become a Master Browser over a server named *X*.

Preferred Master Browser

The *Preferred Master Browser* is a Browser server that has been configured to win browser elections and become the Master Browser. If you are not implementing the Windows Internet Name Service (WINS) in a TCP/IP internetwork, it is important to configure a Preferred Master Browser to perform domain browsing and NetBIOS computer name resolution.

To specify a computer as a Preferred Master Browser, set the IsDomainMasterBrowser parameter's value to either True or Yes. (This value will automatically be set to either False or No, even if the computer is currently the Master Browser.) This parameter is located in the Registry under the following key:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser
\Parameters
```

Potential Browser

A *Potential Browser* is any computer that can be elected to be a Master or Backup browser. This includes:

Operating system	Type of browser
Windows NT Server (domain controller)	Will be either a Master or Backup browser
Windows NT Server (non-domain controller)	Can be a Master or Backup browser
Windows NT Advanced Server	Will be either a Master or Backup browser
Windows NT Workstation	Can be a Master or Backup browser
Windows for Workgroups	Can be a Master or Backup browser
Windows NT 3.1	Can be a Master or Backup browser

Browsing a Wide Area Network

Under Windows NT, each local subnet functions as an independent browsing entity with its own Master Browser and Backup Browsers, because broadcasts do not pass through routers. For this reason, browser elections occur within each subnet.

WAN browsing support is provided only in Windows NT domains, so at least one Windows NT Server domain controller must be on the subnet to be able to browse a WAN.

Domain Master Browsers are responsible for collecting computer name information used in maintaining WAN-wide browse lists of available computers in all domains.

Spanning Multiple Subnets

When a domain spans multiple subnets, the Master Browsers for each subnet use a directed datagram (rather than a broadcast) called a "MasterBrowserAnnouncement" to announce themselves to the Domain Master Browser. To collect a subnet's list of servers, the Domain Master Browser sends a request to the subnet's Master Browser that announced itself.

The Domain Master Browser then merges its own server list with the server list from the Master Browser that issued the announcement. This process is done every 15 minutes and guarantees that the Domain Master Browser will always have a complete browse list of all the servers in the domain. The Domain Master Browser updates each Master Browser with the current list. Each Master Browser updates each Backup Browser. When a client issues a browse request to the Backup Browser, such as a net view, the Backup Browser returns a list of all the servers in the domain, regardless of which subnet they are on.

Because Windows NT-based workgroups cannon span subnets, any Windows NT workgroup name that appears on multiple subnets will function as an independent browsing entity.

In the following figure, the Domain Master Browser contains a browse list for all computers registered (that is, those that have a server component) on subnets A, B, and C.

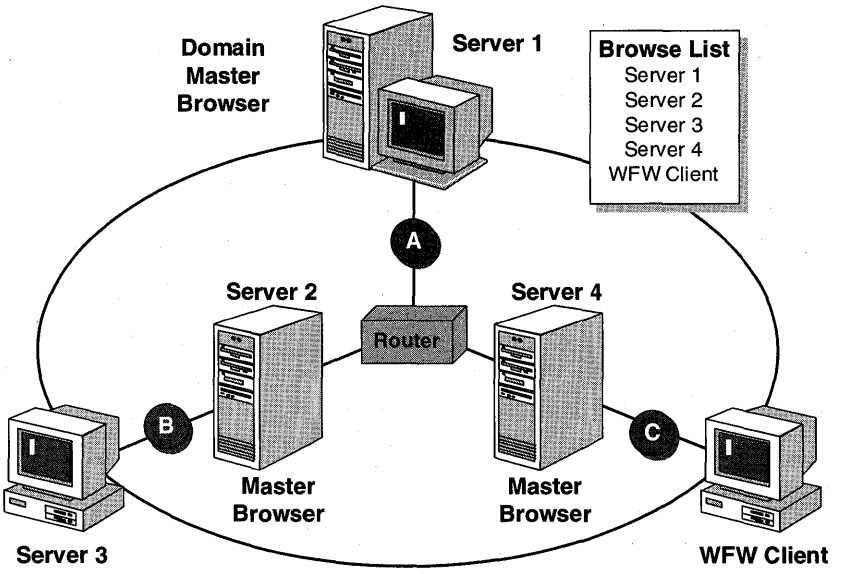


Figure 82: Master Browsers in a wide area network

Synchronizing Master Browsers

To guarantee that each subnet can browse network resources on all subnets, the Master Browsers and Backup Browsers automatically synchronize their browse lists. This is done after the Master Browser has synchronized with the Domain Master Browser.

If a Master Browser is not the PDC, then the Master Browser will synchronize with the PDC. Synchronization is performed every 15 minutes by sending a request to the Domain Master Browser.

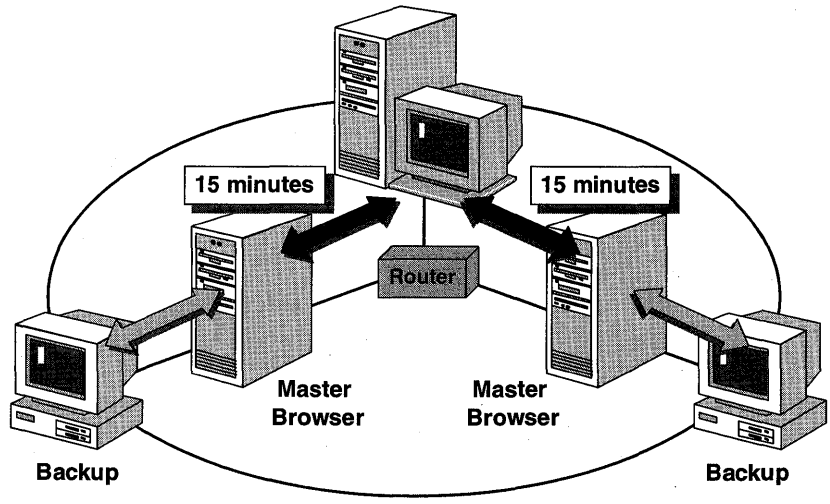


Figure 83: Synchronizing Master Browsers

The Master Browser sends a directed "MasterBrowserAnnouncement" datagram to the Domain Master Browser. This extra level of synchronization guarantees that the Master Browser has a complete list of all servers in the domain, regardless of which subnet the servers are on.

Browsing Multiple Domains

In a multiple domain environment, clients must be able to retrieve lists of:

- Domains.
- Servers within a domain.

To build a multiple domain browse list, the Domain Master Browser in one domain must receive domain announcements from the Domain Master Browser in other domains.

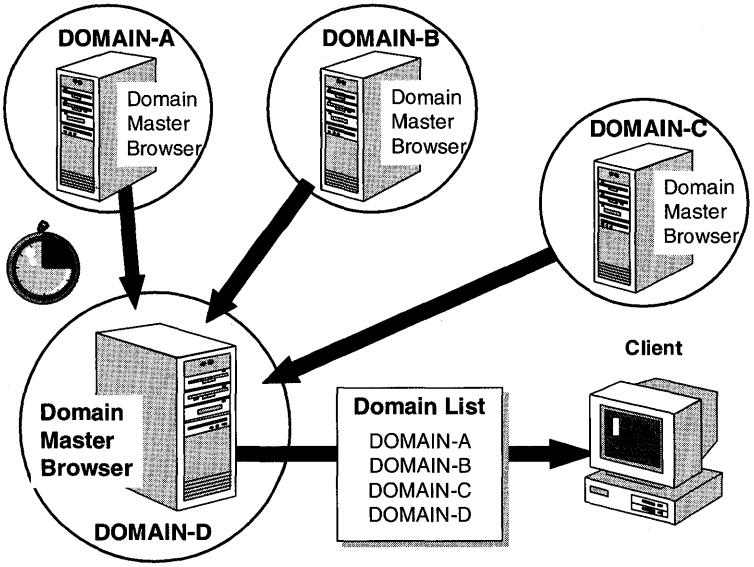


Figure 84: Multiple domain browse lists sent to a client

Retrieving Domain Names

After becoming a Master Browser, a computer broadcasts a "DomainAnnouncement," announcing the existence of the domain every minute for the first five minutes. After the first five minutes, the Master Browser makes "DomainAnnouncement" broadcasts once every 15 minutes.

If a domain has not announced itself for three announcement periods, the domain will be removed from the list of domains. It is possible for a domain to appear in the browse list for up to 45 minutes (3 times 15) after the domain has gone down.

Note These intervals are not configurable.

Domain Announcement Packets

A Master Browser receives "DomainAnnouncement" packets from other domains and places the specified domain in its local browse list.

Upon becoming a Master Browser, a Master Browser can force domains to announce themselves. However, the Master Browser does this only if its domain list is empty, such as when a Potential Browser is promoted to Master Browser.

A "DomainAnnouncement" packet contains:

- The name of the domain.
- The name of the Master Browser for that domain.
- An indication as to whether the browser computer is running Windows NT Workstation or Windows NT Server.

If the browser computer is running Windows NT Server, the "DomainAnnouncement" also specifies whether that computer is the domain's PDC.

Domain Master Browser Failures

If the Domain Master Browser fails, Master Browsers will see only the servers located on their local subnet. This means that all servers that are not on the local subnet will eventually be removed from the browse list.

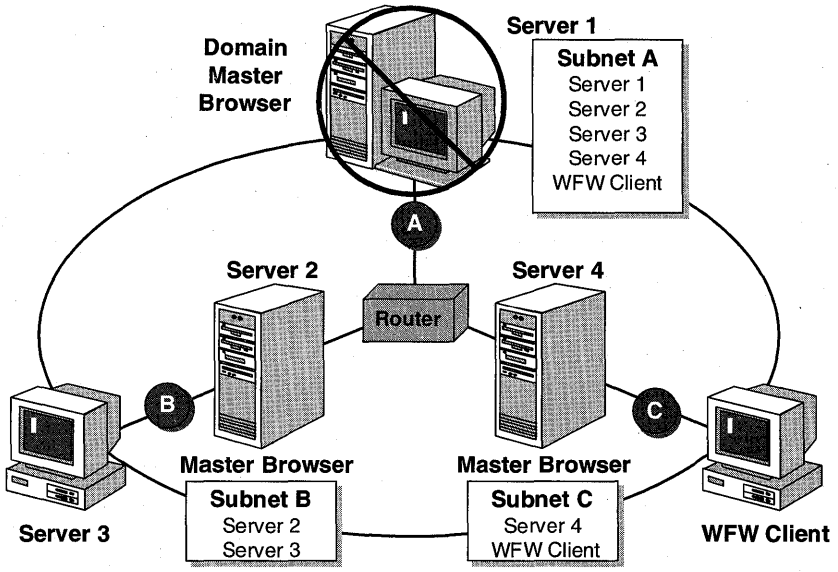


Figure 85: Browse lists generated when the Domain Master Browser is unavailable

Because a Domain Master Browser is also a PDC, you can correct the failure by promoting a backup domain controller (BDC) to a PDC. A BDC can perform most PDC network tasks, such as validating logon requests, but it cannot promote itself to a PDC in the event of a PDC failure.

Determining Browser Roles

In the following procedure, you determine the browser role of each computer in a multiple domain environment.

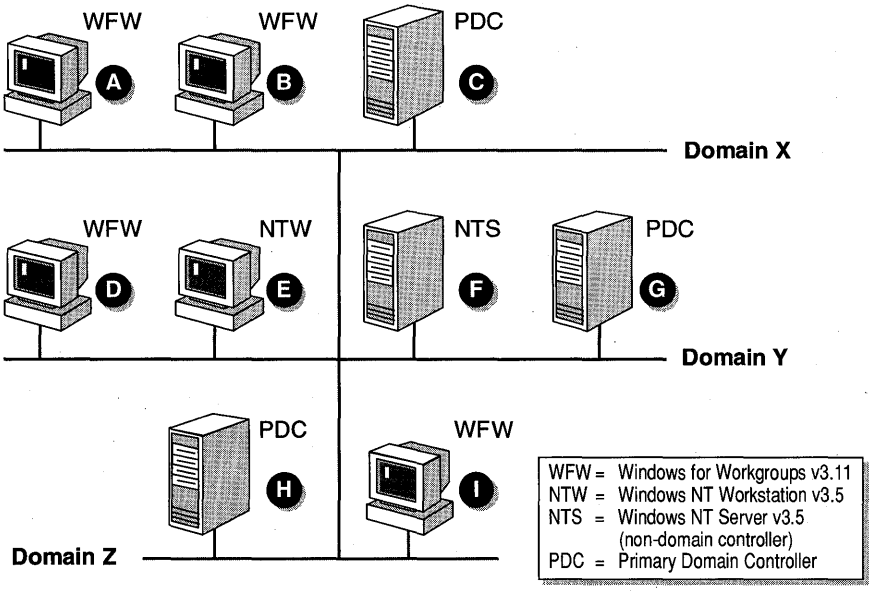


Figure 86: Procedure to determine the browser role

► To determine the browser role

- Using the previous figure, determine the role of each computer in a domain, either Domain Master Browser, Master Browser, Backup Browser, or Potential Browser. Write the corresponding letter in the appropriate column in the following table.

	Domain Master Browser	Master Browser	Backup Browser	Potential Browser
Domain x				
Domain y				
Domain z				

Lesson Summary

To make it easier for clients to access resources in a large network environment, the Windows NT Computer Browser service supports browsing multiple workgroups and domains, as well as wide area networks. It accomplishes this by using different browsing roles for different computers, called Browser servers. The types of Browser servers are Domain Master Browser, Master Browser, Backup Browser, Preferred Master Browser, and Potential Browser. Each browser server plays a role in providing the browse list to client computers.

Lesson 2: Browsing a TCP/IP Internetwork

Windows NT relies on NetBIOS name broadcasts to obtain information from computers on Microsoft networks. In a TCP/IP internetwork in which domains are separated by routers, problems can arise because broadcasts, by default, do not pass through routers. Windows NT Server provides two features to address this problem:

- The Windows Internet Name Service (WINS)
- The local LMHOSTS file

Note Some routers can be configured to forward NetBIOS name broadcasts. If your router can forward NetBIOS name broadcasts, it is not necessary to use the LMHOSTS file or WINS.

In this lesson, you learn how to enable browsing in an IP internetwork using WINS and the LMHOSTS file.

After this lesson you will be able to:

- Describe how the Windows Internet Name Service solves NetBIOS name broadcast problems.
- Configure the LMHOSTS file with the IP address and NetBIOS name mapping of the Preferred Master Browser.

Estimated Completion Time: 10 minutes

The Windows Internet Name Service (WINS)

The Windows Internet Name Service (WINS) solves NetBIOS name broadcast problems by dynamically registering a computer's NetBIOS name and IP address and storing them in a database. When WINS clients communicate with TCP/IP hosts across subnets, the destination host's IP address is retrieved from the database rather than by using a broadcast. This is illustrated in the following figure.

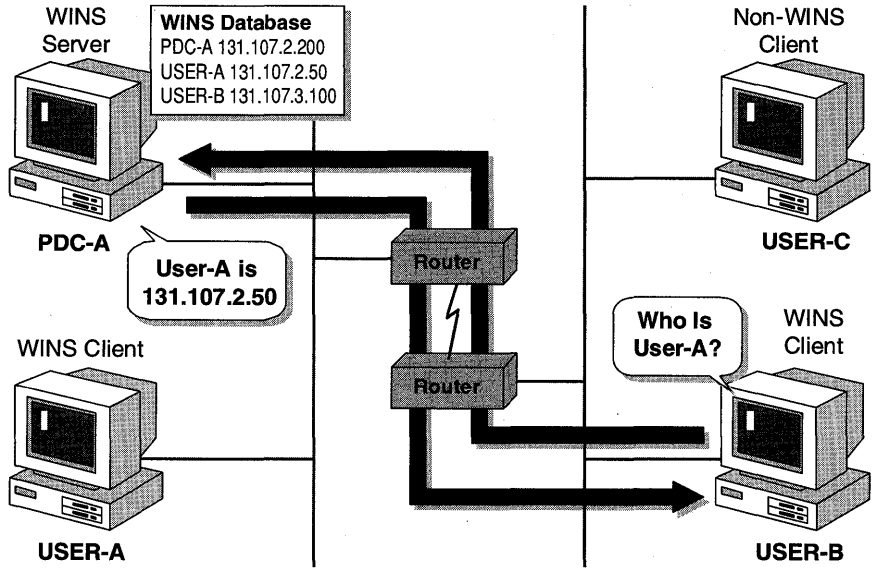


Figure 87: Windows Internet Name Service

Using WINS requires that:

- WINS is configured on at least one computer running Windows NT Server 3.5 within a TCP/IP internetwork. The WINS server maintains a database of IP address–NetBIOS name mappings of clients that are configured to use WINS.
- Clients are WINS-enabled. When a WINS client initializes, it registers its NetBIOS computer name and IP address with the WINS server. To communicate with another TCP/IP host within the internetwork, the WINS client sends a direct request to the WINS server for the IP address–NetBIOS name mapping of the destination computer.

  WINS clients can be configured with Windows NT 3.5, Windows for Workgroups (running TCP/IP-32), Microsoft Network Client software (provided on the Windows NT Server 3.5 CD-ROM), and the LAN Manager 2.2c client supplied on the Windows NT Server 3.5 CD-ROM.

Important If you have Windows for Workgroup clients running Microsoft TCP/IP-32, you must use the modified VREDIR.386 file that is supplied on the Microsoft Windows NT Server 3.5 CD-ROM to participate in WAN browsing.

The LMHOSTS File

Clients that are not configured to use WINS require an LMHOSTS file with the IP address and NetBIOS name of the domain controllers (either PDC or BDC) located on other subnets. This is required even if a WINS Server has been configured in the domain, because NetBIOS name broadcasts do not go through routers. The LMHOSTS file is a static file that maintains IP address–NetBIOS name mappings of TCP/IP hosts located on remote subnets. The LMHOSTS file is cached when TCP/IP is initialized.

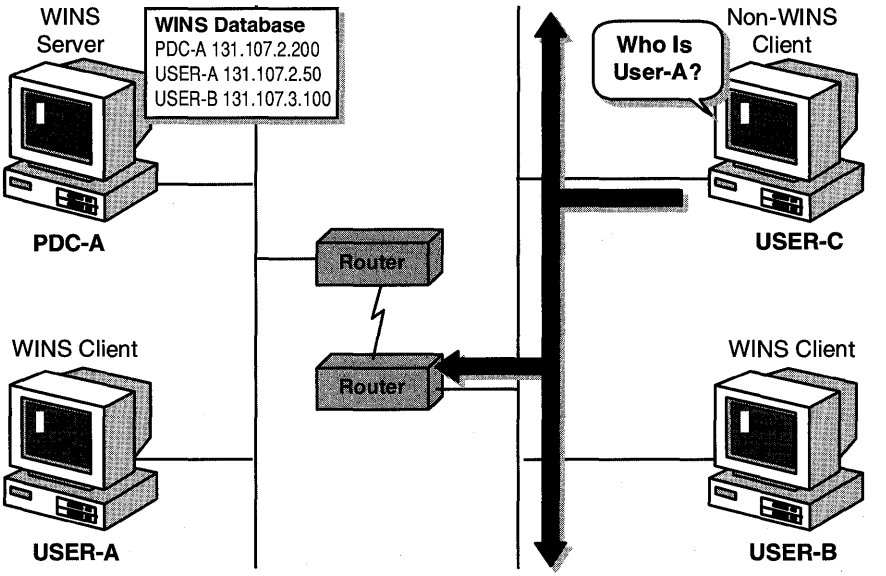


Figure 88: NetBIOS name broadcast from a non-WINS client

The previous figure illustrates a non-WINS client attempting to browse resources from USER-A. The NetBIOS name broadcast is on the local network and does not pass through the router. In this environment, there must be a Master Browser in the domain on the local subnet to provide browsing for non-WINS clients.

To ensure that the Master Browser for each subnet can access the domain's PDC, the PDC for each domain must exist in the LMHOSTS file on each Master Browser with the #DOM extension. The same requirement exists for the BDCs.

The LMHOSTS file on each subnet's Master Browser should contain the following information:

- IP Address and NetBIOS name of the Preferred Master Browser
- The domain name preceded by the #PRE #DOM: tags

For example:

```
130.20.7.80 preferred_master_browser #PRE #DOM:domain_name
```

The LMHOSTS file can be edited using any text editor. It is located in the *\winnt_root*\SYSTEM32\DRIVERS\ETC directory.

The following example shows the browse list that clients would see if an LMHOSTS file were not configured. Clients on subnet A would not see the list of computers on subnet B and vice versa. They would see only the computers on their local subnet.

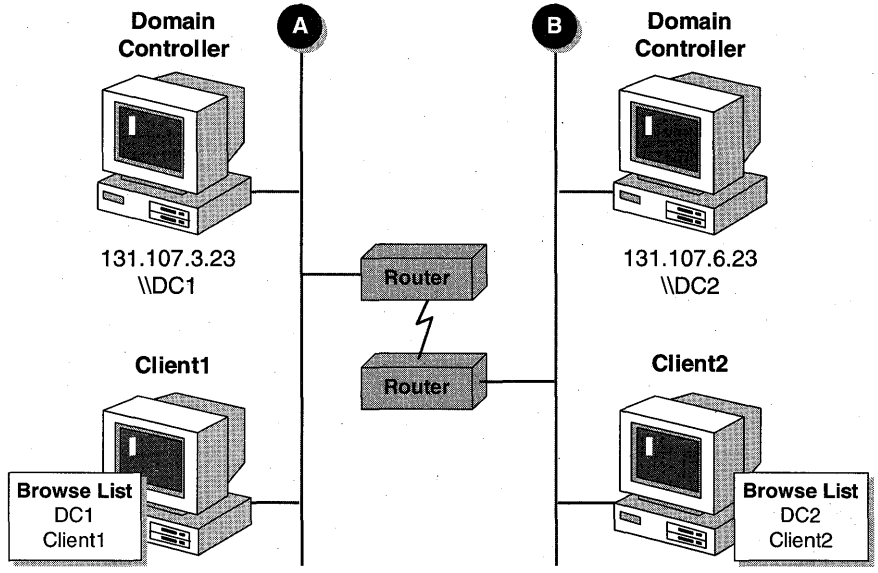


Figure 89: Browsing TCP/IP subnets without an LMHOSTS file

The following example shows the browse list that clients would see if an LMHOSTS file were configured at each domain controller, with the IP address and NetBIOS name mapping of the domain controller located on the other subnet. In this example, clients can see all computers on subnets A and B.

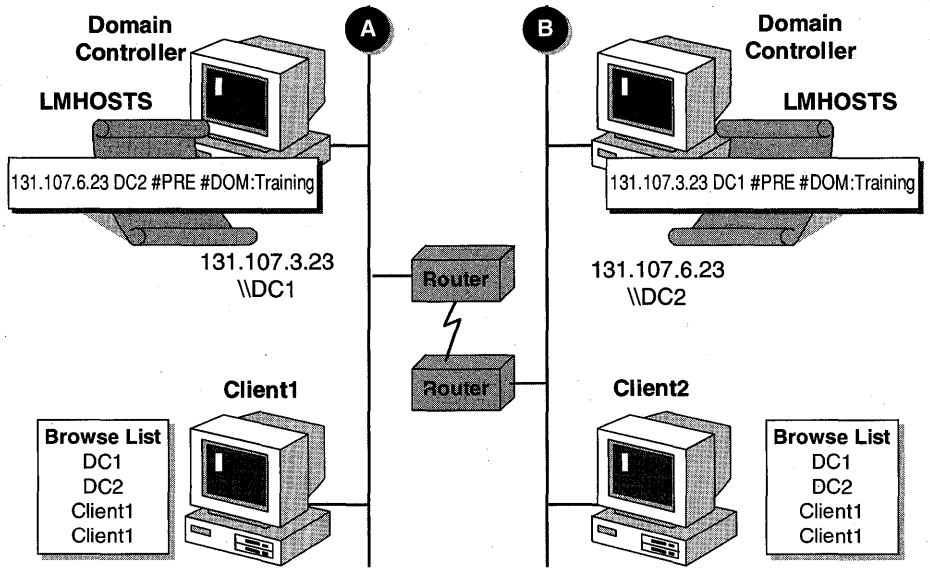


Figure 90: Browsing TCP/IP subnets using the LMHOSTS file

Internetwork Browsing

In this procedure, you determine which computers need an LMHOSTS file to support internetwork browsing.

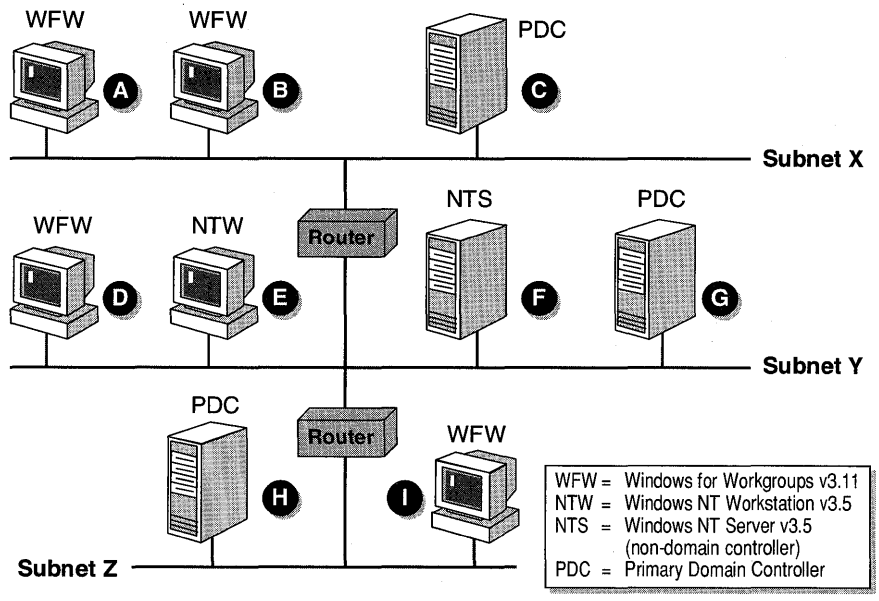


Figure 91: Procedure on LMHOSTS file

► To determine which computers need an LMHOSTS file

- Using the previous diagram, determine which computers need an LMHOSTS file configured to support internetwork browsing.

This computer...	Requires the LMHOSTS file configured with the IP address and NetBIOS name of these computers...

Lesson Summary

Browsing in a TCP/IP internetwork poses special challenges. To ensure Internet-wide browsing in a TCP/IP internetwork, you must implement WINS or configure an LMHOSTS file for each client.

For more information on	See
The Windows Internet Name Service	Chapter 3, "Networking Concepts for TCP/IP," in the *Microsoft Windows NT Server TCP/IP* documentation.
	Chapter 5, "Installing and Configuring WINS Servers," in the *Microsoft Windows NT Server TCP/IP* documentation.
	Appendix F, "Microsoft Windows NT Server 3.5 Dynamic Host Configuration Protocol and Windows Internet Naming Service."
The LMHOSTS file	Chapter 3, "Networking Concepts for TCP/IP," in the *Microsoft Windows NT Server TCP/IP* documentation.
	Chapter 6, "Setting Up LMHOSTS," in the *Microsoft Windows NT Server TCP/IP* documentation.

For online information about	From the Help menu, choose Contents and then
Configuring the LMHOSTS file	Control Panel Network, TCP/IP Protocol Configuration, Advanced, Help, Enable LMHOSTS Lookup.
Using WINS for browsing	Control Panel Network, Add Software, TCP/IP Protocol and Related Components, Help, WINS Server Service.

Lesson 3: Interoperability with Microsoft LAN Manager

The Windows NT Browser service can be configured so that LAN Manager clients can also receive browse lists. In this lesson, you learn how to enable browsing in an environment that contains both Windows NT Server and LAN Manager domains.

After this lesson you will be able to:

- Configure Windows NT Server to make Browser broadcasts to LAN Manager 2.*x* clients.
- Configure the Windows NT Browser service to include LAN Manager domains.

Estimated Completion Time: 5 minutes

Making Browser Broadcasts to LAN Manager 2.*x* Clients

The Make Browser Broadcasts to LAN Manager 2.*x* Clients option causes the browser to announce itself, with a LAN Manager compatible server announcement, to LAN Manager 2.*x* computers. By default, send announcements are not sent to LAN Manager 2.*x* computers.

To make Windows NT Server browse lists available to LAN Manager 2.*x* clients, you perform the following steps:

1. From Control Panel, start Network.
2. Under Installed Network Software, select Server, and then choose Configure.
3. From the Server dialog box, select Make Browser Broadcasts to LAN Manager 2.*x* clients.

   Your screen looks similar to the following.

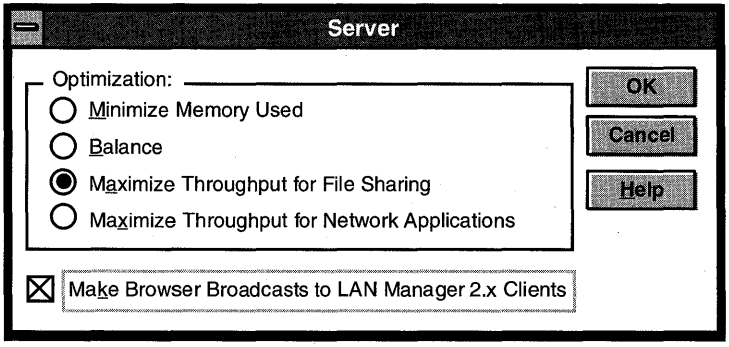


Figure 92: The Server dialog box

4. Choose OK to exit the Network application and return to Control Panel.

This configuration is stored in the Registry under the following key:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanmanServer\Parameters
```

Browsing Other Domains

Each Windows NT Server computer can be configured for browsing up to four other domains. The other domains are LAN Manager–only domains which the local computer is interested in browsing. If any other domains are configured on a Domain Master Browser, the other domains are provided to all members of the domain.

To configure the Windows NT Browser service to include LAN Manager domains, you perform the following steps:

1. From Control Panel, start Network.
2. Select Computer Browser, and then choose Configure.
3. In the Other Domains box, type the name of the other domain.

   If an invalid domain name is added, an error will be recorded in the system log each time the computer restarts.

This configuration is stored in the Registry under the following key:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanmanWorkstation\Parameters
```

Note Other domains can be configured only on Windows NT Server computers.

Lesson Summary

In a mixed environment of Windows NT and LAN Manager computers, special configuration is required to provide complete browsing of network resources. You can configure a Windows NT Server computer to announce itself to LAN Manager clients, and you can add LAN Manager domains to Windows NT Server browse lists for browsing.

For more information on	See
Differences between LAN Manager and Windows NT browsing	Appendix A, "Differences in Administering LAN Manager and Windows NT Server," in the *Microsoft Windows NT Server Upgrade* documentation.
Configuring Browser to include LAN Manager domains	Chapter 2, "Managing Domains and Trust Relationships," in the *Microsoft Windows NT Server Network Operations Quick Reference Guide.*

For online information about	From the Help menu, choose Contents and then
Adding domains to the browse list	Control Panel Network, Computer Browser Configuration, Help.
Making browser announcements to LAN Manager clients	Control Panel Network, Server Configuration, Help.

CHAPTER 9

Installing Microsoft Network Client Software

Before You Begin

This chapter requires that you have completed Chapters 1–5.

In this chapter, you work with two computers in a domain. One computer is the primary domain controller of DOMAIN-B (PDC-B). The computer currently operating as the primary domain controller of DOMAIN-A (PDC-A) will be configured to also start as a Windows for Workgroups client on DOMAIN-B. Of course, if you have an additional computer available, you can use it for your Windows for Workgroups client and leave the two primary domain controllers functioning as they are.

To complete the chapter, you need an MS-DOS system disk. The procedures require that the computer that will become your Windows for Workgroups client is capable of booting as an MS-DOS computer, and that C:\AUTOEXEC.BAT and C:\CONFIG.SYS exist. You need 25 MB of free disk space to complete the procedures.

Lesson 1: Windows NT Server Clients

Any computer that can access a shared resource on a computer running Windows NT Server 3.5 is considered a client. Windows NT Server includes client support for Microsoft networks, including MS-DOS, LAN Manager (both MS-DOS and OS/2), and Windows for Workgroups 3.11 clients.

This lesson covers the client support included in Windows NT Server and the related connectivity utilities.

After this lesson you will be able to:

- List the clients supported by Windows NT Server 3.5.
- Describe the two connectivity utilities.
- Explain the functions of the Network Client Administrator tool.

Estimated Completion Time: 20 minutes

The following client software is provided with the Windows NT Server 3.5 product:

- Microsoft Network Client 3.0 for MS-DOS
- Microsoft LAN Manager 2.2c for MS-DOS
- Microsoft LAN Manager 2.2c for OS/2
- Windows for Workgroups 3.11 (only on CD-ROM)

The following two connectivity utilities ship with Windows NT Server 3.5:

- Remote Access Service 1.1a for MS-DOS
- Microsoft TCP/IP 32 for Windows for Workgroups 3.11

Network Client 3.0 for MS-DOS

The Microsoft Network Client 3.0 is the recommended client for MS-DOS–based computers that do not run Microsoft Windows and need access to resources on a Windows NT Server network. It performs the best of any MS-DOS client available, and it uses less memory and is easier to install than MS-DOS LAN Manager. The software for this client is on the Windows NT Server CD-ROM.

Note For more information on the Network Client 3.0 for MS-DOS, see Appendix A, "Microsoft Network Client Version 3.0 for MS-DOS," in the *Microsoft Windows NT Server Installation Guide*.

Supported Protocols

All four protocols (NetBEUI, IPX, TCP/IP, and Microsoft DLC) that ship with Windows NT 3.5 are included in Microsoft Network Client 3.0. As many as three protocols can be used at one time.

NetBEUI is a small, fast protocol used for LAN environments. It has been supplied in Microsoft networks since LAN Manager, so it has good connectivity to Microsoft network computers.

NWLINK IPX/SPX Compatible Transport is a small, fast protocol stack that is compatible with Novell's IPX/SPX protocol. It is used primarily in environments that include a mix of Microsoft and Novell computers.

TCP/IP is an industry standard protocol that is the most widely accepted protocol for wide-area networking. It offers the most complete set of connectivity options, including the ability to connect to the worldwide Internet. The TCP/IP protocol included with Microsoft Network Client 3.0 supports both DHCP and WINS to simplify configuration and network browsing.

Microsoft DLC is a protocol used to connect directly to network interface printers and to connect to IBM mainframe systems. It cannot be used to access network resources on a Windows NT computer.

Redirectors

The redirectors that come with the Network Client have been optimized to work with Windows NT Server. Redirectors are client software that allow logging on to the network and accessing network resources. There are two versions of redirector.

- Full Redirector—This is the default redirector used when installing a Microsoft Network Client computer. The full redirector uses built-in buffers that make it faster than the basic redirector. The full redirector supports the following:
  - Domain logons
  - Logon scripts
  - Messaging
  - Named pipes
  - Remote procedure calls (RPC)

  Even though the full redirector uses more memory (110K) than a basic redirector (10K), the full redirector is recommended for users connecting to Windows NT domains because of the supported functions and the faster speed. The full redirector is automatically loaded into upper memory if there is sufficient upper memory area available.

- Basic Redirector—The main reason behind the creation of the basic redirector is its use of very little memory (10K). Because it does not use a built-in buffer, the basic redirector is slower than the full redirector. The basic redirector does not support domain logons or the other communications mechanisms of the full redirector. Users cannot log on to a Windows NT domain with the basic redirector. Users can access resources if they have been given permissions, but users will not be validated at logon.

Differences from Microsoft Workgroup Add-On for MS-DOS Client

The Microsoft Network Client 3.0 is based on the Microsoft Workgroup Add-On for MS-DOS 3.11 product, with the exception that Microsoft Network Client 3.0 does *not* include the MS-DOS Mail client or real-mode server. Microsoft Network Client 3.0 does support NetBEUI, IPX, Microsoft DLC, and TCP/IP protocols.

LAN Manager 2.2c Clients

Software for two LAN Manager 2.2c clients is on the Windows NT Server 3.5 CD-ROM, one for MS-DOS and one for OS/2.

LAN Manager 2.2c for MS-DOS

The MS-DOS LAN Manager client ships with NetBEUI, Microsoft DLC, and a TCP/IP protocol stack that has been updated to support DHCP and WINS. It also includes a NetWare Connectivity disk, which allows clients to connect to a Novell NetWare server, although some additional Novell client software is required for full connectivity.

The MS-DOS LAN Manager client is the only Windows NT client that supports the Remoteboot (or remote program load – RPL) service.

LAN Manager 2.2c for OS/2

The OS/2 LAN Manager client supports OS/2 1.*x* and OS/2 2.*x*. The client ships with NetBEUI and TCP/IP. However, its version of TCP/IP does not support DHCP or WINS.

Microsoft Windows for Workgroups 3.11 Client

Windows for Workgroups 3.11 is the recommended network client for MS-DOS–based Windows users because it has 32-bit networking components, which make it the fastest network client available.

Unlike other client software included with Windows NT Server, the Windows for Workgroups client is not free; licenses are required for all copies installed. If disks or documentation are required, the full Windows for Workgroups 3.11 product must be purchased.

Network Redirector

Also included in the Windows for Workgroups client is an updated network redirector, VREDIR.386, which includes:

- Support for named pipes over direct host NWLink.
- Performance enhancements to the direct hosting over NWLink.
- An update to prevent browsers from synchronizing and announcing simultaneously.
- Changes to allow the Windows NT Server tools to run on Windows for Workgroups 3.11.
- Changes to allow browsing of Windows NT computers on a remote subnet.
- Improvements in the client-side caching.

Important VREDIR.386 is on the Windows NT Server 3.5 CD-ROM in the \CLIENTS\WFW\UPDATE directory, for use on computers that already have Windows for Workgroups 3.11 installed.

Connectivity Utilities

The client software provided with the Windows NT Server includes two utilities to enhance network connectivity for MS-DOS and Windows clients.

Remote Access Service 1.1a for MS-DOS

This software is for MS-DOS clients who need to connect to the network by using a modem. Remote Access Service supports both the Microsoft Network Client 3.0 and LAN Manager 2.2c for MS-DOS clients using the NetBEUI protocol.

Microsoft TCP/IP 32 for Windows for Workgroups 3.11

The version of TCP/IP on the Windows NT Server CD-ROM offers the following benefits to a Windows for Workgroups client computer:

- Implemented as a VxD, so it does not use conventional memory
- Supports Windows Sockets 1.1
- Can use DHCP for automatic TCP/IP configuration
- Can use WINS for network browsing support
- Uses the same code base as the Windows NT 3.5 TCP/IP protocol stack

Network Client Administrator

The Network Client Administrator is the main tool used to install and manage the various network clients. This utility, installed automatically when Windows NT Server is installed, makes it easier for you to install client software. An icon for the utility is placed in the Network Administration group.

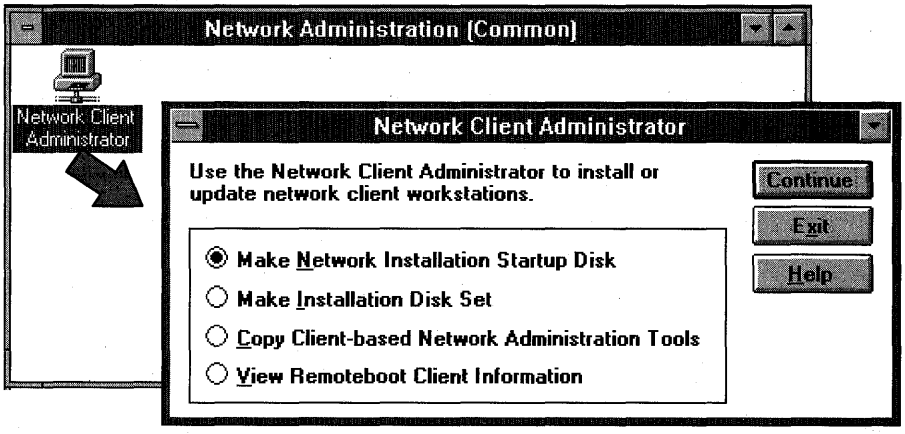


Figure 93: Network Client Administrator dialog box

The Network Client Administrator makes it possible to create:

- An over-the-network installation startup disk to install either the Microsoft Network Client or Windows for Workgroups client on a client computer. The client computer can then use this disk as a boot disk, and it will automatically connect to a server and start installing the selected client software.
- Floppy disk sets for installing the network client software. This utility cannot create disk sets for Windows for Workgroups 3.11.
- An installation share for installing Windows NT Server Tools on Windows 3.*x* or Windows NT clients.

Lesson Summary

Windows NT Server includes several clients for Microsoft networks, such as MS-DOS clients, LAN Manager clients (both MS-DOS and OS/2), and Windows for Workgroups 3.11. Windows NT Server also includes software that enables remote users to dial in to the network and gain access to network resources, and a new TCP/IP protocol for Windows for Workgroups that includes many enhancements for connectivity in a TCP/IP environment.

Review Question

The following question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- You are installing Microsoft Windows NT Server 3.5 in your existing network, which includes LAN Manager, Windows NT 3.1, and Novell NetWare. Which network clients can be installed from the Windows NT Server CD-ROM?

For more information on	See
Microsoft networking clients	Chapter 9, "Network Client Administrator," in the *Microsoft Windows NT Server Installation Guide.*
Microsoft Network Client 3.0	Appendix A, "Microsoft Network Client Version 3.0 for MS-DOS," in the *Microsoft Windows NT Server Installation Guide.*
Using Network Client Administrator	Chapter 9, "Network Client Administrator," in the *Microsoft Windows NT Server Installation Guide.*

Lesson 2: Creating a Network Installation Disk

Before the client computer can start installing the appropriate software from the network, the client computer must be able to access the network. A network installation disk is used to boot the client computer, connect to a server, and start installing the selected client software.

This lesson explains how to use the Network Client Administration tool to create a network installation disk.

After this lesson you will be able to:

- Use the Network Client Administrator utility to share the network client installation files.
- Create a network installation startup disk.
- Use the network installation startup disk to install a network client.
- Install the Windows for Workgroups client over the network.

Estimated Completion Time: 40 minutes

Preparing the Network Client Share

Using the Network Client Administrator utility, the first step you must take in creating a network installation startup disk is to create a share on the Windows NT Server from which clients will be installed.

You can use three methods to access the network client installation files and create a network client installation startup disk or disk set:

- Share the \CLIENTS directory of the Windows NT Server 3.5 CD-ROM locally.
- Copy the network client installation files to a local hard disk and then access the files from there.
- Access the files on a network share point.

You start the process of creating a network installation startup disk from the Network Client Administrator.

To create a network installation startup disk, select the Make Network Installation Startup Disk and choose Continue. The Share Network Client Installation Files dialog box appears.

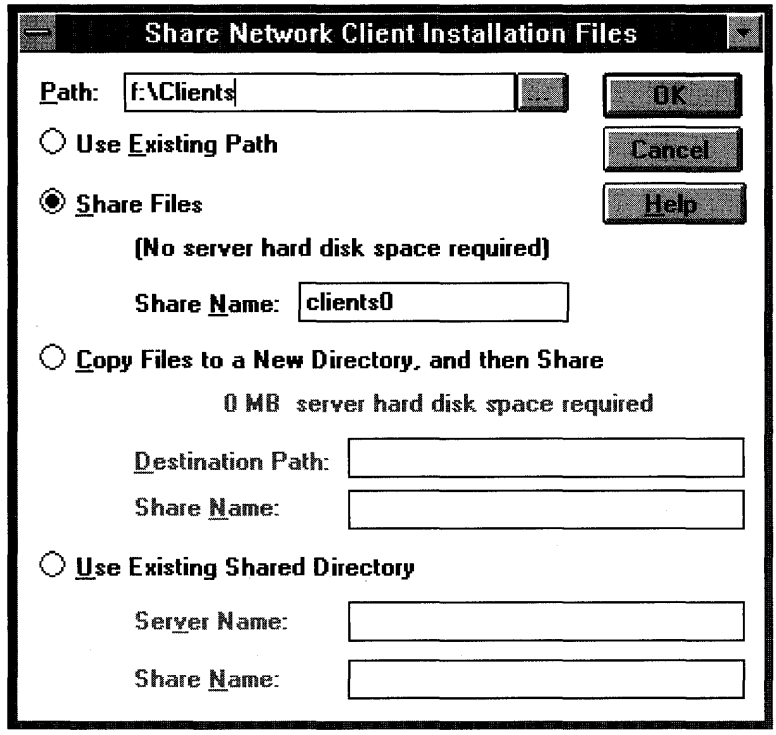


Figure 94: Share Network Client Installation Files dialog box

You use this dialog box to specify how the share should be configured.

Option	Description
Path	Specifies a path to the network client installation files to be used for creating the installation disk or disk set.
Use Existing Path	Directs the Network Client Administrator to use an existing path to the network client installation files. (Use if Network Client Administrator has already been used to create an installation disk or disk set.)
Share Files	Creates a share name for the network client installation files on the Windows NT Server CD-ROM.
Share Name	References the network client installation files on the Windows NT Server CD-ROM.

(continued)

Option	Description
Copy Files to a New Directory and then Share	Copies the files from the Windows NT Server CD-ROM to a local hard disk, and then shares for use. The Destination Path is the drive and directory in which to store the files on the local hard disk. The Share Name references the files on the local hard disk.
Use Existing Shared Directory	Uses an existing share containing the network client installation files. The Server Name is the name of the network server that contains the shared network client installation files. The Share Name is the name of the share at the Server Name that contains the network client installation files.

After the files have been shared, they do not have to be shared again, and you can begin creating network installation startup disks or installation disk sets.

The next step is to specify the configuration on the target workstations. When you chose OK from the Share Network Client Installation Files dialog box , the Target Workstation Configuration dialog box appears.

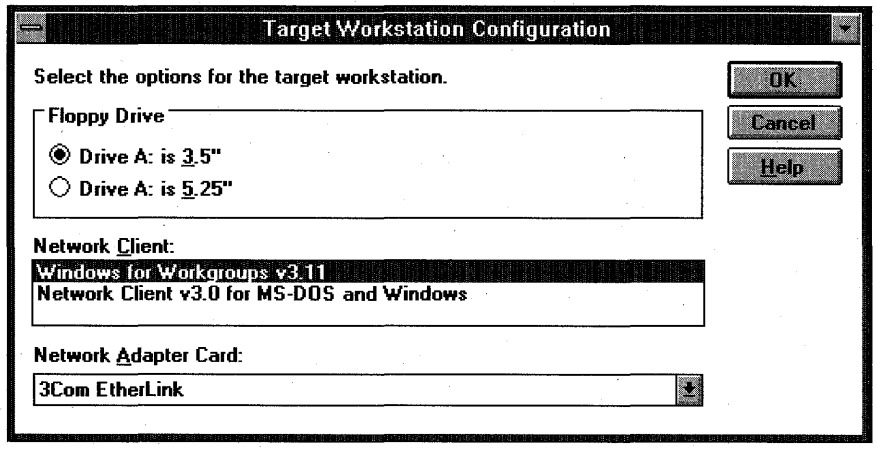


Figure 95: Target Workstation Configuration dialog box

This dialog box allows you to configure the workstation that will use the network installation startup disk. In this dialog box, specify the following information:

- The type of floppy drive to be used on the client computer
- The network client software to install on the client computer
- The type of network adapter installed in the client computer

When you choose OK, the Network Startup Disk Configuration dialog box appears.

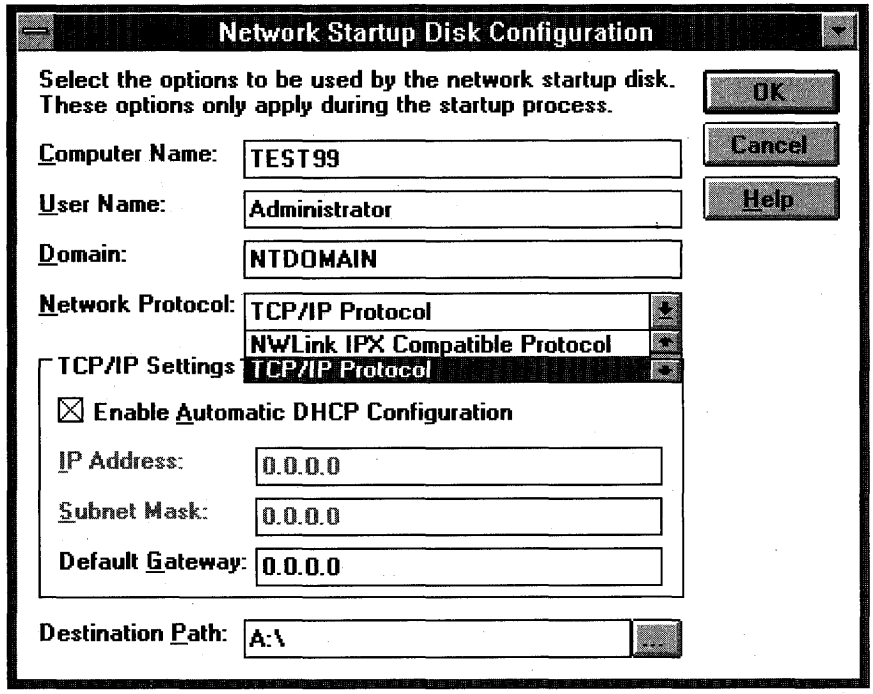


Figure 96: Network Startup Disk Configuration dialog box

This dialog box allows you to configure the network startup disk with the information required for a specific workstation. Complete the following information in this dialog box.

- Computer Name—The computer name that the network installation startup disk uses to start the network and connect to the file server.
- User Name—The user name that the network installation startup disk uses to log on to the network. The user account must have at least Read access to the share on the server.

- Domain—The Domain that the network installation startup disk uses to log on. (If you are using a workgroup user account, there is no need to type a domain name.)
- Network Protocol—To connect to the server, NetBEUI, NWLink, or TCP/IP can be used for the network installation startup disk. The installed client can be configured to use a different protocol than the one used by the installation startup disk. The following issues must be resolved depending on the protocol selected:
  - If the NWLink protocol is used, the Frame Type might have to be changed manually in the \NET\PROTOCOL.INI file on the network installation startup disk. By default, it is set to 802.2 for Ethernet adapters, but it might have to be changed for your frame type.
  - By default, a TCP/IP installation disk is configured as a DHCP client. If a DHCP Server has not been set up on the network, an IP address and subnet mask must be provided.
- Destination Path—The location on the network installation startup disk to which the startup files are copied.

When the process of creating the installation startup disk has been completed, a message appears to remind you to verify information, such as the configuration of the network adapter in the client workstation and the protocol that the installation disk will use.

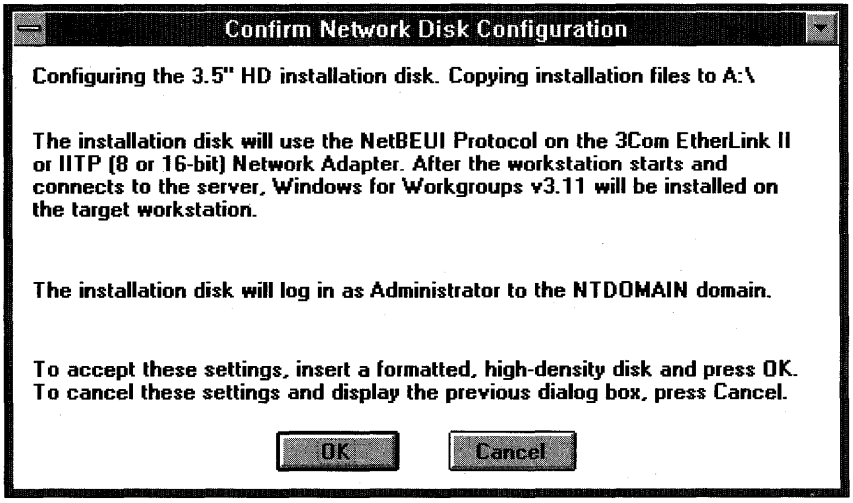


Figure 97: Confirm Network Disk Configuration message

Now that you have seen the basic steps, try creating a startup disk for your computer.

► To start the PDC-A computer as an MS-DOS computer

In this procedure, you shut down your PDC-A computer and then start it as an MS-DOS computer. You need 25 MB of free disk space on your MS-DOS–based computer to complete these procedures.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. Properly shut down your primary domain controller.
2. Restart your computer, and select MS-DOS as the operating system.

   Your computer is now started as an MS-DOS computer.
3. If you do not have 25 MB of free disk space, and the file C:\PAGEFILE.SYS exists, delete it to free additional disk space.
4. Format an MS-DOS system floppy disk (include the MS-DOS system files to make it bootable).

► To create a startup disk

In this procedure, you use Network Client Administrator to create a Startup Disk that downloads Windows for Workgroups onto your MS-DOS–based computer. You need your Configuration Table for this procedure.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

---

1. From the Network Administration group, start Network Client Administrator.

   The Network Client Administrator window appears.
2. Select Make Network Installation Startup Disk, and then choose Continue.

   The Share Network Client Installation Files dialog box appears. You use the client software installation files on the CD-ROM.
3. In the Path box, use the ellipse button to browse and select the \CLIENTS directory on the CD-ROM drive.
4. Select Share Files. The path should indicate the CD-ROM \CLIENTS directory.
5. In the Share Name box, type **clients** and then choose OK.

   The Target Workstation Configuration dialog box appears.
6. Under Floppy Drive, select Drive A for the correct type.
7. In the Network Client box, select Windows for Workgroups v3.11.

8. In the Network Adapter Card box, select your network adapter, and then choose OK.

   The Microsoft Windows for Workgroups Installation message appears.

9. Read the message, and then choose OK.

   The Network Startup Disk Configuration dialog box appears.

10. Complete the requested information, referring to the Configuration Table. The Computer name should be the name of your Windows for Workgroups workstation. Accept defaults of Administrator, DOMAIN-B, your network protocol, and the Destination Path.

11. Insert the MS-DOS system disk that you formatted earlier into drive A, and then choose OK.

    The Confirm Network Disk Configuration message appears.

12. Read the Confirmation box. To accept these settings, choose OK. If you have to make changes, choose Cancel to return to the Network Disk Configuration dialog box, and then make the necessary changes.

    The Copying Files message appears, followed by the Network Client Administrator message, indicating that the files were successfully copied.

13. Choose OK to return to the Network Client Administrator dialog box.

14. Choose Exit.

    The Network Client Administrator message appears, telling you to check certain items before starting the target workstation.

15. Read the information, and then choose OK.

► **To modify your startup disk**

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

It might be necessary to modify the PROTOCOL.INI file on your startup disk. For example, do this if your network adapter card is configured for any nondefault settings, or if you are using NWLink and your frame type is not 802.2. If you need to modify PROTOCOL.INI, do the following steps:

1. Use Notepad to edit A:\NET\PROTOCOL.INI.
2. Modify any parameters that are required.
3. Save the file and exit Notepad.

Important If you receive a message indicating low memory while using the installation startup disk, you should modify the CONFIG.SYS file to include DEVICE=HIMEM.SYS and add the DOS=HIGH setting.

In the following procedures, you use the startup disk created earlier to boot your MS-DOS computer and download Microsoft Windows for Workgroups 3.11.

Important Complete these procedures from the MS-DOS computer.

► To boot the MS-DOS workstation with the startup disk

1. Start your MS-DOS computer using the startup disk just created.
2. When prompted, press ENTER to log on as Administrator.
3. When prompted, press ENTER for no administrator password.
4. When prompted to create a password-list file, type **N** and then press ENTER.

   Your computer makes a connection to the server and runs the Windows for Workgroups setup program.

   The Windows for Workgroups 3.11 Setup dialog box appears.

► To install Windows for Workgroups

You need your Configuration Table for this procedure.

Important While completing this procedure, do not use default values for each value requested.

Complete an Express installation of Windows for Workgroups.

When prompted for...	Do this...
Windows for Workgroups directory	Type **c:\windows** and then press ENTER.
Printer Installation	Select your printer, if any, and then choose Install.
Network Setup	Choose Continue to install Microsoft Windows Network.
Adapter Card Settings (if this appears)	Select the correct value, and then choose OK.

(continued)

When prompted for...	Do this...
Microsoft Windows Network Names	Choose OK.
Set Up Applications	Choose Cancel.
Set Up Application PIFs	Choose Cancel.
Windows Setup	Choose Skip Tutorial.
Exit Windows Setup	Choose Restart Computer.

At the end of the installation, your computer restarts. Proceed to the next procedure immediately.

► To start your Windows for Workgroups computer

1. Remove the network installation disk from drive A.
2. At the Operating System Selection screen, choose MS-DOS.

   Your computer starts as an MS-DOS computer.
3. At a command prompt, type **win** and then press ENTER to start Windows for Workgroups.
4. Log on to your Windows for Workgroups computer as Administrator.

   The Windows for Workgroups dialog box appears, asking whether you want to create a password-list file.
5. Choose No.

   Your Windows for Workgroups computer is ready.

The Windows for Workgroups installation process does not automatically configure the computer for Windows NT Server domain validation. In the following procedures, you configure your Windows for Workgroups computer so that every time a user logs on, the user is validated by your domain controller.

Important Complete these procedures logged on as Administrator from your Windows for Workgroups computer.

► To configure for domain validation

1. From the Control Panel, start Network.
2. Choose Startup.

   The Startup Settings dialog box appears.
3. Under Options for Enterprise Networking, select Log On to Windows NT or LAN Manager Domain.
4. In the Domain Name box, type **domain-b** and then choose OK.
5. Choose OK to close the Microsoft Windows Network.

► **To test for domain validation**

1. In the Network group, start LogOn/Off to log off the computer.
2. If you have network connections, the Windows for Workgroups message appears, warning that logging off will disconnect you from shared resources. Choose Yes.

   The Log On/Off message appears.
3. Choose OK to acknowledge that you were logged off.
4. Start LogOn/Off to log on to Windows for Workgroups.
5. Log on to your computer as Administrator. Do not create a Password List file.

   The Domain Logon dialog box appears.
6. Choose OK to log on to the domain as Administrator.

   The Windows for Workgroups information box appears.
7. What message did you receive?

8. Choose OK.

   Your logon has been validated by your Windows NT Server domain controller.

Lesson Summary

The Network Client Administrator tool is useful when setting up clients that are not yet accessing the network. You can use this tool to create a share for the client installation files and to create a network installation startup disk, which allows you to access the share to perform the necessary installation.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What network client installation functions can be performed using the Network Client Administrator tool?

2. List three methods that can be used to share the network client installation files.

3. What information is required for the Network Startup Disk Configuration dialog box?

4. If you have a variety of machines with different floppy drive sizes and different network adapters, what is required when creating network installation startup disks?

For more information on	See
Installing Microsoft Network Client 3.0	Appendix A, "Microsoft Network Client 3.0 for MS-DOS," in the *Microsoft Windows NT Server Installation Guide.*

For online information about	From the Help menu, choose Contents and then
Sharing Network Client installation files	Network Client Administrator Help, select Make a Network Installation Startup Disk option, then Help.
Using Network Client Administrator to make an installation disk	Network Client Administrator Help, Make a Network Installation Startup Disk.

Lesson 3: Creating an Installation Disk Set

Sometimes you might not be able to access the network or the CD-ROM to perform the client installation. Although it is not generally recommended, you can still install client workstation software using an installation disk set. This lesson explains how to create an installation disk set.

After this lesson you will be able to:

- Use the Network Client Administrator to create an installation disk set for a specified client.

Estimated Completion Time: 5 minutes

Making an Installation Disk Set

Start the process of creating the installation disk set by selecting the Make Installation Disk Set. When you choose Continue, the Make Installation Disk Set dialog box appears.

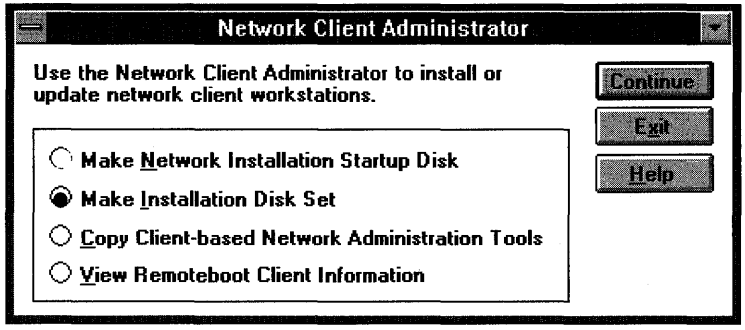


Figure 98: Network Client Administrator dialog box

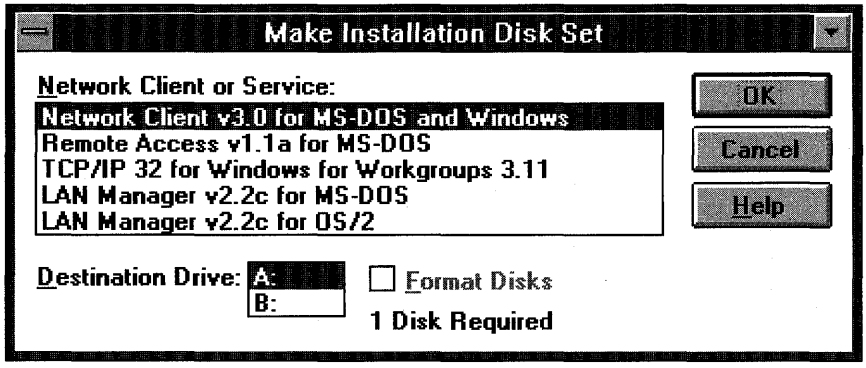


Figure 99: Make Installation Disk Set dialog box

You can use the Network Client Administrator utility to create installation disk sets for the following software:

- Microsoft Network Client 3.0 for MS-DOS (requires one 1.44 MB disk)
- Microsoft LAN Manager 2.2c for MS-DOS (requires four 1.44 MB disks)
- Microsoft LAN Manager 2.2c for OS/2 (requires four 1.44 MB disks)
- Remote Access Service 1.1a for MS-DOS (requires one 1.44 MB disk)
- Microsoft TCP/IP 32 for Windows for Workgroups 3.11 (requires one 1.44 MB disk)

You simply select the specific network client or service, and then choose OK. The appropriate files are copied to the disks. If required, you will be prompted when you need to insert additional disks.

The installation disk set you create can be used only for the specific client or service you selected. If you have multiple computers with different client(s) or service requirements, you must make separate installation disk sets for each network client or service.

Lesson Summary

Windows NT 3.5 Server can create installation disk sets for specific clients and services. You create these disk sets using the Network Client Administrator.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

- What disk sets can you make with Network Client Administrator?

For more information on	See
Using Network Client Administrator	Chapter 9, "Network Client Administrator," in the *Microsoft Windows NT Server Installation Guide.*
Installing Microsoft Network Client 3.0	Appendix A, "Microsoft Network Client 3.0 for MS-DOS," in the *Microsoft Windows NT Server Installation Guide.*

For online information about	From the Help menu, choose Contents and then
Using Network Client Administrator to make an installation disk	Network Client Administrator Help, Make a Network Installation Startup Disk.
Using Network Client Administrator to make an installation disk set	Network Client Administrator Help, Make a Network Installation Startup Disk.

Lesson 4: Client-Based Network Administration Tools

In addition to the Network Client Administrator, there are other administration tools included with Windows NT Server. There are tools for 32-bit and 16-bit Windows-based clients. This lesson explains how to use these tools to manage a domain from various workstations and clients.

After this lesson you will be able to:

- Describe the client-based network administration tools and the platforms on which the tools can be run.
- Use the Windows NT Server Tools to administer a Windows NT domain from a Windows 3.*x* or Windows for Workgroups client.

Estimated Completion Time: 30 minutes

Windows NT Server Tools for 32-bit Windows-Based Clients

The Windows NT Server Tools for 32-bit Windows-based clients allow a Windows NT Workstation computer to administer a Windows NT Server domain.

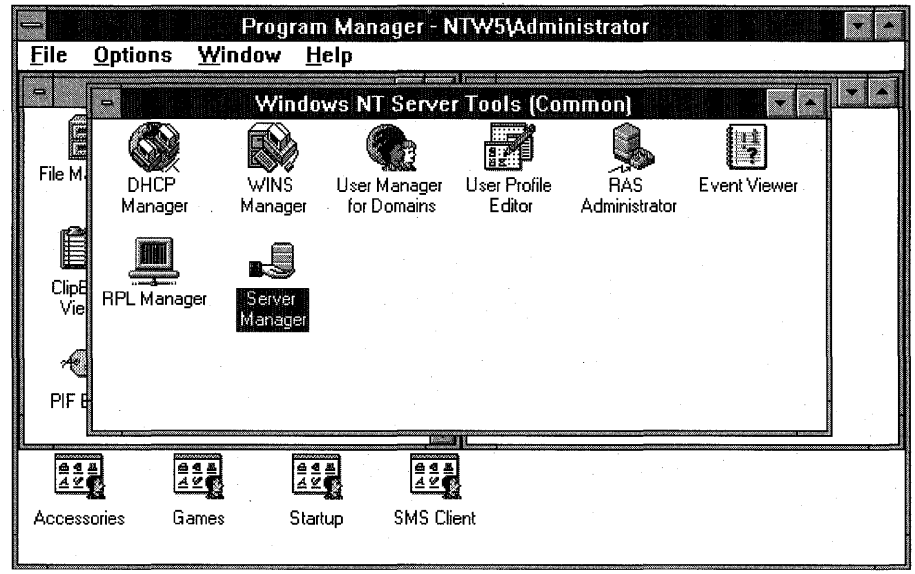


Figure 100: Windows NT Server Tools on a Windows NT 3.5 Workstation

The tools for 32-bit Windows-based clients include the following utilities:

- DHCP Manager—Used for DHCP server administration
- WINS Manager—Used for WINS server administration
- User Manager for Domains—Used to administer user and group accounts
- User Profile Editor—Used to create server-based user profiles
- Remote Access Administrator—Used to administer the Remote Access Service
- Event Viewer—Used to view the Windows NT Server event log
- Remoteboot Manager—Used to administer the remoteboot clients
- Server Manager—Used to manage Windows NT Server resources

To install the Windows NT Server Tools for Windows NT Workstation computers, run the SETUP.BAT file from the \CLIENTS\SRVTOOLS\WINNT directory. The Setup program does not create a program group or add the utilities. You must add them manually.

Win32s®

Win32s is an extension to 16-bit Windows. Using a subset of the Windows 32 API set, Win32s allows applications to run unmodified on both Windows 3.1 and Windows NT Server. The Win32s subset consists of Windows 32 equivalents of 16-bit Windows functions, as well as flat memory management and structured exception-handling features.

Converting the Windows NT Server Tools to Win32s allows the code to remain mainly 32-bit, eliminating the need to rewrite the utilities to 16-bit Windows. Because Win32s is a subset of 32-bit Windows, some of the features that the administration tools have while running under Windows NT Server might not be available with Win32s, such as MacFile and MacPrint.

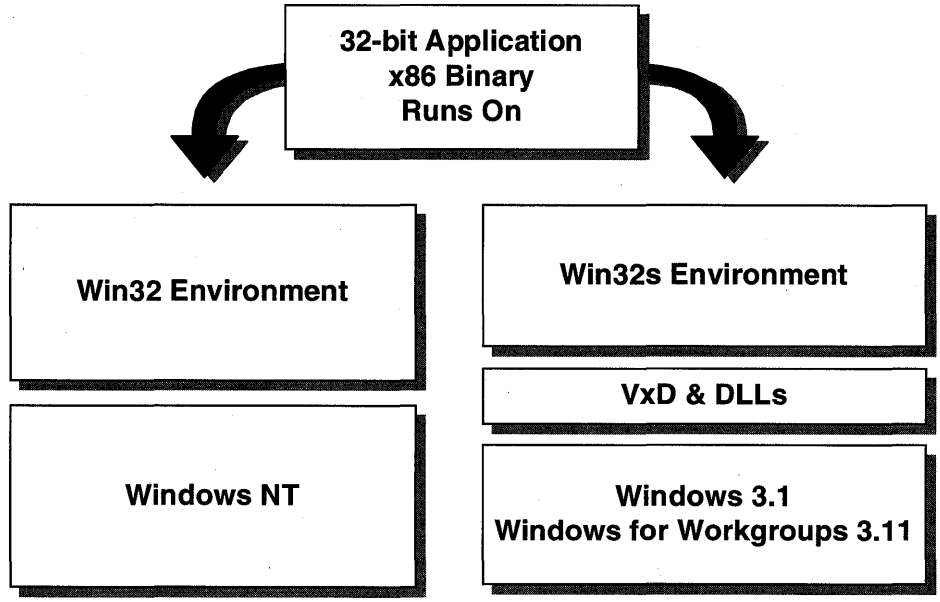


Figure 101: The Win32s environment

Win32s is basically a mapping layer that sits on top of 16-bit Windows functions. The Win32s mapping layer allows 32-bit Windows-based applications to make 32-bit calls to Windows 3.1. Win32s still depends on Windows 3.1 (or Windows for Workgroups) to provide all standard dialog controls such as list boxes, combo boxes, and edit controls. Win32s translates messages between the Windows 3.1 controls and the 32-bit Windows-based application.

Note For more information, see the Win32s Help file included in the *Microsoft Windows NT Software Developer's Kit (SDK).*

System Requirements

Because the Windows NT Server Tools require the Win32s subsystem, the tools have the following hardware and software requirements:

- Microsoft Windows 3.1 or Windows for Workgroups must run in 386 enhanced mode with paging enabled (386 enhanced mode requires an 80386 or higher processor)
- 8 MB of extended memory (more than what Win32s requires, but it is needed for the server tools)
- 5 MB of free hard disk space
- Installation of Microsoft network software

When a user installs the Windows NT Server Tools, Win32s is installed automatically. Because the Windows NT Server Tools require Win32s, the following issues must be addressed:

- Win32s requires virtual memory. It does not matter how much physical memory the system has. Windows must be set up with either a permanent or temporary swapfile for Win32s to work.
- In the CONFIG.SYS file, the Files parameter must be set to at least 50.
- A Win32s subdirectory containing essential drivers is created under the SYSTEM directory. These drivers must not be deleted.

The Windows NT Server Tools for 16-bit Windows-Based Clients

As you have seen, Windows NT Server Tools facilitate the administration of a Windows NT domain. The tools for 16-bit Windows-based clients in some cases provide functionality different from the tools for 32-bit Windows-based clients.

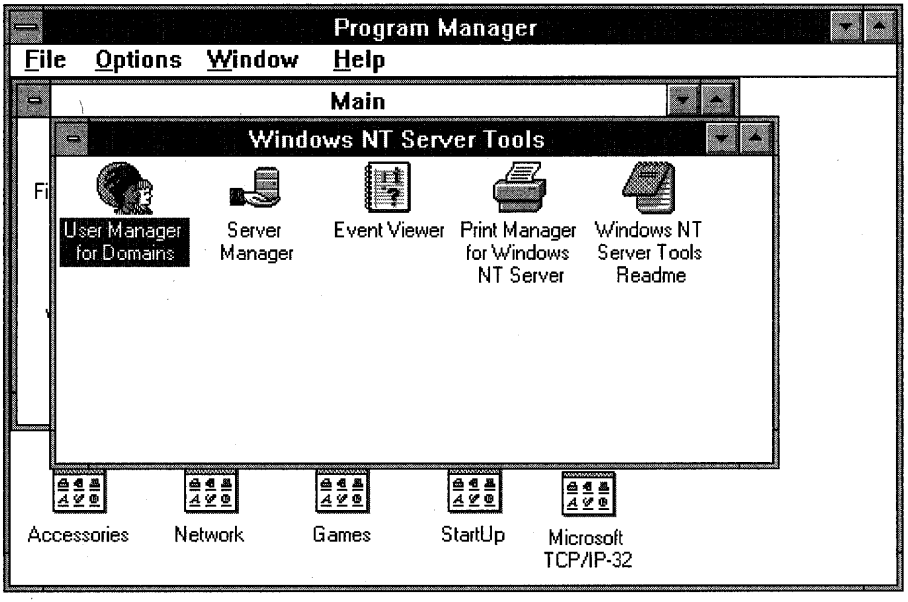


Figure 102: Windows NT Server Tools on a Windows for Workgroups computer

Most of the tools function exactly the same on Windows 3.1, Windows for Workgroups 3.11, and Windows NT Workstation. The following is a list of the tools, as well as information about the tools that are different from the Windows NT 32-bit version:

- User Manager for Domains—Used to administer user and group accounts.
- Server Manager—Used to create and remove shares on Windows NT systems.
- Event Viewer—Used to view the Windows NT Server event log.
- Print Manager for Windows NT Server—Allows users to monitor and control Windows NT printers. This Print Manager works only on Windows NT printers and does not provide any local printer management. The local Windows 3.*x* Print Manager must be used for local printer management.
- File Manager Security menu—Used to control file-level permissions on a Windows NT Server NTFS partition.

  The installation of Windows NT Server Tools modifies the Windows 3.1 or Windows for Workgroups File Manager to add a Security menu similar to the one in the Windows NT File Manager. This allows an administrator on a 16-bit Windows-based client to control file level permissions on a server's NTFS drives.

► **To share client-based Network Administration Tools**

In this procedure, you share the Network Administration Tools on your primary domain controller.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

---

1. Start Network Client Administrator.
2. Select Copy Client-based Network Administration Tools, and then choose Continue.

   The Share Client-based Administration Tools dialog box appears.
3. In the Path box, use the ellipse button to browse and select the \CLIENTS\SRVTOOLS directory on the CD-ROM drive.
4. Select Share Files. The path should indicate the CD-ROM drive's \CLIENTS\SRVTOOLS directory. The Share Name defaults to SETUPADM.
5. Choose OK to accept the suggested share name of SETUPADM.

   The Network Client Administrator message appears, indicating that the Network Administration Tools are now available on a shared directory.
6. Choose OK.

► To load Server Tools onto your Windows for Workgroups computer

In this procedure, you install Server Tools on your Windows for Workgroups client.

Important Complete this procedure logged on as Administrator from your Windows for Workgroups computer.

---

1. Use File Manager to connect to \\PDC-B\SETUPADM.
2. From the network drive's \WINDOWS directory, run SETUP.EXE.

   The Windows NT Server Tools Setup screen appears with the Welcome dialog box.
3. Choose Continue to proceed.

   The Installation Options dialog box appears, with the Install All Files option selected and a Base Installation Path of C:\SRVTOOLS\.
4. Choose Continue to install all files in your C:\SRVTOOLS directory.

   The Time Zone Setup dialog box appears.
5. In the Time Zone box, select your time zone, and then choose Continue.

   The Microsoft Win32s Setup Target Directory dialog box appears.
6. Choose Continue.

   Files are copied onto your workstation. When complete, the Windows NT Server Tools Setup information box appears, indicating the need to add information to your AUTOEXEC.BAT and CONFIG.SYS files.
7. Choose OK to acknowledge the message.

   A message appears indicating successful installation and telling you that your system will restart.
8. Choose Continue.

   Your computer restarts.

► To modify AUTOEXEC.BAT and CONFIG.SYS

In this procedure, you modify your CONFIG.SYS and AUTOEXEC.BAT files to include configuration settings as recommended when using the 16-bit Server Tools on a Windows for Workgroups computer.

Important Complete this procedure from your Windows for Workgroups computer.

---

1. Log on to the computer and the domain as Administrator.
2. Edit C:\AUTOEXEC.BAT. Add the new information that appears in C:\SRVTOOLS\NEW-VARS.BAT.

3. Edit C:\CONFIG.SYS. Add the new information that appears in C:\SRVTOOLS\NEW-CONF.SYS.
4. Exit Windows for Workgroups.
5. Restart your Windows for Workgroups computer as an MS-DOS computer.
6. Start Windows for Workgroups.
7. Log on to the computer and the domain as Administrator.

The server tools are now installed and will function on your Windows for Workgroups computer.

In the following procedures, you use the server tools on your Windows for Workgroups client to administer your Windows NT Server PDC.

Important Complete these procedures logged on as Administrator from your Windows for Workgroups computer.

► **To use Server Manager**

1. From the Windows NT Server Tools group, start Server Manager.
2. Select PDC-B.
3. From the Computer menu, choose Shared Directories.
4. Create a new share on PDC-B.
5. Exit Server Manager.

► **To use User Manager for Domains**

1. From the Windows NT Server Tools group, start User Manager for Domains.
2. Create a new user in your domain named USERB-5 by copying USERB-4.
3. What did you need to do before the user was created?

4. Exit User Manager for Domains.

▶ **To use File Manager**

1. Start File Manager.
2. What menu is new after installing Server Tools that allows you to set permissions on NTFS drives on a Windows NT Server computer?

3. Exit File Manager.
4. Exit Windows for Workgroups.
5. Restart your computer as the Windows NT Server primary domain controller for DOMAIN-A.

Lesson Summary

The Windows NT Server Tools can be used from both 32-bit based systems and 16-bit based systems such as Windows for Workgroups. With the use of Win32s, there are minimal differences in the function of the tools.

Review Question

The following question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- From what location(s) can the Windows NT Server Tools be used to administer a Windows NT domain?

CHAPTER 10

Optimizing Windows NT Server for Performance

Before You Begin

You must have completed Chapter 1. Additionally, you need a second computer running Windows NT Server. To have this second computer, you need to complete either Chapter 4 or Chapter 5; in Chapter 4, you install a backup domain controller; in Chapter 5, you install a primary domain controller in an additional domain.

You also need the lesson disk to do this chapter.

Lesson 1: Introduction to Performance Monitoring

As you have learned in earlier chapters, Windows NT Server has many built-in features that allow you to customize your network to suit the needs of your company most efficiently.

Through the Performance Monitor application you can further determine where to fine-tune your system operation, *on an ongoing basis*, and adjust it to the changing needs of your business environment.

After this lesson you will be able to:

- List four performance goals of performance optimization.
- Describe the uses of the Performance Monitor application.
- Identify the Performance Monitor components.
- Identify the four Performance Monitor views.

Estimated Completion Time: 45 minutes

Monitoring Performance

Windows NT Server provides automatic performance monitoring and optimization features through its self-monitoring capabilities. Windows NT Server can optimize itself for generic problems, dynamically adjusting its configuration and redistributing its resources.

In addition, Windows NT Server includes a tool to help you monitor and track various network behaviors. This tool generates logs and statistics that you can use to identify and eliminate the source of any problems.

This versatile program is called the Performance Monitor.

- It allows you to analyze operation in both real time and recorded time.
- It can look at isolated processors, hard disks, memory utilization, and processes.
- It can look at the system as a whole.
- It can perform these functions separately or simultaneously.

In short, it gives you a comprehensive picture of system performance in the time frame of your choice.

Performance Baseline

Establishing a baseline is a necessary first step in monitoring performance. By maintaining a record of system performance in normal operation, you can build an understanding of reasonable performance values. With this record, you have a baseline for comparison when things change or when something has to be upgraded or replaced. Without this baseline, problem detection can be elusive.

In Lesson 2, you learn how to establish this baseline.

Optimizing Performance

After you have established a baseline, you can monitor system performance and compare current results with your baseline. If the results of your analysis indicate a need to improve a specific performance area, you can optimize the performance. Performance optimization is the process of working with existing resources to maximize performance, resulting in:

- More speed for a specific process.
- Better processor sharing for multiple processes.
- More memory.
- More available hard disk space.

When optimizing a Windows NT Server computer, you start with a given set of resources with regard to processor speed, physical RAM, and hard disk space. Then you optimize performance by setting priorities for these resources and determining the appropriate balance. For example, if memory is the priority, you can increase the virtual paging file; however, doing so decreases the amount of hard disk space available. The performance areas are interdependent, so if you change performance in one area it can affect performance in another area.

If performance has to be improved in *all* areas, consider adding resources, such as upgrading the processor, adding RAM, or adding a hard drive.

Computing tasks can require multiple devices to perform a specific transaction. Each device uses a resource to perform its part of the transaction. Poor performance results when one of these devices requires noticeably more resources than the others to complete its task.

To fix a problem, you must identify the devices that are taking the greatest amount of time to process a transaction.

Optimization Terms

Before we get too far, we will define some terminology. The following are some common terms you will encounter.

Bottleneck

A *bottleneck* in a system is a device that consumes the most time during a task. Identifying the bottleneck is crucial to improving system performance.

Device

Every physical component within a computing environment should be considered a *device*. The devices that tend to become primary bottlenecks are the processor, memory, disk drive, controller, and network card.

Task

A *task* is any kind of operation. Examples of tasks are updating a Microsoft Excel worksheet or sending an electronic mail message.

Working Set

A *working set* is the memory (RAM) that a process uses while it is running.

Capacity Planning

When you optimize performance, you make adjustments that improve performance of the *existing* network configuration. Also, because of all the information you are able to gather from system operation, you can make truly informed decisions about capacity *forecasting*. Through Performance Monitor, you can:

- Track capacity limits for future planning.
- Maintain adequate hardware resources.
- Detect system limitations.

The Performance Monitor Tool

The Performance Monitor tool is designed to track real-time computer activity to identify most performance bottlenecks. (It is exactly the same tool that is included with Microsoft Windows NT Workstation.)

As stated earlier, Performance Monitor also gives you the data needed to take a historical view of system operation.

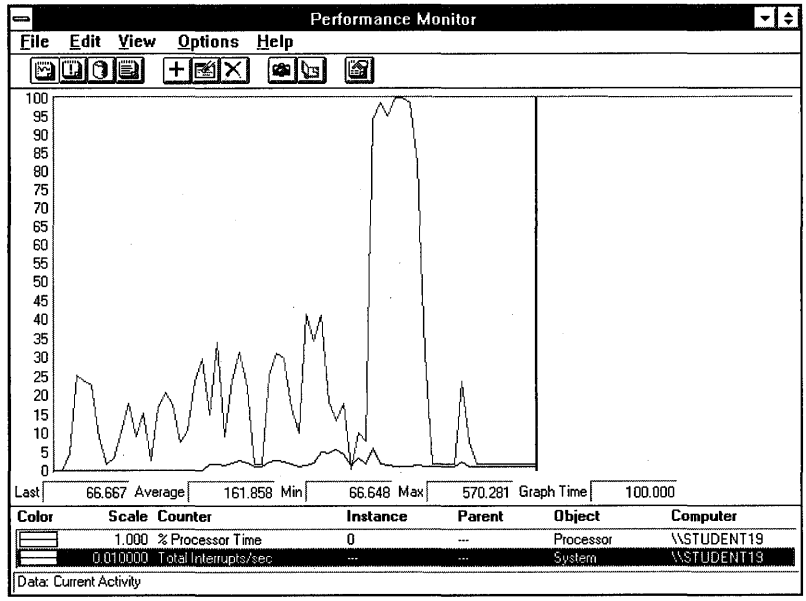


Figure 103: A Performance Monitor chart

Performance Monitor is based on a series of counters that record such things as:

- The number of processes waiting for disk time.
- The number of network packets transmitted per second.
- The percentage of processor utilization.

Uses of Performance Monitor

Performance Monitor generates useful information by:

- Monitoring real-time and historical performance.
- Identifying trends over time.
- Identifying bottlenecks.
- Monitoring the effects of system configuration changes.
- Determining system capacity.
- Monitoring local or remote computers.
- Notifying administrators of significant monitored events that exceed threshold values.

Overview of Performance Monitor Components

Performance Monitor's operation is based on behaviors of the following:

- Objects—standard mechanisms for identifying and using a system resource. Typically, objects represent a general category or type (such as processors).
- Counters—individual pieces of data that you want to monitor for that object.
- Instances—multiple occurrences of an object.

Take a look at the following figure to see how these factors might appear in Performance Monitor.

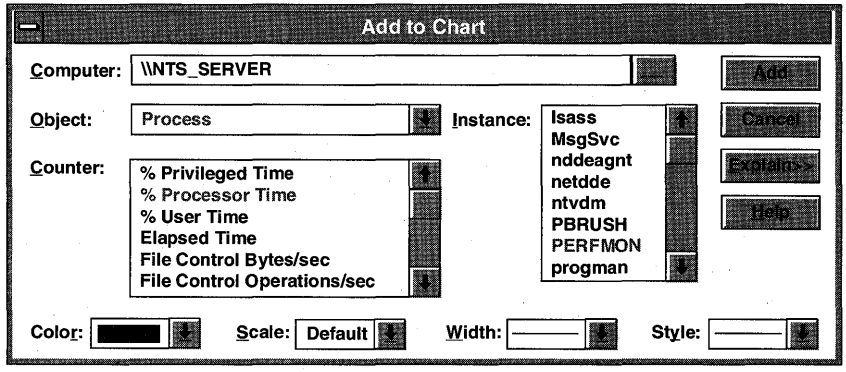


Figure 104: Add to Chart dialog box

In this example, **Process** is an object, **% Processor Time** is a counter for the object Process, and **PERFMON** is an instance of the object Process.

The counters generate numbers, and from these numbers Performance Monitor produces statistics. Collected over time, counter statistics show performance trends that can help you troubleshoot and optimize the network. These statistics are also useful in projecting network expansion.

Let's take a closer look at these components.

Objects

A Windows NT object is a standard mechanism for identifying and using a system resource. Objects are created to group measurable units of activity, resulting in object *types*, which can represent sections of shared memory, physical devices, or processes.

A Windows NT process is created whenever a program runs. A process can be one of the following:

- An application (such as Notepad)
- A service (such as the Spooler)
- A subsystem (such as POSIX)

Some Objects That Can Be Viewed

The following table lists some of the objects that can be viewed.

Browser	NetBEUI Resource*	Processor
Cache	Network Interface*	RAS Port*
Gateway Service for NetWare	Network Monitor Statistics*	RAS Total*
FTP Server*	Network Segment*	Redirector
ICMP*	NWLink IPX*	Server
IP*	NWLink NetBIOS*	System
Logical disk	Objects	TCP*
Memory	Paging File	Thread
NBT Connection*	Physical disk	UDP*
NetBEUI*	Process	WINS Server*

*these objects will appear only if the corresponding component is installed.

Counters

Each of these objects has subcategories called counters, which generate data about aspects of an object's performance. Counters can also be monitored; in fact, Performance Monitor actually reports on the counters instead of the objects.

Counters usually include a reference to their object and are written as OBJECT:COUNTER. For example, PROCESSOR:%PROCESSOR TIME tracks the percent of utilization for a given processor.

Performance Monitor allows you to view an explanation of each counter, as shown in the following figure.

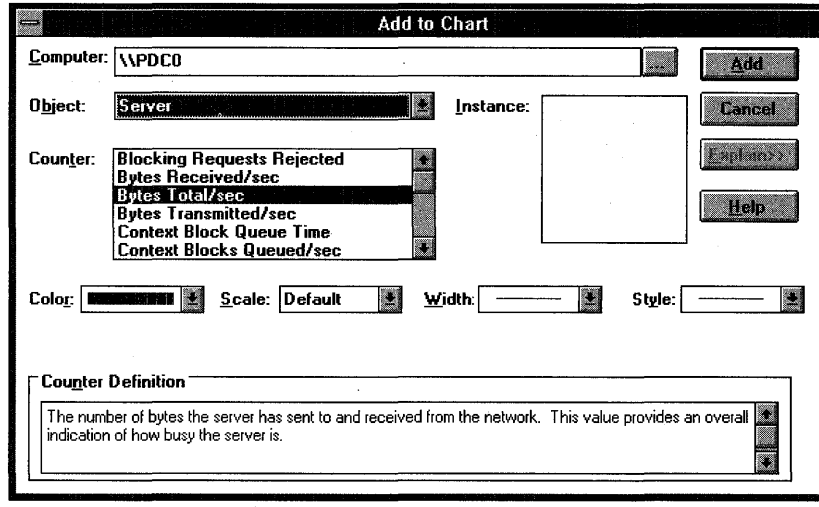


Figure 105: A counter definition

Note Choose Explain to receive a description of a counter.

There are more than 350 counters available in Performance Monitor. Not all objects and counters are automatically installed when Windows NT Server is installed. Some objects and counters are added when a specific Windows NT Server component (such as TCP/IP Protocol) or a Windows NT application or service (such as SQL Server) is installed. In the previous table, all of the objects marked with an asterisk are installed when the appropriate software is installed on the computer.

Note For a list of available counters and the levels of expertise needed to implement them, see the *Microsoft Windows NT Resource Kit.*

Counters for Monitoring the System

The following table shows some important counters that you should monitor on Windows NT Server.

Object type	Counter	What to look for
Processor	% Processor Time	If this value is consistently high (>80%) and disk and network counter values are low, suspect the processor as being the system bottleneck.
Physical Disk	% Disk Time	If this value is consistently high and Disk Queue Length is greater than two, suspect that the disk is the bottleneck in the system.
Memory	Pages/sec	If counter value is consistently above your baseline, suspect memory as the system bottleneck.
Server	Bytes Total/sec	If the sum of Bytes Total /sec for all servers is roughly equal to the maximum transfer rates of your network, you might have to segment the network.

Counters for Monitoring an Application

The following counters are especially helpful in identifying how a process is using resources. They present a reasonable overview of total system use by any given application, and they can tell you how various applications use memory, the processor, and the hard disk.

% Processor Time The percentage of elapsed time that a processor executes a task for a particular process.

Working Set The current number of memory bytes used by, or allocated to, a process. This value could be larger than the minimum number of bytes actually needed by the process.

Capacity Planning Counters

Counters are helpful in forecasting equipment needs, giving you advance notice of when you might need to add additional resources.

To do capacity planning, you must take system measurements on a regular basis. To start, you might try this schedule:

- Begin by logging at five-minute intervals throughout the day.
- Then create new log files, increasing the intervals to 15 minutes.
- Select Time Window from the Edit menu to focus on the most active two hours of the day. To view a portion of a chart, adjust the beginning time bar or ending time bar to shorten the period of time displayed.
- Create an ongoing archive of log files containing this information.

The following table lists capacity planning counters. Notice that some of the counters appearing here are also listed in the previous table. There are many ways to use the same object:counter instances to analyze performance.

Object type	Counter
Processor	% Processor Time, Interrupts/sec
System	File Data Operations/sec
Memory	Pages/sec, Cache Faults/sec, Available Bytes
Server	Bytes Total /sec
Physical Disk	% Disk Time, Avg. Disk sec/Transfer
Logical Disk	% Free Space

Adding a Counter

To add a counter, select it from the existing list of counters and then add it to a chart, log, report, or alert view for monitoring.

You can also install new counters in Performance Monitor by adding Windows NT components or Windows NT applications. For example, installing TCP/IP as a protocol adds a large number of counters that can be used for additional monitoring.

Instances

An instance is an occurrence of an object and counter. The object and counter created for a process can have many instances—one for each active process. For example, when four processes are active at once, Performance Monitor generates four instances, one to monitor each process.

Object and counter instances can reference not only software, such as processes, but also hardware components, such as hard disks and processors. Each of these object and counter pairs can have multiple instances. For example, the Processor object type will have multiple instances if a system has multiple processors. If an object type has multiple instances, each instance can use the same set of counters, but each instance using that counter must be added to your chart or log.

Addresses and Threads

In addition to an executable program, every process consists of a set of virtual memory addresses and at least one thread.

Threads are objects that execute program instructions within processes. They are, in fact, the smallest pieces of executable code. Generally, a thread is a component of an application. An example of this is Autosave in Microsoft Word.

Threads make it possible for different parts of a process to execute on separate processors simultaneously. Each thread running on a system shows up as an instance for the thread object type, and it is also identified with its parent process. You can see this in the following example. The PERFMON instance of the Process object is the parent of the two PERFMON instances of the Thread object.

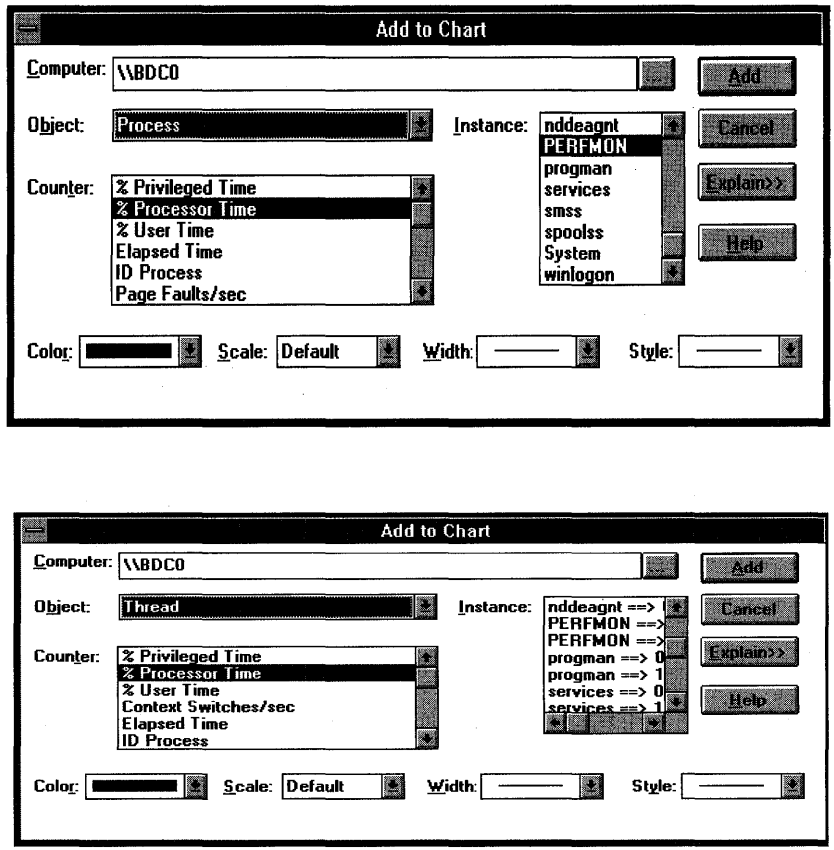


Figure 106: Relationship of processes and threads

Exporting Performance Data

The data produced by Performance Monitor does not have to stay within the confines of the program. You can export Performance Monitor counter data to other products, such as spreadsheets and databases, for further data analysis and capacity planning.

Of course, Performance Monitor does provide you with several internal means to view data. You will see these in the next section.

Viewing Performance Monitor Data

To accomplish its tasks and let users see the information it generates, Performance Monitor offers four "views" of information: charts, logs, reports, and alerts.

The Chart View

You use this view for a quick glance at what is going on in your system in real time or historical time.

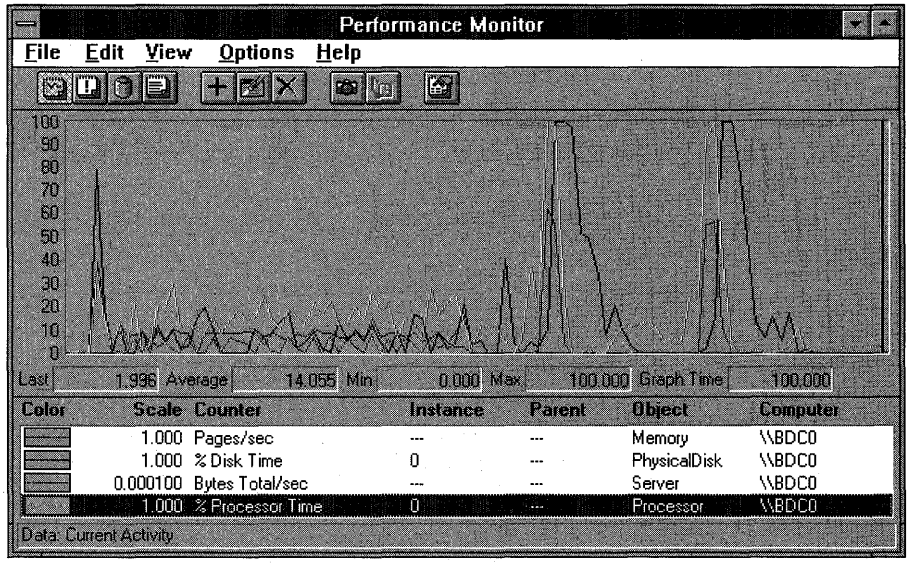


Figure 107: A chart view

Charts provide a way to investigate:

- Why an application is performing poorly.
- Intermittent performance problems.
- Where increased capacity (memory, hard-disk storage, and so on) would be useful.

Many counters can be charted at one time, displaying the counters' values over the entire time the chart is active.

The Log View

You log data to a file over a period of time, so you can predict long-term trends and troubleshoot short-term problems.

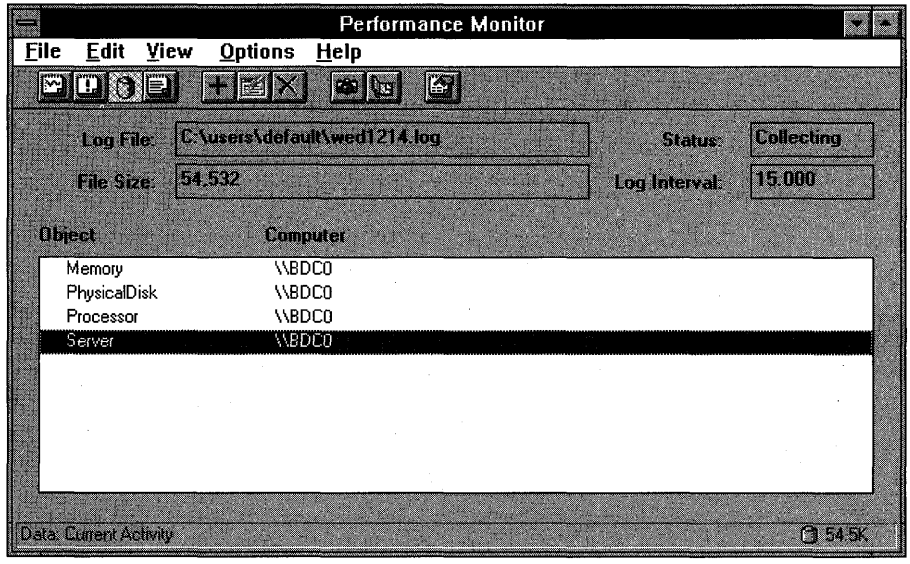


Figure 108: A log view

You log object data to disk. After objects are logged, you can feed the log file back into the Performance Monitor to create charts, reports, or alerts from the logged data. All counters for each object are automatically collected.

Charts present only a one-dimensional picture of system activity; logs can reveal the true nature of a system's behavior, under different conditions, by showing data for long-term trend analysis.

The Report View

You can use the report view to see constantly changing values in a summary format. You can also use it to view historical averages.

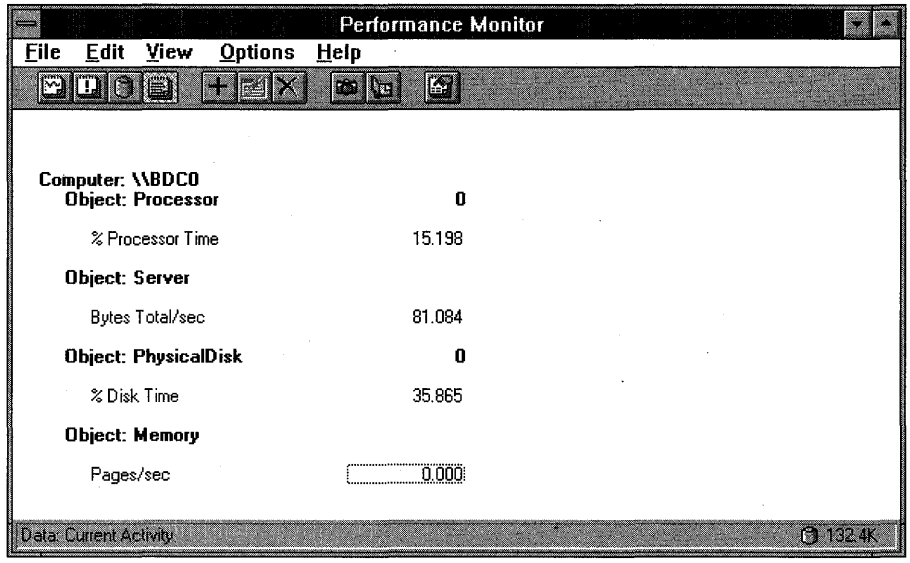


Figure 109: A report view

Reports allow monitoring of real-time performance of selected counters. The reports present the values of the counters in a columnar format. You can create a report of *all* counters in Performance Monitor.

The Alert View

Real-time alerts allow you to continue working while Performance Monitor tracks events.

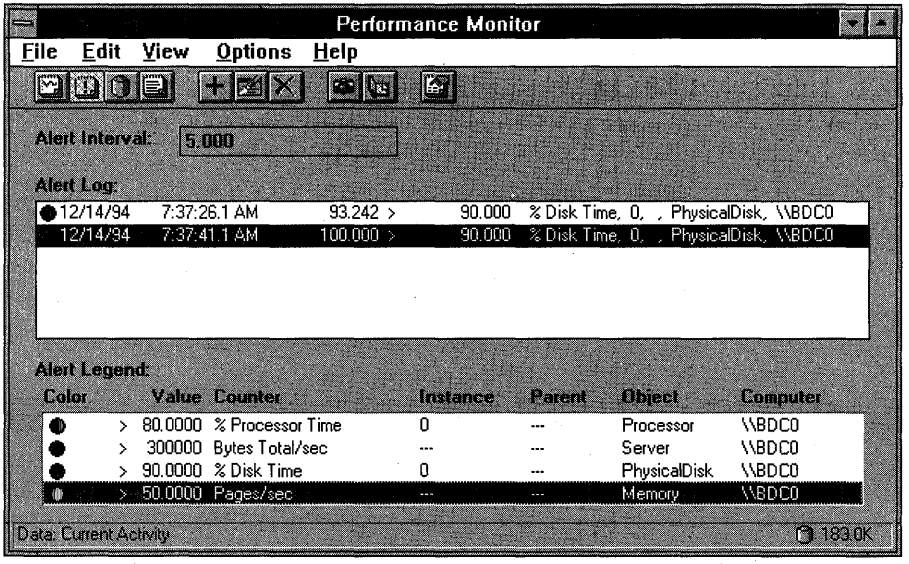


Figure 110: An alert view

You can set an alert on a counter. When the counter exceeds this value, Performance Monitor notifies you by displaying the event.

Notification can occur the *first* time a counter exceeds the given value or *each* time it exceeds the value. A maximum of 1000 events are recorded in the alert view. Above that number, the oldest alert event is deleted when a new alert occurs.

The alert view also allows you to monitor many alerts at one time.

Frequency for Updating Information

You can use Update Time Interval settings to determine how often Performance Monitor updates information in logs, graphs, alerts, and reports.

As information is updated at the Update Time Interval period, each of the values is an average of the last two data reads, separated by the length of the time interval.

Update Time Interval settings can also affect the amount of memory and the processor time used by Performance Monitor. For example, if you set the Update Time Interval to update every one second for a log, this means more processor time, memory, and hard disk space will all be needed to log the values for the counters.

Lesson Summary

One of the goals of a system administrator is to achieve the maximum performance possible out of the computer. When attempting to gain better performance in one area, performance can often decline in another. The Performance Monitor tool of Windows NT assists you in monitoring specific objects, counters, and instances in an attempt to analyze current system performance. By using the information provided in Performance Monitor, you can achieve the most effective performance optimization.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to monitor performance to determine whether your server has reached capacity. What is the first step in analyzing a computer's performance?

2. You have to determine whether your system performance will decline after adding an additional 20 users to the server. How can you figure out whether this will happen?

For more information on	See
Monitoring system usage	Chapter 9, "Monitoring Network Activity and Performance," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
Using Performance Monitor	Chapter 9, "Monitoring Network Activity and Performance," in the *Microsoft Windows NT Server Concepts and Planning Guide.* Chapter 11, "Monitoring Performance," in the *Microsoft Windows NT Server Network Operations Quick Reference.* Chapter 19, "Performance Monitor," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Creating a Chart	Performance Monitor Help, Chart Current Activity.
	Performance Monitor Help, Work with Existing Log Files.
Creating a Log	Performance Monitor Help, Log Current Activity.
Creating a Report	Performance Monitor Help, Create Reports on Current Activity.
	Performance Monitor Help, Work with Existing Log Files.
Creating Alerts	Performance Monitor Help, Set Alerts on Current Activity.
	Performance Monitor Help, Work with Existing Log Files.

Lesson 2: Monitoring Processor and Disk Activities

When you are monitoring, the primary performance indicator you look for is a *bottleneck* where the flow of work is restricted. Detecting the bottleneck involves isolating the hardware component that is responsible for it. It is also helpful to identify the software component that is generating all the activity. In this detection work it soon becomes readily apparent that you have to look at the system as a whole. To begin monitoring, determine how resources are being used.

First, find out how user applications interact with each of the key resources. Then assess the overall load on each resource. This includes monitoring the following:

- Processor activity
- Disk activity
- Memory
- Network activity
- The Workstation service
- The Server service

In this lesson, you learn about processor and disk activities. Lessons 3 and 4 cover the rest of the resources.

After this lesson you will be able to:

- Identify key processor counters.
- Establish a benchmark.
- Troubleshoot a bottleneck.
- Create a report.
- Create a chart.
- Identify key disk counters.
- Compute average disk queue time.
- Identify ways to improve disk performance.

Estimated Completion Time: 45 minutes

Processor Activity

Most monitoring includes processor activity, because every running task in the system requires processor time to execute.

Because the processor is always executing some instruction, the processor time is theoretically always 100 percent. However, blocks of code known as "idle threads" simply perform low-level system tasks and wait for the next event or interrupt to occur, so that any other thread (all threads with higher priority) can be executed.

Because the processor is involved in every attempt by a user to access a computer, monitoring the processor can give a good picture of how the computer as a whole is being used.

Two objects within Performance Monitor provide important information about processor activity:

- System—tracks processor(s) use on a system-wide level.
- Processor—tracks processor use on a processor-by-processor level.

Note On a single-processor system, these values are the same.

Processor Counters

To determine whether the processor is the real bottleneck, you look at three primary counters.

Object	Counter	Purpose	Threshold Guidelines
Processor	% Processor Time	Activity of CPU	>80%—upgrade
Processor	Interrupts/sec	Device service requests	Monitor for increases without processor stress (hardware problem)
System	Processor Queue Length	Number of Threads waiting to be processed	>2

Figure 111: Processor counters

% Processor Time

The % Processor Time counter indicates how busy a processor is. It shows the percentage of elapsed time a processor has spent executing nonidle threads. Generally, if the sustained use of the processor is greater than 80 percent, you might have to reallocate resources to other computers, upgrade the existing processor, or add an additional processor.

Interrupts/sec

The Interrupts/sec counter, which measures the rate of service requests from I/O devices, is also an important processor counter. A dramatic increase in this counter value, without a corresponding increase in system activity, indicates a hardware problem.

Processor Queue Length

The number of threads indicated by the processor queue length is significant because each thread requires a certain number of processor cycles. If demand exceeds supply, long processor queues develop and system response suffers. A sustained processor queue length greater than two generally indicates that the processor is a bottleneck. (This counter is always zero unless you monitor a thread counter as well.)

Processor Spikes

During some operations (such as initialization of an application, a compile, or a worksheet recalculation), the system can experience spikes that approach 100 percent. If such a spike occurs, but it is followed by a return to a more reasonable level, between zero and 80 percent, the processor is probably not the bottleneck in the system.

The Processor As a Bottleneck

The processor does not become a bottleneck until the *total* processor sustains nearly 80 percent utilization. When processor use approaches 100 percent, it can indicate that the processor is inadequate. A second processor, or a faster one, might solve the problem. However, acceptable processor use can depend on computer activity. For instance, sustained processor use above 80 percent would seem to indicate the need for an upgrade. Yet percentages can vary, depending on expected system performance and processor type. Other factors should be considered before deciding on a processor upgrade.

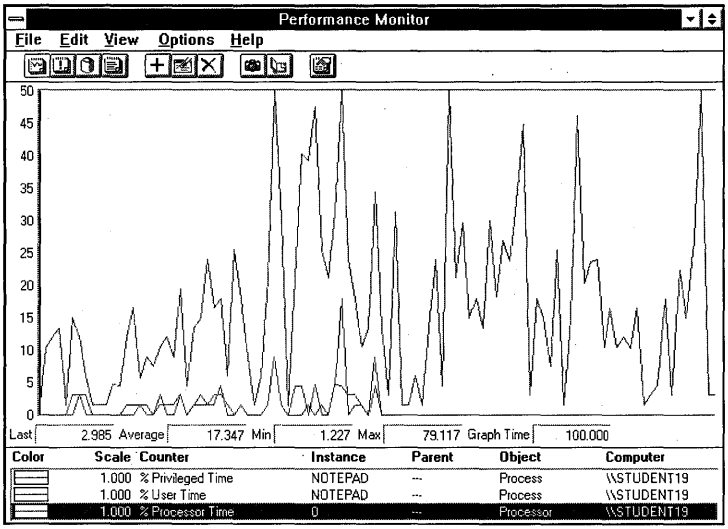


Figure 112: Processor:% Processor Time

For example, if a task takes three seconds, of which one second is spent running the program in the processor and two seconds are spent trying to read the data from the disk, then the disk is the bottleneck. Replacing the processor with one twice as fast would reduce the time to only 2.5 seconds, but it would not help in a significant way because it would not remove the bottleneck. The disk would still take two seconds. If you purchased a disk and a controller that were twice as fast, the time would drop to two seconds.

To find out whether an upgrade is needed, use the Performance Monitor to chart Processor:% Processor Time for all processes. This counter tracks the amount of time that the processor is not processing idle threads. If it turns out that more than a couple of processes are contending for the majority of the processor time, then a faster processor, or an additional processor in a multiprocessor computer, should be considered.

Two additional counters offer important information regarding processor activity:

- % Privileged Time—the amount of time the processor spends executing in *privileged* mode. Privileged mode is synonymous with executive mode time and does not include time spent in idle thread(s).
- % User Time—the amount of time the processor spends executing in *user* mode. This also does not include time spent in idle thread(s).

Troubleshooting

Let's see how these factors work in troubleshooting a system problem. You use three view modes of the Performance Monitor to check for:

- Bottleneck Detection—Identify devices that have become performance bottlenecks, and identify the processes that are loading those devices and causing the bottleneck.
- Design Verification—Test an application to determine whether it uses resources correctly, efficiently, and fairly.
- Capacity Planning—Determine the load level under which resources (such as main memory) will cause a bottleneck. Determine the resource level required to reduce or eliminate bottlenecks under "standard load."
- Design Prediction—Monitor performance variations that occur as an application uses optional methods to assess system resources (such as disk or cache).

Preparing Your Computer

First, you need to prepare your computer by:

- Identifying a logical drive with sufficient free space.
- Copying performance utilities and files to your hard disk.
- Creating a large performance-testing file.
- Turning on disk counters.

This preparation is a prerequisite for all procedures in this chapter.

► **To identify a logical drive with sufficient free space**

Important Complete all procedures in this lesson logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. How much RAM does your computer have?

   You must have disk space equal to the amount of RAM plus 5 MB, on a single logical drive.

2. Calculate how much free disk space you must have (RAM + 5).
3. Identify a logical drive on your computer that has at least this amount of free space. Which drive will be your <perf_drive> ?

► To download the utilities

1. Create a directory named \PERF on the drive you identified as your <perf_drive>.
2. Copy the files from the Lesson Disk PERF directory to the \PERF directory you just created.

► To turn on disk counters

1. Start a Command Prompt.
2. Type **diskperf -y**, and then press ENTER.

   This step is necessary to enable monitoring of disk counters.
3. Shut down and restart your computer.

► To create the testing file

You use the Performance Monitor logging feature to make a big log file that is used later in this chapter. The size of the log testing file should be 5 MB less than the amount of physical RAM in the computer. For example, 16–5=11 MB.

1. Calculate the size that your log file should be (RAM - 5).
2. From the Administrative Tools group, start Performance Monitor.
3. From the View menu, choose Log.
4. From the Edit Menu, choose Add to Log.
5. Select all available objects.

Note To select all objects in the Objects box quickly, select the first object and then scroll to the bottom of the box. Hold down the SHIFT key and then select the last object. All items in the list are now selected.

---

6. Choose Add, and then choose Done.
7. From the Options menu, choose Log.
8. The Log Options dialog box appears.
9. In the File Name box, type <perf_drive>**:\perf\bigfile.log**
10. Under Update Time, select Periodic Update.
11. In the Interval box, type **0.1**, and then choose Start Log.

    Notice the size of the log file in the File Size field. When the log file reaches the calculated size of your log file, continue to the next step.
12. From the Options menu, choose Log.
13. Choose Stop Log.
14. Exit Performance Monitor.

Establishing a Benchmark

You are now ready to benchmark performance.

1. First, you set application responsiveness.
2. Then you run an application named TEST1.EXE, which sets the benchmark.
3. After this is done, you introduce a mystery bottleneck into the system. Then you run the application again to see how performance has changed.

► **To set application responsiveness**

1. From the Control Panel, start the System application.
2. Choose Tasking.
3. Select Foreground And Background Applications Equally Responsive, and then choose OK.
4. Close the System application and minimize the Control Panel.

► **To run a benchmark test before introducing the bottleneck**

1. Start the <perf_drive>:\PERF\TEST1.EXE application.
2. Move the TEST1 window to the top left corner of your screen.
3. From the TEST1 window, choose the Do Test menu option.

   A test, benchmarking performance, is run. The application displays the time needed to execute the test.
4. Record the number of seconds it took to complete the test:

► **To introduce a mystery bottleneck and rerun the benchmark**

1. Start the <perf_drive>:\PERF\TESTING1.BAT file.

   Five background applications are started, introducing a bottleneck into your system.
2. Select TEST1, and then choose Do Test.
3. Record the number of seconds it took to complete the test.

You now have before and after timings. These timings should indicate that performance is now suffering.

Determining Which Device Is the Bottleneck

Next, you create a Performance Monitor report to determine what is causing the bottleneck in system performance.

► **To create a report**

1. Start Performance Monitor.

   Size Performance Monitor as large as possible, leaving enough space for TEST1 and for the background application icons at the bottom of the workspace.
2. From the View menu, choose Report.
3. From the Options menu, choose Report.

   The Report Options dialog box appears.
4. Select Periodic Update.
5. In the Interval box, select or type **1.0** and then choose OK.
6. From the Edit menu, choose Add to Report.
7. Add each of the following objects, counters, and instances.

Object	Counter	Instance
Processor	% Processor Time	0
Physical disk	% Disk time	All instances (0, 1,...)
Memory	Pages/sec	Not applicable

8. When you have finished adding these to the report, choose Done.

   The Performance Monitor report appears.

► **To identify the bottleneck**

1. Use the counter values in the report to determine which device object is the bottleneck. Which counter indicates that the associated device is the most heavily used?

2. You have determined that the CPU is the bottleneck because it is running at approximately 100 percent.

Determining Which Process Is Causing the Processor to Bottleneck

You are now ready to determine which *application* is causing the bottleneck. To do this, you create a Performance Monitor chart.

► To create the chart

1. From the View menu, choose Chart.
2. From the Options menu, choose Chart.

   The Chart Options dialog box appears.
3. In the Gallery box, select Histogram, and then choose OK.
4. From the Edit menu, choose Add to Chart.
5. Add each of the following.

Object	Counter	Instance
Process	% Processor Time	APP1-1, APP1-2, APP1-3, APP1-4, APP1-5, and TEST1

6. Choose Done.

   The Performance Monitor chart appears.

► To identify the application

1. View the chart bars, referring to the color-keyed legend at the bottom of the window.
2. Press CTRL+H.

   The colored graphic bar turns white when the associated counter at the bottom of the display is selected.
3. Use the UP ARROW and DOWN ARROW keys to move through the counters associated with each application.
4. Determine which application is stressing the processor. Which application is using most of the CPU time?

In your troubleshooting efforts you were able to determine both the physical source (processor) and the process (APP1-5) that caused the bottleneck.

If you were actually doing these steps in the course of your job, you could continue your troubleshooting by determining the priority base of your applications.

Cleaning Up the System

Finally, you clean up the system for the next lesson.

► **To clean up the system**

1. Close Performance Monitor.
2. Use the Task List to close APP1-1 through APP1-5 and Test1.
3. Use the Control Panel System to reset Tasking to Best Foreground Application Response Time.

Disk Activity

If the processor is being used efficiently, but you are waiting for your computer to respond, it is quite probable that the *disk* is the bottleneck. By monitoring disk activity, you can identify the most popular share points and move them to the equipment that performs best.

Statistics about disk use can help you balance the workload of network servers. Two hardware aspects of disk drives can affect performance greatly; average access time and the speed of the disk controller.

Standard hard disks now operate in single digits for disk access time. The faster the disk drive, the less time it takes to retrieve data from the drive.

If disk I/O is performing properly, there will be less strain on virtual memory and programs will run faster.

Disk Counters

Performance Monitor provides two objects that contain disk counters:

- Counters important for troubleshooting and capacity planning are found in the object Physical Disk.
- Counters referring to partitions that identify the source of activity on a physical disk are in the object Logical Disk.

The Average Queue Time

The average queue time is the amount of time each disk I/O request actually takes to complete on a specific drive. Obviously, the lower the average queue time, the shorter the wait time for the operation to complete, resulting in quicker responses to the user. Two Performance Monitor counters, which are tied directly to disk performance, are used to calculate average queue time:

- Disk Queue Length is the number of disk access requests waiting in the queue to be processed. It is a temporary value that grows and shrinks rapidly. It is a good idea to watch this figure over a period of time to determine a baseline and average.

- Avg. Disk sec/Transfer is the average amount of time for a disk transfer (either reads or writes) to complete. Reads and writes are monitored separately as well.

Use the following formula to find the average disk queue time:

Avg. Queue Time = Disk Queue Length x Avg. Disk sec/Transfer

Multiplying Disk Queue Length by Avg. Disk sec/Transfer gives an estimate of the amount of time each disk I/O will actually take on that logical drive.

Read/Write Requests

When tracking performance for physical drives, the following counters can be useful in determining how effectively a drive is satisfying read/write requests from users.

- The Avg. Disk sec/Transfer counter indicates how much time a disk takes to fulfill requests. A high value (values greater than 0.3 seconds) can mean that the disk controller is continually retrying the disk because of failures.
- A Disk Bytes/sec count lower than 20K can indicate that an application is accessing a disk inefficiently. The lower the number, the less effective the disk accesses are in retrieving the requested data.

Enabling Disk Monitoring Counters

To activate disk performance statistics on your computer, you use Performance Monitor. At the beginning of the procedures for determining system bottlenecks, you enabled the tracking of logical and physical disk counters. These same counters are also used to track disk activity.

To activate disk activity monitoring, type:

diskperf -y [*computer_name*]

To deactivate disk activity monitoring, type:

diskperf -n [*computer_name*]

The optional *computer name* parameter allows disk activity monitoring to be turned on by a central system administrator.

Caution Using Performance Monitor to monitor disk activity can degrade performance by up to 1.5 percent. The performance degradation on a 386/25, for example, is 1.5 percent. Because of this, disk activity monitoring is not turned on by default.

On a 486 computer, however, the performance loss is so small that it cannot be measured. So, disk monitoring *should* be turned on for Windows NT Server computers that use a 486 or higher processor.

Improving Disk Performance

There are several ways to help improve the disk performance in your system, including:

- Distributing the logical disks over multiple different physical disks by means of disk striping.
- Moving data files around to help balance access to the disks.
- Installing another controller card.
- Installing faster hard drives.

Keep in mind that not all performance problems can be blamed on the disk. As you learn in the next lesson, excessive paging can indicate inadequate memory. This is an example of why it is important to monitor the *whole* system; what appears to be a bottleneck in one area might in fact hide the real bottleneck in another area.

Average disk queue time is an important performance measurement, but it is a relative one; it should be compared with other hard disk drives in your system, by using the following two steps:

- Compute the figures for all disks in your system.
- Compare the results, and distribute as much processing as possible to your best-performing disks.

If you have multiple hard disks on your computer, and each has different access times and average disk queue times, you might be able to improve performance by implementing disk striping. Striping distributes data among the physical drives in the computer, helping to average out the disk access and average disk queue times among *all* of the drives.

If the majority of the disk access is localized to a *single* file or area of the disk, this solution might not increase performance, because striping writes data in a 64K block on the first disk before writing 64K on the next.

Lesson Summary

Being able to determine a system bottleneck is important for supporting and maintaining a computer system, especially a network server. To determine system bottlenecks, Performance Monitor allows you to track how resources, such as processors and disks, are being used.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to monitor the performance of your physical disks, but whenever you look at the data collected for the counters, they always show 0. Why?

2. You have to determine whether a specific application is using too much processor time. How can you do this?

For more information on	See
Using Performance Monitor	Chapter 9, "Monitoring Network Activity and Performance," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
	Chapter 11, "Monitoring Performance," in the *Microsoft Windows NT Server Network Operations Quick Reference.*
	Chapter 19, "Performance Monitor," in the *Microsoft Windows NT Server System Guide.*
For online information about	**From the Help menu, choose Contents and then**
Creating a Chart	Performance Monitor Help, Chart Current Activity.
	Performance Monitor Help, Work with Existing Log Files.
Creating a Report	Performance Monitor Help, Create Reports on Current Activity.
	Performance Monitor Help, Work with Existing Log Files.

Lesson 3: Monitoring Server Memory and Network Activity

When monitoring a computer system, it is important to track processor activity and disk activity, but system memory and network activity are equally important. This is especially true with a network server. In this lesson, you learn how to use Performance Monitor to track memory use and network activity.

After this lesson you will be able to:

- Determine the correct amount of physical memory required.
- Compare file cache reads to reads from physical disk.
- Identify network components that generate statistics.
- Identify network-tracking counters.
- Determine network optimization hardware.
- Create a log.
- Identify a network bottleneck.

Estimated Completion Time: 60 minutes

Server Memory

Memory is the most complex performance variable. It is a combination of the physical memory in the computer and the virtual memory available on disk. When requests for physical memory exceed the memory that exists in the system, data is moved from RAM to the virtual memory paging file. This process is called paging.

Some amount of paging is acceptable in a system. However, *excessive* paging can slow the system down, consuming large amounts of disk space and processor time. The end result of excessive paging is applications that run slower on the computer, as well as a computer that is less responsive to the user.

To achieve the best use of server memory, you must determine three things:

- The correct amount of physical memory.
- The correct size for the paging file(s).
- The correct distribution of the paging file(s).

Physical Memory Needs

To figure out the correct amount of physical memory, you first establish the amount of paging the system is doing. To determine whether paging is excessive:

- Multiply **Memory:Pages/sec * Logical Disk:Avg. Disk sec/Transfer** (where the Logical Disk instance is the disk that contains PAGEFILE.SYS).

The product of these counters is the percentage of the disk access time used by paging. If this number is greater than 10 percent (0.1) on a sustained basis, the system needs more memory.

If excessive paging has been detected, the next step is to determine the additional memory needs. This is done by monitoring the Process:Working Set for each active process in the system. To determine additional memory needs, do the following steps:

- Terminate processes (starting with the process having the largest working set and proceeding towards the smallest). Document the size of the working set of each process as terminated.
- Check the counters (listed above) until the paging drops below the excessive mark.
- Add the working sets of the processes terminated. This will give a rough estimate of the additional memory required. In other words, the procedure to follow is to check the working set size, terminate a process, check the working set size, terminate a process, check the working set size, and so on.

Virtual Memory Needs

The paging file can expand if necessary, but this does add time to the paging process. For this reason, it is best if the paging file is not required to grow during normal operations. The paging file, PAGEFILE.SYS, can also shrink dynamically, but it will do so only if there are free pages at the end of the file.

Increasing the paging file requires additional disk access to allocate the needed sectors, and to update any allocation tables and free sector tables used by the various file systems.

Memory:Commit Limit is the Performance Monitor counter that indicates the number of bytes that can be committed to the paging file without *extending* the paging file; the lower the counter, the greater the possibility that the paging file will grow. To allow time to react to an impending problem, it is best not to let the commit limit dip below 10 to 20 percent of the existing size of the paging file. This provides a buffer to cushion any instantaneous needs for the paging file.

To increase system performance, distribute paging files to the physical disks with the lowest total disk I/O time. A maximum of 16 volumes can have paging files. It is also a good idea to move the paging file from the Windows NT boot partition.

RAM vs. Disk

When accessing data on a computer, access most often occurs from disk. Some data access, however, occurs from RAM. Disk access time is measured in milliseconds. RAM access time is measured in nanoseconds. Retrieving data from RAM is therefore many times faster than retrieving the same data from the disk. To increase performance, it is usually better to invest in RAM.

Using Performance Monitor to Analyze the File Cache

The Windows NT File Cache is used when you read application data requests from the hard drive to physical RAM. The file cache reads more data than what it is asked for (called *read-aheads*). In this section, you use the Performance Monitor to:

- Observe the Windows NT file cache operation.
- Observe physical disk versus file cache access patterns for file cache read operations.

  (Additional optimizations are Read ahead and Write behind.)
- Compare performance differences between the two.

In these procedures you learn how to do cache and disk reads, and then clean up the system.

Preparing your Computer

The first step is to prepare your computer.

► **To prepare your computer**

Important Complete the following procedures logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. Start the <perf_drive>:\PERF\IOTEST.EXE application.
2. Move the I/O Test application window to the top left corner of your display.
3. Using either the Control Panel Services application or Server Manager, stop the Netlogon and Computer Browser services on your computer.

   These services periodically perform some disk I/O. If they are not stopped, they could alter the results of this procedure.
4. Start or switch to Performance Monitor.

Read Data in Cache

Now you are ready to explore reads from cache as opposed to reads from disk.

► To configure Performance Monitor and I/O test

1. From the Performance Monitor File menu, choose Open.
2. In the File Name box, type <perf_drive>**:\perf\rcache.pmc** and then choose OK.

   The RCACHE.PMC settings file sets Gallery to Graph, Periodic Update to .5 seconds, and adds the following counters to the chart:

Object	Counter	Instance	Description
Memory	Cache bytes	Not applicable	Memory allocated as file cache
Physical disk	Disk read bytes/sec	0	Bytes actually read from the hard disk
Cache	Fast reads/sec	Not applicable	Reads satisfied from cache

3. If <perf_drive> is not on Physical Disk 0, add the counter Physical Disk:Disk Read Bytes/Sec for the instance where your <perf_drive> is located.

   It has been a while since the data was written, so the Virtual Memory Manager has had plenty of time to grab some of the associated memory pages and use them for other purposes. Before you perform the read test, run the Write test to make certain the pages are available in cache.
4. From the I/O Test window, choose Settings.
5. Complete the Settings dialog box using the following information:

In this box...	You input...
File Name	<perf_drive>:\PERF\IOTEST.TMP
File Size	3000000
I/O Size	64000
Action	Only Write selected
Pause	0

6. Choose OK.
7. Choose Do Test.

   A 3 MB data file is written to the hard disk. This file will be used to test read performance in the next procedure.
8. Choose Settings.
9. Under Action, select Read, and then clear Write. (Only Read should be selected.)
10. Choose OK.

► To view and test performance

Important Before you continue, carefully read through this procedure.

1. Return to Performance Monitor.
2. From the Edit menu, choose Clear Display.
3. Immediately in the I/O Test window, choose Do Test.

   You will observe some graph activity on the Performance Monitor display. As soon as the Performance Monitor graph activity has stabilized, continue on to the next step.
4. From the Options menu, choose Chart.
5. Under Update Time, select Manual Update, and then choose OK.

   This sequence halts the time bar so that you can view the graph activity without overwriting it.

► To analyze performance

1. Record the number of seconds required to complete the test.

   In this test, I/O Test reads 3 MB of data from <perf_drive>. Thanks to the previous Write test, the data was still in memory (although not allocated as cache). The associated memory pages were mapped back to cache, and the data was read directly from cache.

2. Analyze the Performance Monitor graph activity to answer the following questions.
3. Where was the data read from, cache (green line) or the disk where <perf_drive> is?

4. Does it appear as though any data was read from disk?

Read Data from Disk

For comparison, you will now see how responsive the system is to reads that involve the disk subsystem as opposed to cache.

► To configure Performance Monitor

1. From the Performance Monitor Options menu, choose Chart.
2. Under Update Time select Periodic Update, and then choose OK.

► To force a read from disk

Next, you run a Read test with the data actually coming from disk. However, as you learned in the previous example, the data is still in memory. If you want to force a read from disk, you must first cause the associated memory pages to be modified.

Continue to view the Performance Monitor chart while you perform the next two steps.

1. Using a Command Prompt or File Manager, copy <perf_drive>:\PERF\BIGFILE.LOG to a different directory on your computer.
2. Delete the copy of BIGFILE.LOG you just created.
3. Return to Performance Monitor.
4. How is the Memory:Cache Bytes affected (purple line on the Performance Monitor display) while the file is being copied?

Notice the activity on the disk read line for the <perf_drive> disk that was not present in the previous procedure. Also, the cache read (green) line is constant at zero, as opposed to the previous procedure in which everything was from cache.

Next, you compare the results of the previous procedure with the results of the I/O test after large file I/O.

► To view and test performance

Important Before you continue, carefully read through this procedure.

1. From the Performance Monitor Edit menu, choose Clear Display.
2. Immediately in the I/O Test window, choose Do Test.
3. As soon as the Performance Monitor graph activity has stabilized, continue to the next step.
4. From the Performance Monitor Options menu, choose Chart.
5. Under Update Time select Manual Update, and then choose OK.

► To analyze performance

1. Record the number of seconds required to complete the test.

   In this test, I/O Test read 3 MB of data from your <perf_drive>. Because you performed significant I/O activity before rerunning the Read test, the data was no longer in memory. For that reason, it had to be read from disk.

   Analyze the Performance Monitor graph activity to answer the following questions.

2. Where was most of the data read from, cache (green line) or the disk where <perf_drive> is?

3. Does it appear as though any data was read from cache (green line)?

4. Can you guess why some of the data was read from cache? (Hint: Notice that some data began to come from cache shortly after data began to be read from disk.)

   When you copied BIGFILE.LOG, all of the I/O Test data was purged from memory. However, some of the data did come from cache due to a cache optimization known as read-ahead.

   When the application issues a Read request, the Cache Manager often reads more data from the disk (into cache) than the application requested. When the application issues the *next* Read request (especially if it is asking for data located immediately following the *previously* read data), some of the requested data will most likely be in cache. There is no need to go to disk. The sequence is as follows:

Application	Cache manager
Read *x* bytes	Read *x* + bytes from disk into cache; return *x* bytes to application
Read next *x* bytes	Return *x* bytes to application (from cache)
Read next *x* bytes	Return *x* bytes to application (from cache)
<repeat>	

5. How much less time did it take I/O Test to read the 3 MB from cache (previous test) than from disk (even with read-ahead)? Record the number of seconds.

6. What percent was read from cache faster than from disk (even with read ahead)? ((from disk result – from cache result) / from cache result) * 100 = % faster. Record your answer.

Cleaning Up the System

The final step is to clean up the system.

► **To clean up the system**

1. Close I/O Test.
2. Start the Netlogon and Computer Browser services on your computer.
3. From the File menu of Performance Monitor, choose New Chart to clear the chart display.
4. If you are not going to repeat these procedures, you can delete <perf_drive>:\PERF\BIGFILE.LOG.

Network Activity

Network monitoring consists of two main activities; watching server performance and measuring overall network traffic. On a Windows NT network, you can use Performance Monitor to track server performance and to troubleshoot if a problem occurs. Monitoring overall network traffic requires specialized tools such as dedicated network monitoring software or a packet sniffer, such as Microsoft Network Monitor.

Searching for network bottlenecks is a cumulative process; everything you have done so far still applies. A server that has a disk bottleneck because memory is too tight is still a computer with a disk bottleneck. The fact that it is a *server* only makes it more annoying, because more people are affected. Your efforts this far are not wasted; you simply need to carry them farther and look at the counters that monitor network traffic.

Network Components That Generate Statistics

There are three components that generate statistics:

- Workstation service (RDR.SYS)
- Server service (SRV.SYS)
- Protocols (NetBEUI, NWLink, TCP/IP)

The workstation service (RDR.SYS, also referred to as the redirector) *transmits* requests, while the server service (SRV.SYS) *receives* and *interprets* incoming messages. Each Windows NT computer also uses at least one type of protocol to handle packet formatting and routing. Windows NT supports several protocols, including NetBEUI, NWLink, and TCP/IP.

The workstation, server, NetBEUI, NWLink, and TCP/IP each generate a set of statistics that appear as Performance Monitor counters. Abnormal network counter values often indicate problems with a computer's memory, processor, or disk(s). For this reason, the best approach to monitoring a server is to watch *network* counters in conjunction with other counters such as % Processor Time, % Disk Time, and Pages/sec.

For example, if a server shows a sharp increase in Pages/sec accompanied by a drop in Total Bytes/sec, it might indicate that the computer is running short of physical memory for network operations.

Tracking Network Counters

Tracking the counter values listed in the following table, over an extended period, is a good way to understand network operations.

Network Counters

Object type	Counter	Description
Server	Pool Nonpaged Failures	Monitors the number of times allocations from the nonpaged pool have failed; indicates that the computer's physical memory is too small.
Server	Pool Nonpaged Peak	Maximum number of bytes of the nonpaged pool that the server used at a given time. This maximum indicates the amount of memory (RAM) required in your server.
Server	Bytes Total/sec	The number of bytes sent and received from the computer each second. This value gives an overall indication of how busy a server is.

(continued)

Object type	Counter	Description
NetBEUI	Frame Bytes 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 Received/sec	
	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 very low.
NetBEUI Resource	Times Exhausted	This is a cumulative counter that indicates the number of times since system startup that all resources (buffers) were in use. A sharp and consistent increase in values for instances 0 through 4 (links, addresses, address files, connections, and requests) usually indicates network problems.

Note The last two objects, NetBEUI and NetBEUI Resource, are listed as examples of counters for a specific protocol. If you are using and analyzing a different protocol, such as TCP/IP, use the appropriate counters for that protocol.

Monitoring Network Performance

The following procedures give you the opportunity to use the Testnet application to generate traffic on the network. You use Performance Monitor to:

- Create a log containing counters from two different computers.
- Record data on network traffic produced by an application.
- Identify bottlenecks in your network.
- Use bookmarks to isolate data gathered over time.

Preparing the Server

First, you need to prepare the computer that will be used as the server.

- Copy performance utilities and files to your hard disk.
- Share the utilities for network access.

► **To download the utilities**

The primary domain controller of DOMAIN-B will function as a server for purposes of monitoring network performance.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

---

1. Create a directory named \UTILS on a drive that has at least 10MB free.
2. Copy the files from the Lesson Disk UTILS directory to your UTILS directory.
3. Share your UTILS directory as UTILS, with Everyone having Full Control permissions.

Creating a Log File

In this procedure, you create a log file to gather data regarding network activity. The log file includes objects from your computer (the primary domain controller of DOMAIN-A), which is acting as a *workstation* for this problem. The log file also includes an object from the primary domain controller of DOMAIN-B, which is acting as a *server* for this problem.

► **To create a log file**

Important Complete all remaining procedures in this lesson logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. From the Performance Monitor View menu, choose Log.

   The Log window appears.
2. From the Edit menu, choose Add To Log.

   The Add to Log dialog box appears. You now add objects from your own computer.
3. Select the following objects, and then choose Add.
   - Logical Disk
   - Memory
   - Redirectory

   You now add the server object from the primary domain controller of DOMAIN-B to your log.
4. Choose the ellipse button to the right of Computer.

   The Select Computer dialog box appears.
5. In the Computer box, type **\\PDC-B** and then choose OK.

   The Add to Log dialog box reappears, indicating the computer \\PDC-B.

6. Select the Server object, and then choose Add.
7. Choose Done.
8. From the Options menu, choose Log.

   The Log Options menu appears.
9. In the File Name box type <perf_drive>**:\perf\network.log**
10. Under Update Time, select Periodic Update.
11. In the Interval box, type **2.0** and then choose Start Log.

    The Log window appears, showing data being collected.

Generating and Recording Network Test Data

Next, you use the primary domain controller of DOMAIN-A to generate network test data. Then you use Performance Monitor to create a log of the activity.

► **To run the Testnet program**

Important Do not run Testnet from your local drive.

1. Use File Manager to connect to \\PDC-B\UTILS.
2. From the network drive, run TESTNET.EXE.

   The Testnet screen appears. Testnet is running and ready to stress-test your network.

► **To generate the network test data**

You will run a series of tests, each using the same procedures. You should read through the entire procedure before starting to familiarize yourself with the process.

1. Switch to Performance Monitor.
2. From the Performance Monitor Options menu, choose Bookmark.

   The Add Bookmark dialog box appears.
3. In the Comment box, type **Test 1**, and then choose Add.

   You have now added a bookmark named "Test 1" to mark the beginning of the first test.

   Bookmarks are place markers generated by Performance Monitor and are used to indicate where one test ends and the next begins. Bookmarks appear when you are using Time Windows for viewing portions of data from a log.

4. Switch to Testnet.

   Refer to the first line of the Testnet Testing Data table that follows. As necessary, change the Record Size and Repetitions settings to match those in the chart by performing the following steps:

5. Use the arrow keys to highlight the parameter setting you want to change, and then press ENTER.
6. Type the setting you want, and then press ENTER.
7. Press F1 to begin stressing the network.

   When the test is complete, the "Continue Testing?" prompt appears at the bottom of the Testnet window.

8. Record the K/Sec and Total Seconds figures from the screen in the Testnet Testing Data chart below.
9. Press Y to continue testing in Testnet.

   The Testnet screen appears, allowing you to change Testnet parameters.

10. Repeat all steps in this procedure, using the Record Size, Repetitions, and Bookmark names in the Testnet Testing Data table.

Record Size	Repetitions	Total Bytes	KB/Sec.	Total Seconds	Bookmark
1024	1000	1 MB			Test 1
2048	1000	2 MB			Test 2
4096	1000	4 MB			Test 3
4096	2000	8 MB			Test 4
1024	1000	1 MB			Test 5
1024	4000	4 MB			Test 6

When you complete the table, you have all the data you need for the following procedures.

▶ To end Testnet and stop logging data

1. After recording the last data, when the "Continue Testing?" prompt appears at the bottom of the Testnet window, press N.
2. Switch to Performance Monitor.
3. From the Options menu, choose Log.
4. Choose Stop Log.

Isolating the Bottleneck

Now that you have gathered all the data, you create a chart from the logged data and determine where the bottlenecks are.

► **To isolate the bottleneck**

1. From the View menu, choose Chart.
2. From the Options menu, choose Data From.
3. The Data From dialog box appears.
4. Select Log File, and then choose the ellipse button.
5. In the Open Input Log File dialog box, select <perf_drive>:\PERF\NETWORK.LOG, and then choose OK.
6. Choose OK.
7. From the Edit menu, choose Add to Chart.
8. Add to your chart the objects and counters that appear in the Counter Thresholds table that follows. When adding the Server counters, make sure that you select the computer that was functioning as the server for purposes of monitoring network performance, PDC-B, in the Computer box.

Object	Counter	Average value	Max	Threshold
Server	Bytes Total/sec			—
	Pool Paged Failures			>=1
	Work Item Shortages			>=1
Redirector	Current Commands			>1 per net adapter
	Bytes Total/sec			—
	Network Errors/sec			>=1
	Writes Denied/sec			>=1
	Reads Denied/sec			>=1

Note If a value falls above the indicated threshold range, it could indicate a performance problem.

9. Using the Average and Max values from your chart, answer the following questions.
10. Which computer (your computer or PDC-B) has counters that are exceeding the threshold?

11. Which counter indicates that you have a bottleneck?

12. Which device is your bottleneck?

13. From the Edit menu, choose Time Window.
14. Use your bookmarks to isolate and view data generated by the different tests.
15. What is the value of the bookmarks?

Cleaning Up the System

Finally, you clean up the system.

► **To clean up the system**

1. Close Performance Monitor.
2. Disconnect from \\PDC-B\UTILS.

Optimizing Network Hardware

Choosing the correct equipment to begin with is better than trying to adjust or tune incorrect equipment. Although little can be done to optimize the network card directly, choosing the correct adapter for your Windows NT Server computer can potentially *double* its performance. There are some pointers, however, for selecting network cards.

- Choose an adapter that uses the full width of the I/O bus in your system. If you have an EISA machine, use an EISA device instead of a 16-bit or 8-bit card. The following is a general performance guideline for different network adapter cards.

Network Adapter Cards	Performance
8-bit	400K
16-bit	700K
32-bit	1.14MB

- When you choose a network adapter, this also involves the network adapter *driver*. So choose an adapter that is NDIS 3.*x*–certified. These can be found on the Windows NT Hardware Compatibility list.

Lesson Summary

Being able to determine a system bottleneck is important in supporting and maintaining a computer system, especially a network server. Performance Monitor allows you to track resource utilization, such as memory and network activity, to assist in determining system bottlenecks.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. The programmer is not allowed to decide whether data is read from cache or disk. Under what conditions will the data be read from cache?

2. On a computer that runs a fixed set of processes, Performance Monitor helps you determine that 70 percent of cacheable reads and writes are being satisfied by physical disk access. What can be done to increase the cache hit rate?

For more information on	See
Using Performance Monitor	Chapter 9, "Monitoring Network Activity and Performance," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
	Chapter 11, "Monitoring Performance," in the *Microsoft Windows NT Server Network Operations Quick Reference.*
	Chapter 19, "Performance Monitor," in the *Microsoft Windows NT Server System Guide.*

For online information about	From the Help menu, choose Contents and then
Creating a Chart	Performance Monitor Help, Chart Current Activity.
	Performance Monitor Help, Work with Existing Log Files.
Creating a Log	Performance Monitor Help, Log Current Activity.
	Performance Monitor Help, Work with Existing Log Files.
Adding Bookmarks	Performance Monitor Help, Log Current Activity, Adding Bookmarks.
Changing the Time Window	Performance Monitor Help, Work with Existing Log Files, Changing the Time Window.

Lesson 4: Optimizing Windows NT Server

After you have identified system areas that should increase performance, you should optimize as many of these areas as possible. Optimizing existing resources avoids having to spend money on hardware resources. However, there is only so much that can be optimized in software. Any remaining performance improvements will have to be achieved through hardware upgrades.

After this lesson you will be able to:

- Recognize factors that indicate workstation bottlenecks.
- Identify server monitoring counters.
- Identify two Performance Monitor entries that signify a server is at maximum memory.
- Compare the two network data transfer modes.
- List five ways to solve system performance problems using your existing resources.

Estimated Completion Time: 15 minutes

Optimizing Windows NT as a Workstation

Although Windows NT workstation is fairly self-optimizing, you should still be able to recognize factors that indicate workstation bottlenecks. Performance Monitor has workstation indicators in the Redirector object. The counters to watch include Current Commands and Network Errors/sec.

Current Commands

The Current Commands counter shows the number of commands that the redirector has queued. If this number is greater than one per network adapter, the redirector might be a bottleneck in the system. This can occur for any of the following reasons:

- The remote server that the redirector is communicating with is slower than the local redirector.
- The network might be experiencing capacity problems.
- The redirector is so busy that the adapter cannot keep up with it.

If network capacity problems are identified, it might be necessary to subnet the network in an attempt to partition network traffic.

MaxCmds

When accessing data from a network server, the local redirector allocates buffers to store the transmitted data.

The MaxCmds Registry parameter controls the number of SMB Buffers that the Redirector maintains at any given time.

This parameter defaults to 5 and can be set between 0 and 255. Increasing this value will increase the number of buffers that the Redirector will maintain. This saves on the overhead of allocating additional buffers.

Note For more information, see the *Windows NT Resource Kit* for Windows NT 3.5.

Network Errors/sec

Network Errors/sec is a Performance Monitor value that counts the number of serious network errors detected by the redirector. If it shows a number that exceeds your baseline, this indicates that further research is needed. Start by looking at the Event Log on the machine that identified the error.

Optimizing Windows NT Server

Windows NT Server is optimized in almost the same way as Windows NT Workstation, although there are more settings that can be configured. One setting that can be configured is the amount of memory that the server service allocates to itself.

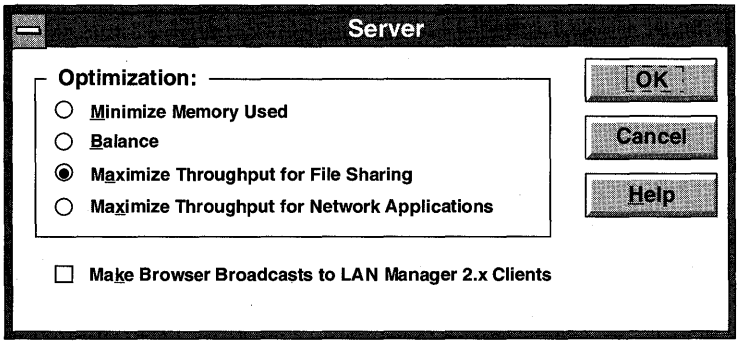


Figure 113: Server service configuration

The Server service can be configured with the Network application from the Control Panel. The four settings in the Server dialog box are:

Optimization option	Description
Minimize Memory Used	Selects parameters for the server to minimize its use and to accept a low number of connections initially(up to ten).
Balance	Initially allocates memory for up to 64 connections.
Maximize Throughput for File Sharing	Initially allocates memory for an unlimited number of connections (71,000 connections).
Maximize Throughput for Network Applications	Allocates memory for an unlimited number of connections, but does not set aside as much memory for cache.

Optimizing a Windows NT Server computer is similar to optimizing a Windows NT Workstation computer, with two minor exceptions:

- There is less need to optimize the user interface components, such as the keyboard, mouse, and video. Under most circumstances, the computer will not be subject to heavy interactive access by end users.
- It is very likely that the default server components will be more important than the redirector. If memory becomes a constraint, you might want to reduce memory for the redirector and provide more memory for the server.

Note For more information, see Appendix C, "The Server Service Configuration Parameter Values."

Monitoring the Server

Specified counters are available for monitoring server performance.

Work Items

The Server object can be closely monitored through the Performance Monitor, and it can be optimized by changing values in the Registry, including:

- InitWorkItems
- MaxWorkItems

A work item is a buffer used by the server to queue and track requests from client computers. If the server is extremely busy or has just started, a request from a client computer could be rejected because there are no work items available.

To track the number of client requests that are rejected due to a shortage of work items on the server, follow the Performance Monitor value Work Item Shortage in the Server object.

Performance Monitor Entries

Two Performance Monitor entries inform you when the server has reached the maximum memory that it is allowed to use or that is available in the system.

- Pool Nonpaged Failures counts the number of times the server attempted to allocate nonpaged memory and was denied due to lack of resources. This is a clear indication that there is not enough physical memory in the machine to run the server in its current configuration.
- Pool Paged Failures counts the number of times the server attempted to allocate paged memory and was denied due to lack of resources. In this case, either physical memory or a paging file could be at capacity.

Remote Server Bottlenecks

Reads Denied/sec and Writes Denied/sec are two Performance Monitor values that indicate whether the server is having problems with memory allocation.

- Check the servers to, or from which, the workstation would be doing large file transfers. If it is impossible to increase memory used by RAW I/O at the server level, you can deny workstation use of RAW I/O.
- Instruct the workstation not to use RAW I/O by setting the Registry entries UseRawReads and/or UseRawWrites to False.

Network Data Transfers

When one computer accesses data on another computer, the data is in either large or small blocks. The transfer mode you use depends on the size of the data block. There are two modes for transferring data:

- RAW mode data transfer
- CORE mode data transfer

By knowing the type of transfer mode to use, you can optimize performance.

RAW Mode Data Transfer

RAW mode data transfer (RAW I/O) saves client computers and servers transmission overhead during large data transfers. It limits the Server Message Blocks (SMB) protocol header of frames transmitted on the network.

RAW Mode

When RAW mode is used, the redirector creates and sends only *one* SMB request message per application I/O request. The server receives data directly into, and sends data directly from, either the server computer's file cache (if applicable and available) or special 64K buffers set aside specifically for RAW data transfer. In this way, when using RAW mode, the redirector can prepare and send a single SMB request message that represents up to 64K of data. There is a definite performance advantage to using RAW mode.

RAW Work Items

The server needs special work items to support RAW I/O. If the server is extremely busy doing file transfers, it might exhaust its supply of RAW work items. When this happens, either the Reads Denied/sec or the Writes Denied/sec in the Performance Monitor indicates the rejections.

There is a Registry value (MaxWorkItems) that tells the server the number of buffers to allocate. The default is determined according to the Server service configuration as described above.

Conditions for Using RAW Mode Data Transfer

The redirector uses RAW mode data transfer when the following conditions apply:

- Application I/O request size is larger than:
  - 2 times the server's request buffer size for read requests

    –or–
  - 1.5 times the server's request buffer size for write requests
- RAW mode is not explicitly *disabled* on the client computer or server.
- The data transfer is not over a very slow link.
- Multiple client computer threads are not simultaneously issuing I/O requests to the same server.
- The server has enough available memory to allocate the requisite (up to 64K) raw buffer.

In all other cases, the redirector uses CORE mode data transfer.

CORE Mode Data Transfer

CORE mode data transfer is used for transferring smaller blocks of data. This mode requires more overhead because data transfer is limited to the size of a server's request buffer.

CORE Mode

When CORE mode is used, the number of SMB request messages that the redirector must create and send per application I/O request depends on the size of the server's request buffer. With CORE mode, the server must receive the data into, and send data from, one of its request buffers.

As an example, when an application issues a read request for 8K bytes of data, the request takes longer to complete if the redirector has to satisfy it by creating and sending two 4K SMBs rather than one 8K SMB.

Default Server Request Buffer Size

Each SMB message that must be created and sent carries with it a small amount of overhead. By default, the server request buffer size is 4356 bytes. Because of this, the SMB data size plus overhead cannot exceed 4356 bytes.

The overhead for a *read* SMB is 63 bytes. The overhead for a *write* SMB is 64 bytes. The rest of the buffer can be data. So when the server's request buffer size is set to default, and conditions require that the redirector use CORE:

Max size **read** request that will be satisfied with 1 SMB = 4356 - 63 = **4293 bytes**
Max size **write** request that will be satisfied with 1 SMB = 4356 - 64 = **4292 bytes**

Solving System Problems

The normal response to common Windows NT Server performance problems is to add more resources. This can be an expensive solution. Besides, if not carefully planned, it might not even *fix* the problem.

The following are some alternatives:

- Create multiple paging files. Create a paging file for each physical disk, as long as the disks use a controller that can access multiple disks simultaneously, or the disks are on different controllers.
- Run memory-intensive applications when the server is not busy, or run them on the computers that perform best.
- Balance the load on the servers. Distribute applications among servers until each computer displays reasonably equivalent values for the following counters:
  - Physical Disk:% Disk Time
  - Memory:Pages/sec
  - Processor:% Processor Time
  - Server:Bytes Total/sec

- Unbind infrequently used network cards or attach them to a subnet that will be more frequently used.
- Configure the network so that servers are on the same network subnet as the people who access them.

Lesson Summary

Optimizing a Windows NT computer can be accomplished by configuring the Server service for the appropriate type of user connections (small number or large number, file server-based or client-server based), and by using Performance Monitor to track the appropriate Redirector and Server counters for network activity.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Explain two factors in choosing a network adapter card.

2. You are running an application that uses very large data files. The requests from the client computers to the server are normally for large sections of the data file. What type of data transfer (RAW or CORE) should be used?

For more information on	See
Tuning Windows NT	Chapter 10, "Tuning for Network Performance," in the *Microsoft Windows NT Server Concepts and Planning Guide.*
For online information about	**From the Help menu, choose Contents and then**
Configuring the Server Service	Control Panel Network, Server Configuration, Help.

CHAPTER 11

Integrating Novell NetWare with Windows NT Server

Before You Begin

This chapter requires that you have completed Chapters 1–5. It assumes that DOMAIN-B trusts DOMAIN-A, which you configured in Chapter 5.

In addition to the primary domain controllers in your two domains, this chapter requires a properly configured NetWare server (version 2.*x*, 3.*x*, or 4.*x* running bindery emulation). For proper functioning in this chapter, the NetWare server should be configured as follows:

1. Create a group named NTGATEWAY.
2. Give the NTGATEWAY group trustee rights to the directory SYS:Public.
3. Create a user account named ADMINISTRATOR, with no password.
4. Add the ADMINISTRATOR account to the NTGATEWAY group.
5. Create a text file named NWGATE.TXT in SYS:Public.

Your NetWare server must be online before starting the first procedure in this chapter.

Lesson 1: Interoperability with Novell NetWare

Novell NetWare is a very common network operating system. Windows NT 3.5 Server includes various protocols and functions that allow you to connect to a Novell NetWare network.

This lesson introduces you to the NWLink IPX/SPX compatible protocol and discusses the features and capabilities of NWLink and its configuration parameters. The lesson also looks at workstation and server bindings specific to the NWLink and NWNBLink protocols.

After this lesson you will be able to:

- List the two features that make interoperability with Novell NetWare possible.
- Describe NWLink and its purpose.
- Configure frame types and bindings.
- Explain direct hosting.
- Explain workstation and server bindings.

Estimated Completion Time: 30 minutes

Connecting to a NetWare Network

If part of your computer resources are on a Novell NetWare network, your Windows NT network will have to communicate and share resources with the NetWare network. With Windows NT Server, NWLink protocol, and Gateway Service for NetWare (GSNW), Microsoft network clients can now communicate and share resources with a NetWare network. This is possible even though the Microsoft network clients have no NetWare client software installed.

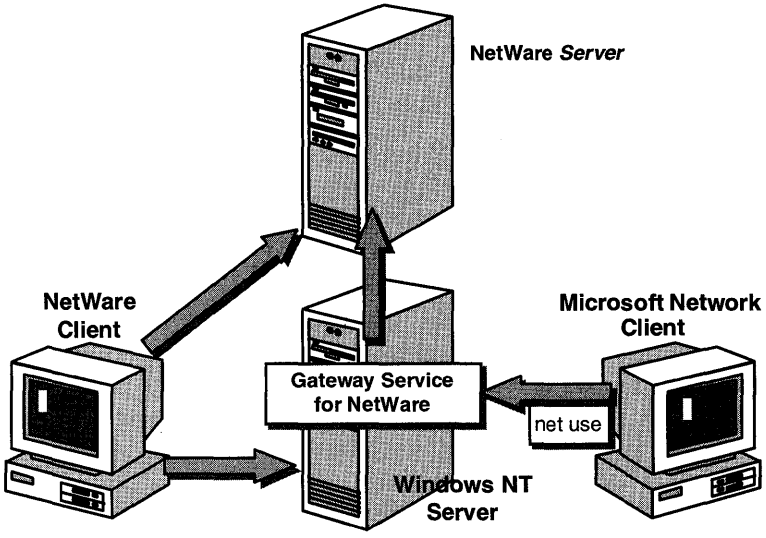


Figure 114: Connecting the Microsoft network to the NetWare network

In the previous figure, a NetWare client can access data stored on a NetWare server by directly accessing the NetWare server and the Windows NT Server computer that is running NWLink through client-server applications. The Microsoft network client can access the NetWare server through the Windows NT server running the Gateway Service for NetWare.

NWLink

NWLink is an implementation of the Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocol used in NetWare networks. The NWLink Transport Protocol is a native 32-bit Windows NT implementation of IPX/SPX. It supports application servers in a NetWare environment. NWLink also supports multiple communications mechanisms.

A Windows NT Server computer configured with NWLink can be used as an application server for NetWare clients. Microsoft NetWare Link protocol (NWLink) is a Network Device Interface Specification (NDIS)–compliant version of the IPX/SPX protocol, which is used on Novell NetWare networks. NWLink allows computers running Windows NT to communicate with other Windows NT computers or NetWare servers. Two networking Application Programming Interfaces (APIs) are supported to allow this communication:

- Windows Sockets—This interface supports existing NetWare applications written to comply with the NetWare IPX/SPX Sockets interface.
- NetBIOS—This interface supports sending and receiving Novell NetBIOS packets between a NetWare workstation running Novell NetBIOS and a Windows NT computer running NWLink NetBIOS.

NWLink also provides NetWare clients access to Windows NT Server applications such as SQL Server and SNA Server.

Windows NT Server computers running NWLink can support client applications for MS-DOS, OS/2, Windows, or Windows NT computers through a variety of communications mechanisms, such as Windows Sockets, Remote Procedure Calls (RPC), or Novell NetBIOS, over the IPX/SPX transport.

NWLink Features

The NWLink protocol has many features to enhance communication on a Windows NT network.

- SPX II—NWLink supports Windows Sockets on the new Novell SPX II protocol. SPX II has been enhanced to support windowing and has the ability to set a maximum frame size.
- Multiple Bindings—NWLink can be bound to multiple network adapters with multiple frame types.
- Frame Type Auto Detect—NWLink automatically detects which frame type is being used on the network during startup and uses that frame type. If there are multiple frame types detected, NWLink defaults to the 802.2 frame type.

Note Frame type Auto Detect might be an issue, because NWLink in Windows NT Advanced Server 3.1 defaulted to the 802.3 frame type. The CONFIG parameter (on the NetWare server) allows users to view information about IPX bindings and frame types. The CONFIG parameter is not a feature of NWLink.

- Direct hosting over IPX—The Windows NT Server service (not the redirector) supports direct hosting technology. This allows Windows for Workgroups 3.11 clients to communicate up to 20 percent faster than they could using NetBIOS over IPX with Windows NT 3.5 computers.

Frame Type and Binding

Two terms are important to understand when working with a NetWare environment; frame type and binding.

- Frame type—The way in which the network adapter formats the data to be put on the network. NetWare IPX clients and servers can be configured for different frame types, but for the computers to communicate, they must be configured for the same frame type. For example, if a NetWare client's IPX protocol is bound to the 802.2 frame type, the NetWare server's IPX has to be bound to an 802.2 frame type. Also, each supported topology (Ethernet, Token Ring, FDDILink™, and ArcNet®) requires a different format.

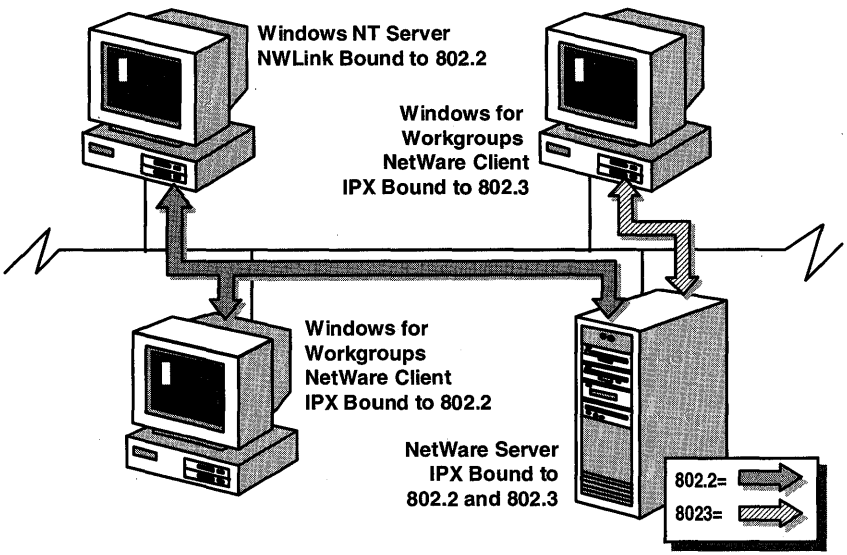


Figure 115: Frame types

- Binding—The process of associating a protocol driver with the network adapter with which it will work, and establishing a communication channel between the two.

Auto Frame Type Detection

The Auto Frame Type Detection allows Windows NT to determine which IPX frame type is being used on the network and to set the NWLink frame type automatically. NWLink checks frames being passed to the network card to which the protocol is bound. If it detects frames of the type 802.2 or no frames at all, it sets the frame type to 802.2. Otherwise, it sets the frame type to whatever is being passed on the network.

Note Novell changed from 802.3 to 802.2 frame format for Ethernet networks with NetWare version 3.12.

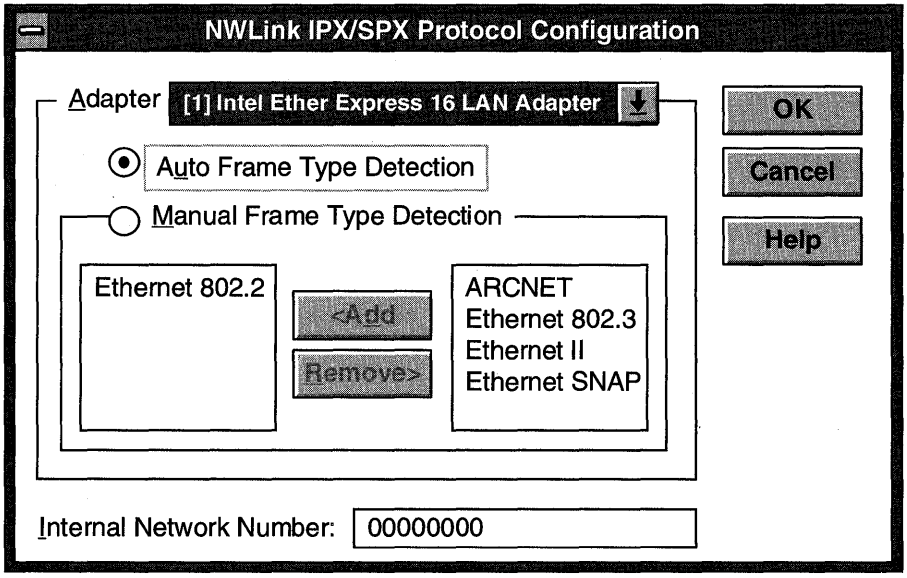


Figure 116: Frame Type Detection

Although frame types are automatically detected during installation of Windows NT 3.5, it is still considered a good practice to double-check that the correct frame type was detected.

Note The Auto Frame Type Detection selection selects only a single frame type to use on the network adapter.

Manual Frame Type Detection

The NWLink protocol in Windows NT Server 3.5 can use multiple frame types on a single network adapter. This can be done on a Windows NT Server computer by configuring NWLink in the Control Panel Network application and manually selecting the frame types to be used on the network adapter.

Note To use multiple frame types, each frame type wanted must be manually selected.

If a connection is successfully established using NWLink but is very slow, the frame type should be checked.

Network Topologies Support of Frame Types

NWLink supports the Ethernet, Token Ring, FDDILink, and ArcNet topologies, and each topology supports certain frame types.

Topology	Supported Frame Types
Ethernet	Ethernet II, Ethernet 802.3, Ethernet 802.2, Ethernet SNAP (defaults to 802.2)
Token Ring	802.2, SNAP (clients that used to configure the Token-Ring frame type should use 802.2)
FDDILink	802.2, SNAP
ArcNet	ArcNet

The Windows NT Server version of NWLink supports binding NWLink to multiple network adapter cards. While this allows a Windows NT computer to connect to multiple networks, it should be noted that Windows NT Server is not currently capable of acting as an IPX router.

If NWLink is bound to multiple network adapter cards, or if NWLink is bound to a single network card with multiple frame types, you might have to set an 8-digit hexadecimal Internal Network Number for the server. The Internal Network Number must be set if Windows NT Server is being used as an application server running applications that use Service Advertising Protocol (SAP), such as SQL Server or SNA Server.

The SAP Agent is used to advertise services using the NetWare SAP Protocol. If Windows NT Server did not include the SAP Agent, a NetWare server would be required for these services to announce themselves using the SAP Protocol.

Direct Hosting

NWLink supports direct hosting which provides an enhanced IPX layer between Windows NT Server computers and Windows for Workgroups clients. Direct hosting is the ability of network applications to communicate directly to the IPX/SPX protocol without a NetBIOS layer.

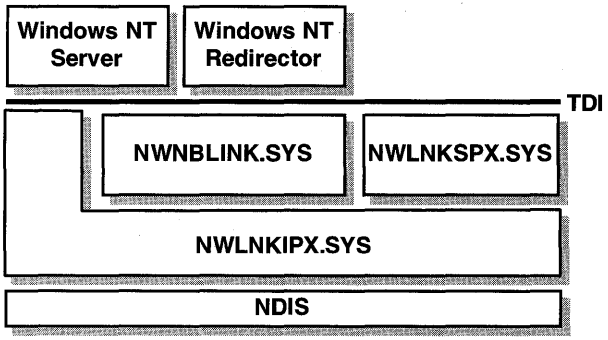


Figure 117: Direct hosting architecture

Normally, a Microsoft network client requires a NetBIOS layer to run on most protocols, such as NetBEUI, TCP/IP, NWLink, and DECnet™. NWLink allows applications that support direct hosting to bypass the NetBIOS layer and send requests directly to the IPX protocol.

Note Direct hosting is not supported in the redirector portion of Windows NT. Therefore, a Windows NT server cannot provide direct hosting to another Windows NT computer. There must be a NetBIOS layer involved in the communication.

Windows for Workgroups Direct Hosting Support

The Windows for Workgroups 3.11 server application supports direct hosting. Also, the Windows for Workgroups protected mode redirector (VREDIR.386) has been enhanced to provide support for direct host sessions to Windows NT. The updated file is supplied on the Windows NT Server CD-ROM.

Network Direct Hosting

To establish a direct host session over IPX, the redirector on one computer and the server service on the other computer must both support the following:

- Direct hosting.
- Communicating directly with the IPX protocol.
- Registering a socket address.

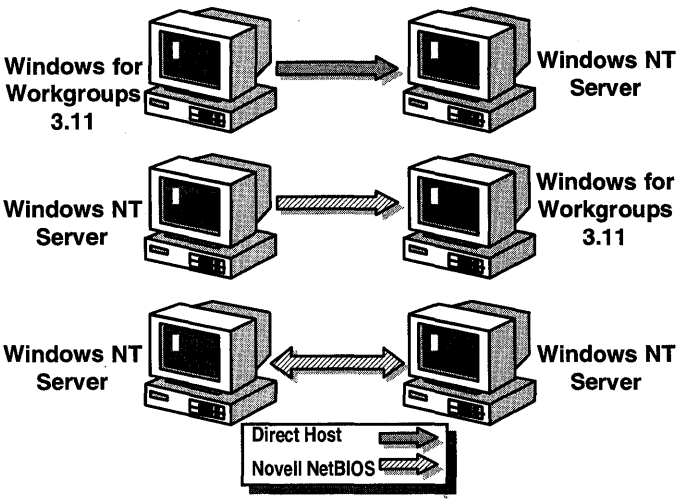


Figure 118: Direct host and Novell NetBIOS configurations

The following examples describe some of the circumstances for using direct hosting. These examples assume that NWLink is installed on all machines and that the Directhost= switch is not set to NO in the Windows for Workgroups machine's SYSTEM.INI.

- Windows for Workgroups 3.11 machines will direct host if they initiate the session with a Windows NT Server or Windows NT Workstation computer.
- Windows NT Server and Windows NT Workstation computers cannot direct host with each other.
- Windows NT Server and Windows NT Workstation computers cannot direct host if they initiate the session with a Windows for Workgroups 3.11 computer.

Note Windows for Workgroups 3.11 machines will, by default, direct host with each other.

To connect to a remote computer's server service, the redirector broadcasts a name query packet with the server's computer name.

All servers that are capable of direct hosting have already registered a special socket number and will receive this packet. The server that recognizes the computer name contained in the name query packet responds to the redirector with its unique network address. Using this address, the redirector can establish a session with the server.

Server Bindings

A server binding associates the server service with the protocol and adapter that it will use.

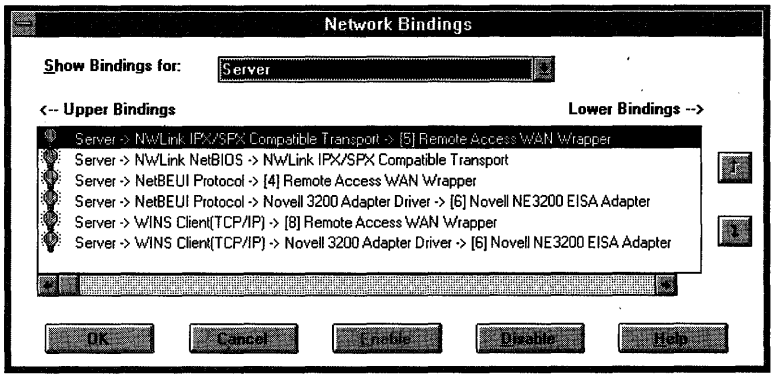


Figure 119: Server bindings

Notice that the server is bound to both NWLink NetBIOS and NWLink IPX/SPX Compatible Transport, showing support for direct hosting on the server component.

Workstation Bindings

A workstation binding associates the workstation service with the protocol and adapter that it will use.

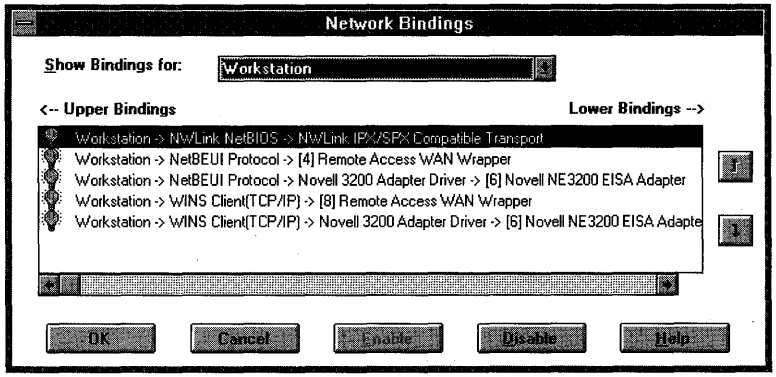


Figure 120: Workstation bindings

Notice that because the workstation is bound only to NWLink NetBIOS, it will not support direct hosting.

Note Because the Windows NT redirector does not support direct hosting, a Windows NT computer cannot initiate a direct host session.

Installing NWLink

NWLink is installed by default during the Windows NT Server installation. Because NWLink operates through the NDIS 3.0 stack, the NWLink protocol can be run on any network adapter card that uses an NDIS-compatible driver.

When NWLink is installed in Windows NT, the frame type is set to Auto Frame Type Detection by default. This allows Windows NT to determine which IPX frame type is being used on the network and set the NWLink frame type accordingly.

Note It is important to make sure that NWLink on a Windows NT computer is configured with the same frame type as on the NetWare server. Setting the incorrect frame type prevents the workstation from seeing NetWare servers.

▸ To confirm the NWLink installation

In this procedure, you confirm the correct installation of NWLink by viewing the configuration of NWLink under Network settings in Control Panel. You need your Configuration Table for the NWLink parameters.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A. Also, your NetWare server must be running.

1. From Control Panel, start Network.

   The Network Settings dialog box appears.

2. Verify that the Installed Network Software box lists NWLink IPX/SPX Compatible Transport.

   If NWLink IPX/SPX Compatible Transport does not appear on the list, you have not yet installed this protocol. Skip the remainder of this procedure and go to the next procedure, entitled To install the NWLink protocol.

   If NWLink IPX/SPX Compatible Transport does appear on the list, you have already installed this protocol. Continue with this procedure to confirm your installation.

3. In the Installed Network Software box, select NWLink IPX/SPX Compatible Transport, and then choose Configure.

   The NWLink IPX/SPX Protocol Configuration dialog box appears.

4. Confirm your frame type and internal network number, and then choose OK.

   The Network Settings dialog box appears.

5. Choose OK.
6. If you made changes to your configuration, the Network Settings Change dialog box appears. Choose Don't Restart Now.
7. Skip the following procedure. You already have NWLink installed.

► To install the NWLink protocol

In this procedure, you install the NWLink protocol. You need your Configuration Table for the location of distribution files and NWLink parameters.

Important Complete this procedure only if NWLink IPX/SPX is not installed on your primary domain controller of DOMAIN-A.

Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. If you have not already done so, from Control Panel, start Network.

   The Network Settings dialog box appears.

2. Choose Add Software.

   The Add Network Software dialog box appears.

3. Select NWLink IPX/SPX Compatible Transport, and then choose Continue.

   The Windows NT Setup dialog box appears, asking for the location of the Windows NT distribution files.

4. Type the path to the location of Windows NT Server distribution files, and then choose Continue.

   The NWLink software is installed on the computer, and the Network Settings dialog box appears.

5. Choose OK.

   The NWLink IPX/SPX Protocol Configuration dialog box appears.

6. Configure your frame type and internal network number, and then choose OK.

   The Network Settings Change message box appears and prompts you to shut down and restart your computer. This is required to implement the configuration.

7. Choose Restart Now.

   Your computer is shut down and restarted. The Welcome box appears.

8. Log on as Administrator.

   You now have the NWLink protocol installed and configured on your computer.

Monitoring NWLink Performance

Performance Monitor is the Microsoft tool for measuring computer activity to optimize performance. You can use Performance Monitor, located in the Administrative Tools group, to monitor the following objects:

- NWLink IPX
- NWLink SPX
- NWLink NetBIOS

Each of these objects can return information on network performance (bytes sent or received per second), stability (disconnects, listen failures), and many other important indicators. This can help you locate problem points before they reach the critical stage.

The object you monitor depends on the application that is using NWLink. For example, if you are interested in data relevant to Windows NT Server, use the NWLink NetBIOS object. For GSNW, monitor the NWLink IPX object.

Note For more information on Performance Monitor, see Chapter 10, "Optimizing Windows NT Server for Performance."

Lesson Summary

NWLink is an IPX/SPX compatible protocol that allows Microsoft Network clients to access Novell NetWare services. It supports multiple frame types and direct hosting.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What is one advantage of direct hosting?

2. What does setting the frame type to Auto Detected do?

3. You have just installed Windows NT Server with NWLink, and now your NetWare users want to use the Windows NT Server for file and print sharing. Will they be able to do so?

4. You have just installed SNA Server for Windows NT on your Windows NT Server. What else must be done at the server and on your NetWare clients for them to be able to access Windows NT and SNA Server?

For more information on	See
Configuring NWLink IPX/SPX Compatible Protocol	Chapter 4, "Gateway Service for NetWare," in the *Microsoft Windows NT Server Installation Guide.*

For online information about	From the Help menu, choose Contents and then
Configuring NWLink IPX/SPX Compatible Protocol	Additional Networking Services for Windows NT, Gateway Service for NetWare.

Lesson 2: The Gateway Service for NetWare (GSNW)

One feature of Windows NT Server is its ability to access files and printers on a Novell NetWare server. This is accomplished by using the Gateway Service for NetWare (GSNW). This lesson introduces you to the Gateway Service for NetWare and shows you how to install the Gateway Service for NetWare.

After this lesson you will be able to:

- Explain the purpose of the Gateway Service for NetWare (GSNW).
- Implement the Gateway Services for NetWare (GSNW).

Estimated Completion Time: 45 minutes

Microsoft Gateway Service for NetWare (GSNW) is a 32-bit Windows NT service. In combination with NWLink, GSNW allows a Windows NT Server to access files or printers on a Novell NetWare server. The service also allows a Windows NT Server to act as a nondedicated gateway to NetWare file systems for any Server Message Block (SMB) client, including Windows for Workgroups, Windows NT, or any Microsoft networking client.

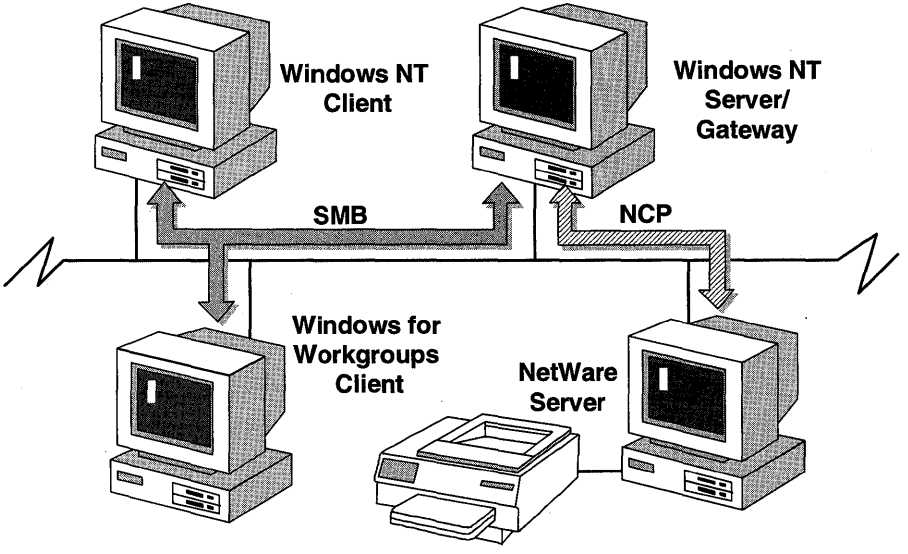


Figure 121: Using GSNW to access a NetWare server

GSNW can be used to access file and print services on NetWare 2.*x* and 3.*x* file servers, and on NetWare 4.*x* file servers running bindery emulation. GSNW does not support the NetWare 4.*x* NetWare Directory Services (NDS).

When to Use GSNW

The Gateway Service for NetWare is not intended as a full service router for NetWare services. Performance suffers if the Gateway is used for unlimited server access, because all users are receiving the services through one NetWare connection.

Microsoft designed this service for users who only occasionally need access to NetWare servers and prefer not to have the memory overhead associated with running multiple redirectors on their own computers.

Note The Gateway Service for NetWare also includes all of the functionality of the Client Service for NetWare.

With GSNW, the Windows NT Server computer connects to the NetWare file server's directory and then shares it, just as if the directory were on the Windows NT computer. Microsoft network clients can then access the directory on the NetWare server by connecting to the share created on the Windows NT Server computer.

Preparing the Gateway Service

For a Windows NT Server to act as a gateway to resources on a NetWare server, the NetWare server must have a group named NTGATEWAY. In addition, the user name to be used as the gateway account must be included in the group NTGATEWAY. Use the NetWare Syscon utility to create the group and user account.

Any resources that you want to be shared through the gateway must be made available to the members of the group NTGATEWAY through the Syscon group options.

Installing GSNW

You install GSNW using the Control Panel Network application. The NWLink transport must be installed before installing GSNW, because GSNW requires the IPX protocol enabled by NWLink. It requires no files from Novell.

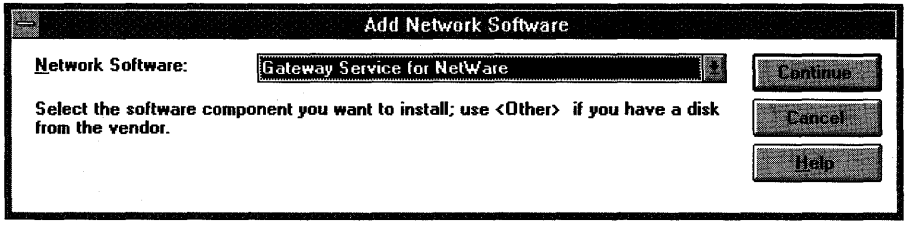


Figure 122: Adding GSNW

The frame type that NWLink uses must match the frame type being used on any NetWare servers that must be accessed.

When installation is complete, the computer must be restarted for the changes to take effect. The first time the computer restarts, the system requests the preferred server for the current user.

The GSNW installation creates a new icon, labeled GSNW, and adds it to Control Panel. GSNW is used to select the defaults for the preferred NetWare server and the NetWare print queue.

► To install the Gateway Service for NetWare

In this procedure, you install the Gateway Service for NetWare. You need your Configuration Table for the location of Windows NT Server distribution files.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. From Control Panel, start Network.

   The Network Setting dialog box appears.

2. Choose Add Software.

   The Add Network Software dialog box appears.

3. Select Gateway Service for NetWare, and then choose Continue.

   The Windows NT Setup dialog box appears, asking for the location of the Windows NT distribution files.

4. Type the path to the location of Windows NT Server distribution files, and then choose Continue.

   Windows NT Server installs the Gateway Service for NetWare.

5. Choose OK to close the Network Settings dialog box.

   The Network Setting Change message prompts you to shut down and restart your computer.

6. Choose Restart Now.

Lesson Summary

If you occasionally need access to NetWare servers and do not want the memory overhead associated with running multiple redirectors on your computer, you can install and use the Gateway Service for NetWare.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What is the purpose of the Gateway Service for NetWare?

2. You are the administrator of both the Windows NT servers and the NetWare servers. You are sitting at a Microsoft network client and you need to make changes to users on the NetWare server. You start the NetWare SYSCON utility on the client and it fails. Why?

For more information on	See
Gateway Service for NetWare	*The Microsoft Windows NT Server Services for NetWare* documentation.

For online information about	From the Help menu, choose Contents and then
Gateway Service for NetWare	Additional Networking Services for Windows NT, Gateway Service for NetWare.

Lesson 3: Configuring the Gateway Service for NetWare

To use GSNW, you must configure the service. This lesson introduces you to configuring the Gateway Service for NetWare, making a connection to a NetWare server, and setting Gateway file security.

After this lesson you will be able to:

- Configure the Gateway Service for NetWare.
- Make a connection to a NetWare server.
- Set Gateway file security.

Estimated Completion Time: 30 minutes

After the user account and group are set up and the installation is complete, the gateway can be configured. This is done through the Gateway Service for NetWare application in Control Panel.

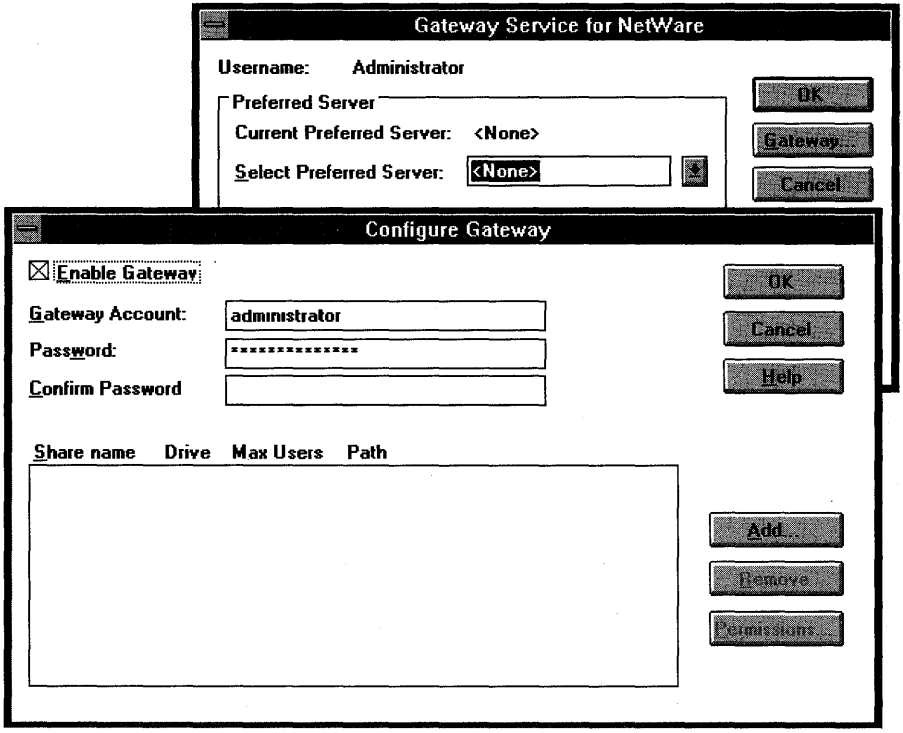


Figure 123: Configure Gateway dialog box

To configure GSNW, you must do the following:

- Select a server
- Set up the gateway
- Make a connection by establishing a sharable resource

Selecting a Server

To configure the Gateway Service for NetWare, you must select the preferred server for the Gateway to connect to. This is done from the Select Preferred Server drop-down list box in the Gateway Service for NetWare dialog box.

After the preferred server has been selected, Windows NT attempts to connect to the NetWare server. If the attempt to make the connection is unsuccessful, you are given the opportunity to select another preferred server.

Setting Up the Gateway

To set up the gateway, check the Enable Gateway box and add the Gateway's user account and password that were created earlier. Remember that this user account must be a member of the NTGATEWAY group on the NetWare server.

Establishing a Connection

The Gateway must establish a connection to the NetWare server to provide transparent access to NetWare resources.

To set up directories to be available on the Windows NT Server system from the NetWare server, you choose the Gateway button in the Gateway Service for NetWare dialog box.

You use Print Manager to connect to a NetWare print queue and select the Share This Printer on the Network check box to enable the computer to act as a NetWare print queue gateway.

Note Network paths must be provided using UNC syntax, for example \\NW311\SYS\USERS.

► To configure the NetWare gateway

In this procedure, you create shares on the Windows NT Server computer for resources located on the NetWare server. Microsoft network clients will access the NetWare directories through the Gateway Service for NetWare. You need your Configuration Table for the name of your NetWare server, your gateway account, and the password of your gateway account.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

---

1. Log on as Administrator.

   The Select Preferred Server for NetWare dialog box appears.
2. Select your NetWare server, and then choose OK.
3. If prompted, type the password for the gateway account, and then choose OK.
4. From Control Panel, start GSNW.

   The Gateway Service for NetWare dialog box appears.
5. Choose Gateway.

   The Configure Gateway dialog box appears.
6. Select Enable Gateway.
7. In the Gateway Account box, type **administrator**
8. In the Password and Confirm Password boxes, type the password for your gateway account, and then choose Add.

   The New Share dialog box appears.
9. In the Share Name box, type **nwdata**
10. In the Network Path box, type *NetWare_server***sys\public** and then choose OK.
11. Create another share with the name NWPUBLIC, also pointing to the path *NetWare_server*\SYS\PUBLIC.

    You will set different permissions on these shares later.

Gateway File Security

The only security that is available for the Gateway resources is on the shared directories.

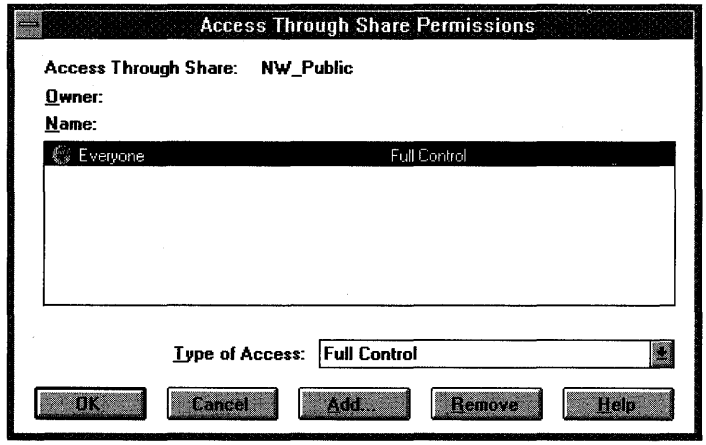


Figure 124: Access Through Share Permissions dialog box

The following permissions are available:

- No Access—No access is allowed to files or subdirectories.
- Read—User is granted access to Read files and subdirectories.
- Change—User is granted access to Read, Change, and Delete both files and subdirectories.
- Full Control—Allows user to Read, Write, Delete, and Change files.

The default permissions for gateway-shared directories are Full Control for Everyone.

Any file level security has to be assigned to the NetWare user account specified when the Gateway was enabled. For example, if the SUPERVISOR account was used when the Gateway was enabled, all file-level rights are assigned to users who are accessing files through the Gateway. The only way to change these rights would be to change the share-level permissions for the Windows NT Gateway share. You have to decide whether file-level security is needed. If it is, you can assign the correct rights to the user account that is used by the Gateway.

Adding User and Group Permissions

The Add Users and Groups dialog box is used to add users and groups to the permissions list for a Gateway Service for NetWare resource. This dialog box determines which users can access the shared resource. Physical access is granted to the NTGATEWAY account at the NetWare server.

► **To set the permissions on the NetWare server**

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-A.

1. From the Configure Gateway dialog box, select the share name NWDATA, and then choose Permissions.

   The Access Through Share Permissions dialog box appears.
2. Verify that the group Everyone has Full Control permissions.
3. Choose OK to close the Access Through Share Permissions dialog box.
4. Select the share name NWPUBLIC, and then choose Permissions.
5. Select the group Everyone.
6. In the Type of Access box, select Read, and then choose OK.
7. Choose OK to close the Configure Gateway dialog box.
8. Choose OK to close Gateway Services for NetWare.

Lesson Summary

Configuring GSNW involves selecting a NetWare server, setting up the gateway, and establishing Windows NT Server shares for the NetWare resources. Security for the gateway is limited to permissions on the shared directories.

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Why is selecting a preferred server important?

2. You are configuring security on the Gateway Service for NetWare and you leave the default settings. What permissions will users have at the NetWare server?

For more information on	See
Gateway Service for NetWare	The Microsoft Windows NT Server Services for NetWare documentation.

For online information about	From the Help menu, choose Contents and then
Gateway Service for NetWare	Additional Networking Services for Windows NT, Gateway Service for NetWare.

Lesson 4: Using NetWare Resources with GSNW

After the gateway connection is configured, you can use both File Manager and Print Manager to access directories and print queues on a NetWare server.

After this lesson you will be able to:

- Use File Manager to make a connection to directories on a NetWare server.

Estimated Completion Time: 30 minutes

File Manager

Users can connect to directories on NetWare file servers using File Manager. With File Manager, users can browse and connect to resources on both Windows NT Server computers and NetWare computers. After being connected to a NetWare drive, users can simply drag and drop directories and files.

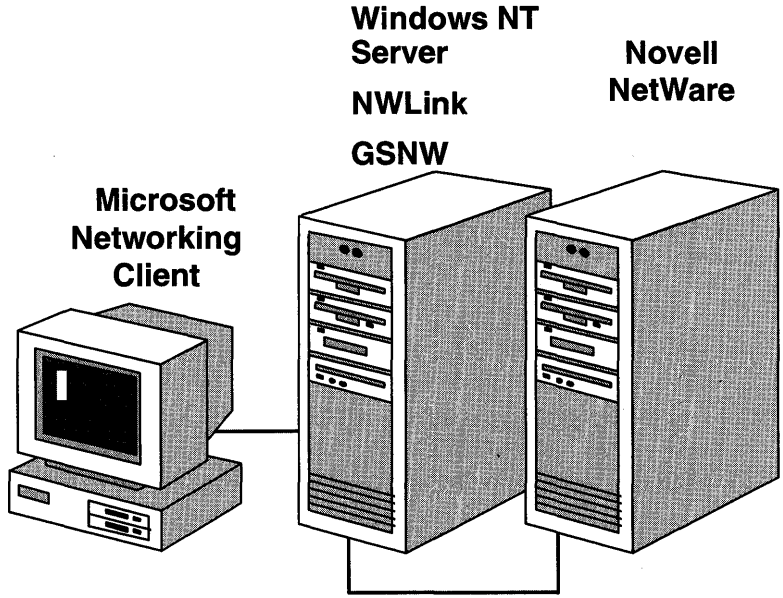


Figure 125: Accessing files on a Novell NetWare server

On NetWare networks, the servers, volumes, and directories are organized in a treelike structure. Both volumes and directories are represented by the shared directory icon.

NetWare server volumes, directories, and print queues can be represented by their universal naming convention (UNC) names:

\\NetWare_Server\volume\directory

NetWare syntax is also supported:

NetWare_Server/volume:directory

► **To access the NetWare server through the gateway**

In this procedure, the primary domain controller of DOMAIN-B connects to the NetWare server through the gateway on the primary domain controller of DOMAIN-A. You need your Configuration Table for the computer name of your primary domain controller of DOMAIN-A, the share names for the NetWare resources, and the name of the text file on the NetWare server.

Important Complete this procedure logged on as Administrator from the primary domain controller of DOMAIN-B.

---

1. Using File Manager, connect drive N to \\PDC-A\NWDATA.
2. Connect drive P to \\PDC-A\NWPUBLIC.
3. Close File Manager.
4. Use Notepad to open the file P:\NWGATE.TXT.
5. Make changes to the file and attempt to save the file. Were you successful? Why or why not?
6. Use Notepad to open the file N:\NWGATE.TXT.
7. Make changes to the file and attempt to save the file. Were you successful? Why or why not?
8. Disconnect drive N.
9. Disconnect drive P.
10. Log off.
11. If an administrator wanted to set permissions on a specific file or directory, how would you do this? Who would be affected by it?

Print Manager

To print to a NetWare print queue, users connect to it using Print Manager. When you connect to a NetWare print queue, you are prompted to install a local printer driver.

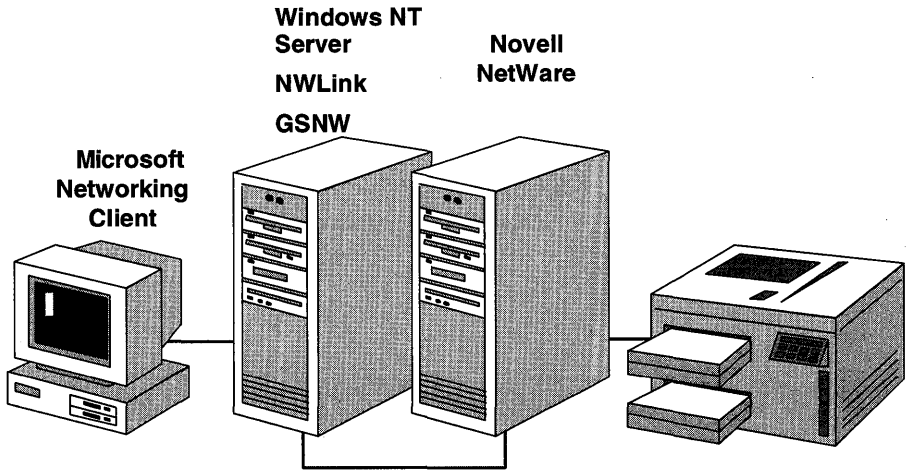


Figure 126: Accessing printers on a Novell NetWare server

If the NetWare system is first in the network search order for print providers, the list of servers on the NetWare system is automatically displayed in the Shared Printers box. After connecting, users can print to the NetWare print queue, just as they would to a Windows NT print queue.

The printing options that are supported for NetWare print queues include settings for:

- Form feeds.
- Print notification.
- Banner pages.

Printing options are set for the user who is logged on to Windows NT. Settings affect all NetWare print queues used from a given Windows NT workstation.

Lesson Summary

To access files and printers on a NetWare server after GSNW has been established, you can use File Manager or Print Manager and access the Novell NetWare services in the same way that you access Windows NT Server services.

Questions and Answers

Getting Started

Page 22

Review Questions

1. What are the differences between the workgroup model and the domain model?

   Using a workgroup model, resources and administration are distributed throughout the network.

   Using a domain model, all the accounts and account policies for the entire network can be managed from a single location.

2. What are the advantages of using a domain model?

   Centralized administration—All the accounts and account policies for the entire network can now be managed from a single point instead of computer-by-computer and user-by-user.

   Resource sharing—Assigning permissions to resources becomes more structured. This is crucial where sensitive information is concerned, or where there are many resource share points on the network.

   Defining a user's environment—Administrators can create user profiles to determine what each Windows NT Workstation user's logon environment will be like. This is helpful with users who are not computer literate.

Chapter 1

Lesson 1, page 15

Review Questions

1. Explain when you would use a domain instead of a workgroup.

   If you want centralized administration of user accounts and security policies, use a domain. If you want each computer to control its own user accounts and security policies, use a workgroup.

2. What are the differences in a PDC, BDC, and server?

   PDC—contains master copy of domain information and validates users. Only one allowed per domain.

   BDC—maintains copy of domain information and validates users. Multiple allowed per domain.

   Server—functions as file, print, and application server; does not validate users.

3. Which type of server is recommended to install first? How is this determined?

   The PDC is the first Windows NT Server computer that is named to be part of the domain. This occurs during installation by designating the server as a PDC.

Chapter 2

Page 45

► **To view the built-in groups that are allowed to log on locally by default**

4. Which built-in groups are assigned the right to log on locally at a Windows NT Server domain controller?

   Account Operators, Administrators, Backup Operators, Print Operators, Server Operators

Lesson 2, page 49

Review Questions

1. List two local groups provided for Windows NT Server that are configured as a server and domain controller.

   Administrators, Users, Guests, Backup Operators, Replicator.

2. List two operator groups provided only for Windows NT Server domain controllers.

   Server Operators, Print Operators, Account Operators.

3. Name an existing group that would provide an account with authority limited to managing printers.

   Print Operators.

Page 52

► **To determine built-in global group membership**

1. From User Manager for Domains, select Domain Admins. Which default users are automatically members of Domain Admins?

   Administrator.

3. Select Domain Guests. Which default users are automatically members of Domain Guests?

   Guest.

5. Select Domain Users. Which default users are automatically members of Domain Users?

   Administrator.

2. To which built-in global group(s) is Admin-A automatically assigned?

   Domain Users.

5. Were you successful? Why or why not?

   No, the logon policy of this computer does not permit Domain Users to log on interactively.

10. Were you successful? Why or why not?

    Yes, the logon policy of this computer does permit Domain Admins to log on interactively.

Lesson 4, page 62

Review Questions

1. You are implementing Windows NT Server in your network, and have decided that you do not want to allow all users to have complete access to the NTFS partitions on the servers. How can you secure the NTFS partitions?

   Set the security permissions on the root of the NTFS partition to remove the special group Everyone (which has default access permission of Full Control). Alternatively, you could change the default permissions to Read for the group Everyone.

2. You are creating a shared directory for user access. You have decided to ensure that all users accessing the resource over the network can view the files but not change them. How can you secure the shared files?

   Set the security permissions on the shared directory to remove the special group Everyone (which has default access permission of Full Control). Then add the special group Network, and assign Read permissions.

Page 65

► **To test user rights and groups**

2. Were you successful? Why or why not?

   No, the logon policy of this computer does not permit Domain Users to log on interactively.

11. Were you successful? Why or why not?

    Yes, you are a member of a group (Everyone) that has been permitted to log on at the domain controller.

Page 67

► **To add a global group to a local group**

6. Which user account(s) receive permissions and rights based on group memberships of LocalA-Red?

   UserA-1 and UserA-2, through membership in GlobalA-X.

7. Which user account(s) receive permissions and rights based on group memberships of LocalA-Green?

   UserA-3, through membership in GlobalA-Y.

Page 67

► **To assign permissions using groups**

14. Were you successful? Why or why not?

    Yes, successful in connecting to, but not in reading, the directory. You could not read the directory because UserA-1 is not a member of LocalA-Green.

17. Were you successful? Why or why not?

    Yes, successful in connecting to and reading the directory, though there might not be any files present.

Chapter 3

Page 77

► **To assign a home directory**

8. What is the path to UserA-1's home directory?

   \\PDC-A\users\UserA-1

Page 79

► **To test the ability of the user account to log on**

2. Were you able to log on? Why or why not?

   If your local time is between 8:00 AM and midnight, you could not log on. Time restrictions prevented logging on between these hours.

   If your local time is between midnight and 8:00 AM, you were able to log on.

Page 80

► **To test the ability of the user account to log on at the PDC**

2. Were you able to log on? Why or why not?

   Yes. The user no longer has logon hours restrictions and is allowed to log on to this computer.

4. What is the default directory?

   H:\USERA-2 (the home directory assigned earlier).

Page 81

► **To test the ability of the user account to log on at PDC**

2. Were you able to log on? Why or why not?

   No. Your account is configured to prevent you from using this workstation.

Page 82

► **To clear the workstation restrictions**

6. Were you able to log on? Why or why not?

   Yes. The logon workstation restriction was removed.

Page 83

► **To test the expiration date**

2. Were you able to log on? Why or why not?

   No. The account has expired.

Page 83

► **To test the expiration date**

2. Were you able to log on? Why or why not?

   Yes, the account expiration has been cleared.

Page 84

► **To test the local account**

2. Were you able to log on? Why or why not?

   No. The error message indicates that no account exists in the domain account database.

Page 85

► **To test the global account**

2. Were you able to log on? Why or why not?

   Yes, the account has been enabled for local domain logons.

Page 90

► **To test a local profile**

4. Were all the configuration changes you made restored?

   Yes.

Page 91

► **To test logging on without a local profile**

2. Were all the configuration changes you made earlier restored?

   No, the profile has been deleted, so the User default profile was used for UserA-1.

Page 95

► **To test the mandatory user profile**

2. Is the desktop scheme what you set for UserA-1 (Bordeaux)?

   No, it is set to Arizona (as designated in the mandatory profile).

3. Is the wallpaper a tiled ZIGZAG?

   No, it is set to tiled Marble.

4. Is drive L: connected to \\PDC-A\Share-A?

   No, drive L: is not connected, though drive N: is connected to \\PDC-A\Netlogon.

5. Can you perform a File Run command from Program Manager?

   No, the Run command from the File menu of Program Manager is disabled.

7. Were you successful?

   No, Program Item and Common Program Group are disabled.

8. Which profile is loaded, local user or server-based mandatory?

   Server-based mandatory.

11. Did the Games group remain minimized?

    No, because the profile was mandatory, changes made by users are not saved to the profile.

Page 102

► **To test the user logon script**

3. Is the desktop environment as configured in the user profile?

   Yes.

5. Is the file DAILY.TXT in UserA-1's home directory?

   Yes.

Chapter 4

Lesson 1, page 120

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to verify that all sessions on your server are being initiated by users with accounts in your domain. How can you make sure that this is the case?

   Use Server Manager. Access the Properties dialog box for the server, and then choose Users. In the last column of the User Sessions dialog box is the Guest column. If any users that are not logged on using domain accounts are accessing resources on the local computer, this column will display Yes.

2. You need to shut down the server for maintenance, and you want to make sure that all users have closed all open files on the server before shutting it down. How can you verify that it is safe to shut down the server?

   Using Server Manager, access the Properties dialog box for the server and then choose In Use. Any open resources will be listed here. If any users have open resources on the local computer, you can then use the Send Message option to send a notice of the impending shutdown.

Page 123

► **To add a computer account to the primary domain controller**

6. What is the Type of the new computer account?

   Windows NT Backup.

Page 126

► **To verify that the domain is out of sync**

2. Were you able to log on? Why or why not?

   No. The BDC tried to validate the logon, but the UserA-4 account information had not yet replicated to the BDC.

Page 127

► **To verify that the domain is synchronized**

2. Were you able to log on? Why or why not?

   Yes. The domain's account database has replicated to all controllers in the domain.

Page 133

► **To test the pulse parameter**

8. What database was synchronized, and with how many updates?

   The SAM database, and 1 update was recorded.

Page 135

► **To verify server information**

2. Does this information match the information on the other domain controller in your domain? Why or why not?

   Yes. Server Manager is looking at the same set of domain members.

Page 135

► **To promote a BDC to a PDC**

3. What warning message appears?

   Promoting might take a few minutes. Promoting will close client connections to the BDC.

4. How does this affect your network if you are remotely running Server Manager over a RAS connection?

   (Choose HELP) You cannot promote if either computer is your RAS server, because all the connections will be lost.

6. What actions are occurring during the promotion? Watch the messages in the status dialog box and record them below.

   Synchronize the BDC. Stop the NetLogon Service on the BDC, then the PDC. Demote the PDC and then promote the new PDC. Start the NetLogon Service on the new BDC, then the PDC.

Page 136

► **To verify server information**

2. Does this information match the information on the other controller in your domain? Why or why not?

   Yes. Server Manager is looking at the same set of domain members.

3. How does this information compare to the information in the first procedure?

   The Roles (Types) are reversed for PDC-A and BDC-A.

Lesson 2, page 137

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You have installed a domain with a single domain controller. After conferring with other network administrators, you realize that this is not the best policy and decide to add two backup domain controllers to the domain. How can this be accomplished now that the domain has already been created?

   Using Server Manager, add accounts for the two new BDCs. Install the BDCs as backup domain controllers for the domain. At the end of the installation process, they will automatically synchronize the domain's account database.

2. You have a domain that has a remote site connected over a slow link. What can you do to make sure that when domain synchronizations occur, the synchronization process does not use the entire bandwidth of the WAN link?

   Use the ReplicationGovernor parameter on the remote BDC to designate a percentage of data transfer. The exact percentage will have to be tested on your link, but a good starting point is 50%.

Page 145

► **To start the Directory Replicator service**

7. If the To List box is left empty, which import servers will receive the exported files?

   Import servers in the same domain as the export server.

Page 152

► **To manage directory replication at the import server**

3. View the status of imported directories. What is the status of the Profiles directory? Why?

   No Sync. The Directory Replicator service knows that the directories are no longer identical.

5. When would you place a lock on a directory on the export server?

   When you do not want that directory to be exported to any import server.

6. When would you place a lock on a directory on the import server?

   When you do not want the directory, on this import server only, to be overwritten when replication occurs.

Lesson 3, page 153

Review Questions

The following questions are intended to reinforce the key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Your company has decided to use logon scripts to support the MS-DOS–based network clients on your network. However, you have more than one domain controller in the domain. How can you make sure that the logon script is available to a user being validated by any domain controller?

   By creating the logon script at the PDC and setting it up as an export server to export to the local domain and/or to all domains. Then set up each BDC in the domain(s) to import the logon script from the PDC.

2. Give an example of how replication can be used.

   Logon scripts, mandatory user profiles, and read-only files.

3. For replication to work, which computers have to be running the Directory Replicator service?

   Export servers and import computers.

4. What is the default export directory path?

   ***winnt_root*\SYSTEM32\REPL\EXPORT**

5. What is necessary to set up replication on an import computer that is part of the export server's domain?

   Grant the replicator user account (created on the export server) membership in the local Replicator group.

   Configure the Directory Replicator service to start automatically and to log on under the directory replicator user account created on the export server.

   Using Server Manager, configure the import server or workstation to receive files from other servers or domains.

Chapter 5

Lesson 1, page 162

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Define a trust relationship.

   A trust relationship is a link between two domains, in which one domain trusts user accounts to be validated in one domain, and allows those users to access resources in the local domain.

2. List two key advantages that trust relationships offer administrators and users.

   User accounts need only be maintained in one domain.

   Resource permissions can be assigned to accounts not in the local domain.

3. Why are all trusts based on a one-way relationship?

   Trust relationships are based upon one domain trusting another domain. A two-way trust relationship is the sum of establishing two one-way trust relationships.

4. Differentiate between a trusted domain and a trusting domain in a trust relationship.

   A trusted domain is the domain with the user and group accounts which the trusting domain uses for access permissions. The trusting domain has the resources which users in the trusted domain need to access.

5. List three planning considerations when preparing to establish trust relationships.

   Trust relationships can be established only between Windows NT Server domains.

   The domain that contains the accounts is the trusted domain.

   The domain that contains the resources is the trusting domain.

   User and group accounts in trusted domains can be given permissions to resources in trusting domains.

   You can log on to a trusted domain from a trusting domain.

   Trusts are one way. If both domains need to trust each other's accounts, then two one-way trusts must be set up.

Page 171

► **To complete the one-way trust relationship**

7. If you do not receive this message, what message did you receive? Take corrective action as indicated in the message. (Write the message below.)

   Could not find domain controller for this domain.

   The password is incorrect.

   The trust relationship could not be verified at this time.

Page 175

► **To identify the domains trusted by DOMAIN-A**

4. Which names appear in the From box of a trusted domain?

   Only DOMAIN-A, the trusted domain.

Page 176

► **To identify the domains trusted by DOMAIN-B**

4. Which names appear in the From box of a trusting domain?

   Both DOMAIN-A (the trusted domain) and DOMAIN-B (the trusting domain).

Page 176

► **To complete the logon process**

2. Were you able to log on? Why or why not?

   No. No domain account for USERA-3 exists in DOMAIN-B.

4. Were you able to log on? Why or why not?

   Yes. The domain account USERA-3 exists in DOMAIN-A.

Page 191

► **To design group membership**

1. Why is Admin-A currently able to administer DOMAIN-A?

   Admin-A is a member of DOMAIN-A's global group Domain Admins. This global group is automatically a member of DOMAIN-A's local Administrators group. Therefore, Admin-A is currently able to administer Domain-A.

2. Write the steps you would use to allow all administrators of DOMAIN-A to administer DOMAIN-B.

   Add the global group DOMAIN-A\DOMAIN ADMINS to the local group DOMAIN-B\ADMINISTRATORS.

Page 192

► **To test the administration capability**

5. Were you successful in viewing the shared directories? Why or why not?

   Yes. Admin-A is a member of DOMAIN-A\DOMAIN ADMINS, which is a member of DOMAIN-A\ADMINISTRATORS.

10. Were you successful in viewing the shared directories? Why or why not?

    Yes. Admin-A is a member of DOMAIN-A\DOMAIN ADMINS, which is a member of DOMAIN-B\ADMINISTRATORS.

Chapter 6

Lesson 1, page 206

Review Questions

The following review questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You are planning to implement disk striping with parity after installing Windows NT Server. With this in mind, why would you possibly not want to place application data on one large partition with the Windows NT system files?

   Neither the system nor boot partitions can be part of a stripe set with parity. Either place the data on a separate partition, or use mirroring instead of striping with parity.

2. You have heard that Windows NT Server supports RAID and wonder which fault-tolerant options you can implement with your server installation.

   For data protection, Windows NT Server supports disk mirroring (RAID level 1) and striping with parity (RAID level 5).

3. Which partitions cannot be included in a stripe set?

   The system and boot partitions.

4. List three differences between striping with parity and mirroring.

   The system and boot partitions can be mirrored.

   Striping requires less disk overhead than mirroring.

   Mirroring uses two disks; striping with parity uses at least three disks and can use up to 32 disks.

Lesson 2, page 213

Review Question

The following review question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- You want a user to create a mirror set on her Windows NT Server computer to protect it from data loss. What must you do so that the user is able to implement the mirror set?

  The user must be added to the local Administrators group of the Windows NT computer. Either Add the user to the Administrators local group or have the user log on as Administrator.

Lesson 3, page 220

Review Questions

The following review questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

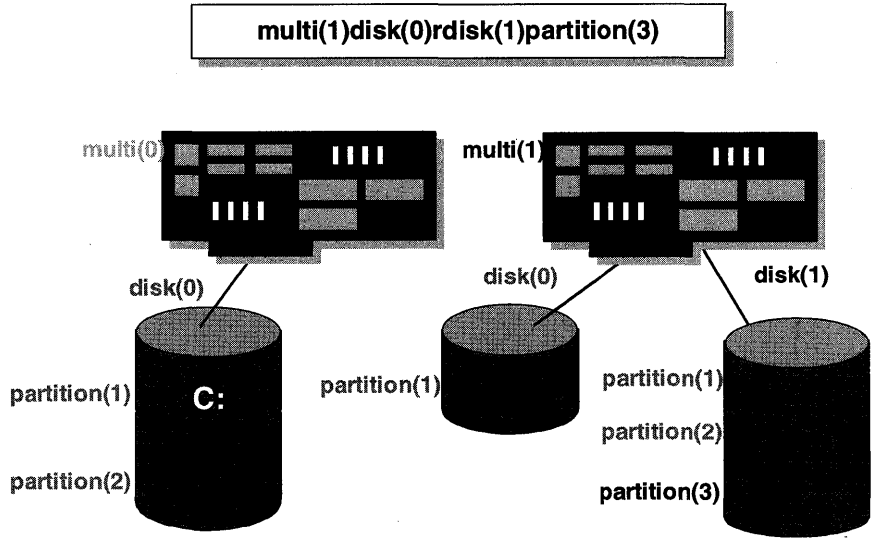
1. You have decided to establish a mirror set with the system partition of your hard disk, which also contains the Windows NT Server system files. How can you protect yourself in the event that the boot drive becomes inaccessible?

   Create a Windows NT boot disk that points to the mirrored partition.

2. Here is an example of an ARC name:

   multi(1)disk(0)rdisk(1)partition(3)

   Draw a picture of what the configuration looks like.



Chapter 7

Page 245

► **To verify the DHCP configuration**

4. What is the DHCP-assigned IP Address of the domain controller?

   The address will vary. It is not the same address that was manually assigned earlier; it will be in the range of the DHCP Scope.

5. What is the address of the DHCP Server?

   131.107.2.150

Chapter 9

Lesson 1, page 273

Review Questions

The following question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- You are installing Microsoft Windows NT Server 3.5 in your existing network, which includes LAN Manager, Windows NT 3.1, and Novell NetWare. Which network clients can be installed from the Windows NT Server CD-ROM?

  Microsoft Network Client 3.0 and Windows for Workgroups, which are on the CD-ROM, have IPX protocols and redirectors that allow access to Novell NetWare servers. The LAN Manager for MS-DOS client software includes NetWare Connectivity, but additional Novell client software is required to install it.

Page 283

► **To test for domain validation**

7. What message did you receive?

   You were successfully logged on to DOMAIN-B as Administrator by \\PDC-B with administrator privilege.

Lesson 2, page 283

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What network client installation functions can be performed using the Network Client Administrator tool?

   Create a Network Installation Startup Disk—this allows you to create an over-the-network installation disk to install either Microsoft Network Client or Windows for Workgroups client.

2. List three methods that can be used to share the network client installation files.

   Share the \CLIENTS directory on the Windows NT 3.5 CD-ROM.

   Copy files to a new directory on the hard disk and share the directory.

   Use an existing shared directory.

3. What information is required for the Network Startup Disk Configuration dialog box?

   Computer Name—the name used for the computer when booting from the startup disk.

   User Name—the name used to log on to the domain when using the startup disk.

   Domain Name—the domain from which you are logging on.

   Network Protocol—the protocol used by the startup disk to connect to the server containing the installation files.

   Destination Path—the location on the startup disk to which the startup files are copied.

4. If you have a variety of machines with different floppy drive sizes and different network adapters, what is required when creating network installation startup disks?

   You must create an installation disk for each type of network adapter and floppy disk type.

Lesson 3, page 287

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

- What disk sets can you make with Network Client Administrator?

  Network Client 3.0 for MS-DOS and Windows

  Remote Access 1.1a for MS-DOS

  TCP/IP 32 for Windows for Workgroups 3.11

  LAN Manager 2.2c for MS-DOS

  LAN Manager 2.2c for OS/2

Page 294

► **To use User Manager for Domains**

3. What did you need to do before the user was created?

   Verify the administrator password.

Page 295

► **To use File Manager**

2. What menu is new after installing Server Tools that allows you to set permissions on NTFS drives on a Windows NT Server computer?

   Security.

Lesson 4, page 295

Review Question

The following question is intended to reinforce key information presented in this lesson. If you are unable to answer the question, review this lesson and then try the question again.

- From what location(s) can the Windows NT Server Tools be used to administer a Windows NT domain?

  The Windows NT Server Tools can be used to administer a Windows NT Server domain from 16-bit Windows-based or Windows NT Workstation computers.

Chapter 10

Lesson 1, page 312

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to monitor performance to determine whether your server has reached capacity. What is the first step in analyzing a computer's performance?

   The first step in analyzing a computer's performance is to develop a baseline of performance. Performance Monitor can be used to create the baseline. Determine what areas of system usage you want to monitor, such as disk, memory, server, and so on, and then add those objects, counters, and appropriate instances to a log. Generate a log file during times when activity is "normal" on the computer.

2. You have to determine whether your system performance will decline after adding an additional 20 users to the server. How can you figure out whether this will happen?

   First, develop a baseline of current performance using Performance Monitor's log view. Then add the new users with their normal activities on the server and generate a new log of server activity. Finally, compare the baseline performance with the current performance figures, using Performance Monitor's chart view.

Page 320

► **To run a benchmark test before introducing the bottleneck**

4. Record the number of seconds it took to complete the test:

   Results will vary.

Page 320

► **To introduce a mystery bottleneck and rerun the benchmark**

3. Record the number of seconds it took to complete the test.

   Results will vary.

Page 321

► **To identify the bottleneck**

1. Use the counter values in the report to determine which device object is the bottleneck. Which counter indicates that the associated device is the most heavily used?

   Processor

Page 322

► **To identify the application**

4. Determine which application is stressing the processor. Which application is using most of the CPU time?

   APP1-5

Lesson 2, page 326

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. You want to monitor the performance of your physical disks, but whenever you look at the data collected for the counters, they always show 0. Why?

   Disk counters are not enabled by default in Windows NT. This is because of performance degradation in the system on 80386-based systems. To enable disk performance counters, use the DISKPERF -Y command, and then restart the computer.

2. You have to determine whether a specific application is using too much processor time. How can you do this?

   Use Performance Monitor and create a chart with the Process:% Processor Time counter for the appropriate application instance.

Page 331

► **To analyze performance**

1. Record the number of seconds required to complete the test.

   Results will vary.

3. Where was the data read from, cache (green line) or the disk where <perf_drive> is?

   Cache.

4. Does it appear as though any data was read from disk?

   No.

Page 332

► **To force a read from disk**

4. How is the Memory:Cache Bytes affected (purple line on the Performance Monitor display) while the file is being copied?

   It increases as the copy is performed, and then drops back down when complete.

Page 333

► **To analyze performance**

1. Record the number of seconds required to complete the test.

   Results will vary.

2. Where was most of the data read from, cache (green line) or the disk where <perf_drive> is?

   Disk.

3. Does it appear as though any data was read from cache (green line)?

   Yes, some was read from cache.

4. Can you guess why some of the data was read from cache? (Hint: Notice that some data began to come from cache shortly after data began to be read from disk.)

   Read-aheads.

5. How much less time did it take I/O Test to read the 3 MB from cache (previous test) than from disk (even with read-ahead)? Record the number of seconds.

   Results will vary.

6. What percent was read from cache faster than from disk (even with read ahead)? ((from disk result – from cache result) / from cache result) * 100 = % faster. Record your answer.

   Results will vary.

Page 340

► **To isolate the bottleneck**

10. Which computer (your computer or PDC-B) has counters that are exceeding the threshold?

    Results can vary; it could be either of the two computers.

11. Which counter indicates that you have a bottleneck?

    Results can vary, but in any event you will notice a lot of data being transmitted. If you do have a bottleneck, it could be either Redirector Concurrent Commands on PDC-A or Work Item Shortage on PDC-B.

12. Which device is your bottleneck?

    If any, it is probably the network adapter card in the PDC-A.

15. What is the value of the bookmarks?

    They allow you to focus on a particular test, isolating specific network traffic. If you anticipate network traffic similar to that generated by one of the tests, you can see potential bottlenecks that might not be visible if you looked only at the averages.

Lesson 3, page 342

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. The programmer is not allowed to decide whether data is read from cache or disk. Under what conditions will the data be read from cache?

   For read-aheads, or if many users are requesting the same data.

2. On a computer that runs a fixed set of processes, Performance Monitor helps you determine that 70 percent of cacheable reads and writes are being satisfied by physical disk access. What can be done to increase the cache hit rate?

   Add more RAM or distribute reads and writes to another processor.

Lesson 4, page 349

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Explain two factors in choosing a network adapter card.

   Supports full bus width of computer.

   Must be NDIS 3.*x* compatible.

2. You are running an application that uses very large data files. The requests from the client computers to the server are normally for large sections of the data file. What type of data transfer (RAW or CORE) should be used?

   RAW.

Chapter 11

Lesson 1, page 363

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What is one advantage of direct hosting?

   Applications that support direct hosting can bypass the NetBIOS layer and send requests directly to the IPX protocol.

2. What does setting the frame type to Auto Detected do?

   Setting the frame type to Auto Detected causes a Windows NT Server computer to attempt to determine the frame type running on the network.

3. You have just installed Windows NT Server with NWLink, and now your NetWare users want to use the Windows NT Server for file and print sharing. Will they be able to do so?

   No, NWLink is only a protocol. Your NetWare users will be able to access the Windows NT Server only for client-server applications.

4. You have just installed SNA Server for Windows NT on your Windows NT Server. What else must be done at the server and on your NetWare clients for them to be able to access Windows NT and SNA Server?

   On the server you must have NWLink protocol installed.

   On the clients, they must have a front end (client-side) application to access the SNA Server (server-side) application.

Lesson 2, page 368

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. What is the purpose of the Gateway Service for NetWare?

   It allows Microsoft network clients to occasionally access the NetWare servers in their environment without the overhead of having multiple redirectors installed on their machines.

2. You are the administrator of both the Windows NT servers and the NetWare servers. You are sitting at a Microsoft network client and you need to make changes to users on the NetWare server. You start the NetWare SYSCON utility on the client and it fails. Why?

   The Gateway Service for NetWare converts SMBs to NCPs for the NetWare server. SYSCON is an NCP utility which expects to see NCP returned from the NetWare server, but the Gateway Service for NetWare converts the NCPs to SMBs, which causes SYSCON to fail.

Lesson 3, page 373

Review Questions

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review this lesson and then try the question again.

1. Why is selecting a preferred server important?

   This is the server that will validate the initial NetWare logon request.

2. You are configuring security on the Gateway Service for NetWare and you leave the default settings. What permissions will users have at the NetWare server?

   They will have the same permissions as the account that made the connection from the gateway to the NetWare server.

Page 376

► **To access the NetWare server through the gateway**

5. Make changes to the file and attempt to save the file. Were you successful? Why or why not?

   No. The permissions for NWPUBLIC are Read.

7. Make changes to the file and attempt to save the file. Were you successful? Why or why not?

   Yes. The permissions for NWDATA are Full Control.

11. If an administrator wanted to set permissions on a specific file or directory, how would you do this? Who would be affected by it?

    Set permissions on the NetWare server.

    It would affect everyone using the gateway, because permissions are assigned to the gateway account.

APPENDIX A

Installation Files and Components

Migration of Windows 3.*x* Configuration Data to Windows NT

When Windows NT is installed on top of Windows 3.*x*, *.INI file data, *.GRP file data, and REG.DAT (this file contains all of the OLE data for Windows 3.1) data is migrated into the Windows NT environment. Currently the migration process is one-way only, from Windows 3.*x* to Windows NT, and occurs only the first time that a user name logs on to the computer after installation using the Setup program. Each time a new user logs on to the computer, the user will be prompted to migrate the Windows 3.*x* settings. The migration process actually occurs in two stages:

Stage One

When WINLOGON.EXE starts the first time after Windows NT has been installed over Windows 3.*x*, the REG.DAT file and the portions of the WIN.INI that are mapped to the Registry SOFTWARE hive are migrated into the Windows NT Registry. This includes the following:

- All of the OLE information stored in the Windows 3.1 Registry (REG.DAT). This information is stored in the Windows NT Registry under HKEY_CLASSES_ROOT.

- The following sections and variables from the Windows 3.*x* WIN.INI are migrated:
  - [Devices]
  - [PrinterPorts]
  - [Embedding]
  - [Compatibility]
  - [Fonts]
  - [FontSubstitutes]
  - [Windows]

    Spooler

    DeviceNotSelectedTimeout

    TransmissionRetryTimeout

If any errors occur during the migration process, they will be logged in the Event Viewer's Application log.

Stage Two

This portion of the migration process occurs the first time every new user logs on to a Windows NT computer that has been installed over Windows 3.*x*.

Note The "Administrator" and "System" user names are exempt and will never start a migration. For all other user names, the migration occurs only once, the first time that specific user name is used to log on to the computer.

This part of the migration process begins with a dialog box being displayed to allow the user to select which parts of the Windows 3.*x* configuration, if any, to migrate—the *.INI files and *.GRP files. If you choose Cancel, the migration will not occur, and the next time that user name logs on, the user will again be asked which portions to migrate. Choosing OK will begin the migration process; however, if both *.INI and *.GRP files were cleared, nothing will be migrated and the user will not be asked again.

- The following sections and variables from the WIN.INI are migrated during this stage:
  - [Cursors]
  - [DeskTop]
  - [Extensions]
  - [Intl]
  - [Clock]
  - [Terminal]
  - [TrueType]
  - [Colors]
  - [Sounds]
  - [Windows]

    CursorBlinkRate

    BorderWidth

    ScreenSaveTimeOut

    ScreenSaveActive

    KeyboardSpeed

    KeyboardDelay

    Beep

    SwapMouseButtons

    DoubleClickSpeed

    MouseThreshold1

    MouseThreshold2

    MouseSpeed

- The following sections and variables from the SYSTEM.INI are migrated during this stage:
  - [boot]

    SCRNSAVE.EXE

- The following sections and variables from the CONTROL.INI are migrated during this stage:
  - [Current]
  - [Color Schemes]
  - [Custom Colors]
  - [MMCPL]
  - [Patterns]
  - [Screen Saver.Marquee]
  - [Screen Saver.Mystify]
  - [Screen Saver.Stars]

Upgrading Windows NT 3.1 to Windows NT Server 3.5

Registry Entries Deleted

Under \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, several Registry entries are deleted during the text mode portion of an upgrade. These include:

\Services\Eventlog\System\fat_rec

\Services\Eventlog\System\hpfs_rec

\Services\Eventlog\System\ntfs_rec

\Services\Eventlog\System\cdfs_rec

\Services\Eventlog\Security\SC Manager Audit

\Services\Eventlog\Security\NetDDE Audit

\Services\fat_rec

\Services\hpfs_rec

\Services\ntfs_rec

\Services\cdfs_rec

\Services\videoprt

\Services\mvopl3

\Services\vga

Registry Entries Added

Several Windows NT 3.5 Registry entries are added during text mode:

\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
\Windows NT\CurrentVersion

\Winlogon

\System:REG_SZ:lsass.exe

\WOW\Compatibility

123W	SPJWIN30
ANIMATE	COBOL
WIN2WRS	PHOTOSHO
PM4	PSTYLER
PB030	CHARM40
XPRESS	QPW
WPWIN	WPWPRINT

\MCI32

- WaveAudio
- Sequencer
- CDAudio

\MCI

- AVIVideo

\Drivers32

- msacm.msadpcm
- msacm.imaadpcm
- msacm.msgsm610
- vidc.iv31
- vidc.iv32

\IniFileMapping\NtNetIni

- Shared Parameters

\IniFileMapping\System.Ini\boot

- SCRNSAVE.EXE

\IniFileMapping\WinIni

- Console

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet

\Control\GroupOrderList

Video

Extended base

SCSI miniport

\Control\NLS\Language

0408

\Control\WOW

KnownDLLs

\Control\Session Manager\Subsystems

Windows

\Control\Session Manager

GlobalFlag

\Control\CrashControl

DumpFile

\Control\FileSystem

Win31FileSystem:REG_DWORD:0

\Services\EventLog

ImagePath

Type

\Services\EventLog\System\Netlogon

EventMessageFile:REG_EXPAND_SZ:"%SystemRoot%\System32\NetMsg.dll"

TypesSupported:REG_DWORD:00000007

ParameterMessageFile:REG_EXPAND_SZ:"%SystemRoot%\System32\kernel32.dll"

\Services\Cpqarray

Group

Tag

\Services\Delldsa

Group

Tag

\Control\ServiceGroupOrder

List

\Control\Service\ATI

InstalledDisplayDrivers

To add the above entries to the Registry, the contents of the TXTSETUP.SIF (SIF — Setup Information File) are used. In addition, for the previous entries that do not have a value type or value specified, there are templates of \HKEY_LOCAL_MACHINE\SOFTWARE (SOFTWARE._) and \HKEY_LOCAL_MACHINE\SYSTEM (SYSTEM._) on the installation media, which include the appropriate values to be added.

Files Deleted

Several files are deleted during text mode. Two are of special interest:

- LMUICMN0.DLL
- LMUICMN1.DLL

AMI4448.SYS	CDFS_REC.SYS
FAT_REC.SYS	HPFS_REC.SYS
NTFS_REC.SYS	LMUICMN0.DLL
LMUICMN1.DLL	SVCCTRL.DLL
EVENTLOG.EXE	MSGSVC.EXE
SCREG.EXE	OEMNADDP.INF
CTYPE1.NLS	CTYPE2.NLS
CTYPE3.NLS	BOWSER.SYS
MVOPL3.DLL	MVOPL3.PAT
MMSNDSRV.DLL	MVOPL3.SYS
WINMSDP.EXE	NETBIOS.DLL
MSADPCM.DLL	IMAADPCM.DLL
MSGSM610.DLL	FILELIST.INF
OLE2PR32.DLL	MSCON.TTF
MSCON.FOT	

Because the upgrade process will have deleted the files listed above, certain applications and utilities may generate an error message, indicating that one or more of the above files is missing or cannot be found when run under Windows NT 3.5. This problem will be encountered with some of the utilities included in the Windows NT 3.1 Resource Kit, such as Domain Monitor and Browser Monitor, and when the Windows NT 3.1 Administrative Tools, such as User Manager or Server Manager, are run under Windows NT 3.5. In both cases, an error message will be generated, saying that LMUICMN0.DLL could not be found in the path. The Windows NT 3.5 Resource Kit provides updated versions of the utilities that will work properly under Windows NT 3.5.

Installing Windows NT Server 3.5 on RISC-Based Computers

The JZSETUP.EXE utility is used to configure the built-in Multiboot functionality on RISC-based computers. JZSETUP.EXE has the following options:

- Load Default Configuration—This option allows new values to be specified in the firmware, such as screen resolution, and so on.
- Load Default Environment—This resets the default environment variables to their defaults. (See the following Environment Variable section for more information.)
- Change Active Boot Selection—This allows the default (highlighted) Multiboot menu item to be changed.
- Add/Delete Boot Selection—This allows selections to be added or removed from the built-in Multiboot menu.
- Change Environment Variable—For more information on the environment variables that can be set through this option, see the Environment Variable section below.
- Set CMOS Time—This can be used to change the system time.
- Set Ethernet Address—This can be used to change the Ethernet Address for the built-in Ethernet card.

Environment Variables

The following are the environment variables necessary to boot Windows NT on an ARC-based system:

- LOADIDENTIFIER—This is the name for the boot selection that the built-in Multiboot loader menu will display.
- SYSTEMPARTITION—This is an ARC pathname to the system partition. By default, this will be: scsi()disk(0)rdisk()partition(1).
- OSLOADER—This is an ARC pathname to OSLOADER.EXE. The default is scsi()disk(0)rdisk()partition(1)\OS\NT\OSLOADER.EXE.

- OSLOADPARTITION—This is an ARC pathname to the partition containing the Windows NT Kernel (NTOSKRNL.EXE). The default is scsi()disk(*x*)rdisk()partition(*y*), where *x* is the drive number and *y* is the partition number where Windows NT is installed.
- OSLOADFILENAME—This is the path on the OSLOADPARTITION to the Windows NT Kernel (NTOSKRNL.EXE). The default is *\winnt_root*\SYSTEM32\NTOSKRNL.EXE
- OSLOADOPTIONS—This variable specifies any Windows NT boot parameters. This variable can be either DEBUG or NODEBUG.

Other Important Environment Variables

- CONSOLEIN—This is used to specify the system's input device. The default is multi()key()keyboard.
- CONSOLEOUT—This is used to specify the system's output device. The default is multi()video()monitor().
- AUTOLOAD—This is used to specify whether the built-in Multiboot menu will automatically load. By default it is set to YES, which will start Multiboot.
- TIMEZONE—This variable specifies the time zone that the system is in.
- A:—This is an ARC path to the A disk drive. The default is multi()disk()fdisk(0).
- CD:—This is an ARC path to the CD-ROM drive. The default is scsi()cdrom(2)fdisk().

Setup Under Windows NT

After a computer completes the boot process from the first two Setup boot disks, the computer is running under Windows NT. During the process of loading from the Setup boot disks, while SETUPLDR.BIN and then SETUPDD.SYS are running, the white bar at the bottom of the screen displays the Windows NT components being loaded. The components loaded during this process include the following (all loaded from the second Setup boot disk, unless otherwise noted):

- Windows NT Executive — This is the kernel (NTKRNLMP.EXE) from the first Setup boot disk.
- Hardware Abstraction Layer (HAL) — This will be HAL486C.DLL, HALMCA.DLL, or HALNCR.DLL, depending on the type of computer detected. These are all located on the first Setup boot disk. All of the HALs used on the Setup disk are multiprocessor HALs, because a multiprocessor HAL can be used on a single processor system.
- Windows NT Configuration Data — This loads SETUPREG.HIV, which is a small Registry used by the Setup process. It contains a single Control Set that causes Windows NT to load a single driver (SETUPDD.SYS).

- Locale-Specific Data — This is loading C_1252.NLS, C_437.NLS, and I_INTL.NLS.
- Setup Font — This is VGAOEM.FON, the font used during the installation process.
- Windows NT Setup — This loads SETUPDD.SYS, which is a Windows NT kernel mode driver that does most of the installation work.
- Video Driver — This loads VGA.SYS and VIDEOPRT.SYS.
- Floppy Disk Driver —This loads FLOPPY.SYS.
- Keyboard Driver — This loads I8042PRT.SYS, KBDCLASS.SYS, and KBDUS.DLL.
- FAT File System — This loads FASTFAT.SYS.
- SCSI Port Driver —This driver is loaded from Setup boot disk 2 or 3, if a SCSI device is found after the SCSI detection stage. After this driver is loaded, any other necessary drivers such as SCSI CD-ROM, SCSI Floppy Disk, and SCSI Disk are loaded.
- ESDI/IDE Hard Disk or Micro Channel Hard Disk —For ESDI/IDE, ATDISK.SYS is loaded, and for Micro Channel, ABIOSDSK.SYS is loaded. These drivers are loaded from Setup boot disk 3, and only if a hard disk of their type is in the computer.
- High Performance File System (HPFS) —This loads PINBALL.SYS from Setup boot disk 3.
- Windows NT File System (NTFS) —This loads NTFS.SYS from Setup boot disk 3.

How a Diskless Installation and Upgrade Works

The diskless installation and upgrade works by copying the files that are normally on the three Setup boot disks from the server to the system partition on the computer being installed or upgraded.

- c:\$LDR$—This file is a copy of SETUPLDR.BIN, which is also in the \$WIN_NT$.~BT directory.
- c:\TXTSETUP.SIF—This is the Setup Information File (SIF) that controls the install/upgrade process.
- c:\WIN_NT.~BT—The WIN_NT.~BT directory is similar in concept to the WIN_NT.~LS directory, used by WINNT.EXE and WINNT32.EXE for temporary local storage of the Windows NT files, in that it is only used temporarily. However, the WIN_NT.~BT directory is different, because it is where all the files that would normally be located on the three Setup boot disks are temporarily stored. When the system reboots the first time, instead of using boot disks the files are loaded from the WIN_NT.~BT directory.

  The BOOTSECT.DAT file and NTLDR are also located in this directory.

- c:\$WIN_NT$.~BT\BOOTSECT.DAT—The BOOTSECT.DAT is used to boot the system after WINNT.EXE or WINNT32.EXE has copied all the files from the network server to the local hard disk. BOOTSECT.DAT loads and starts c:\$LDR$ (SETUPLDR.BIN), which starts the text mode portion of the installation or upgrade.
- c:\WIN_NT.~BT\SYSTEM32—This directory has the same contents as the \SYSTEM32 directory on the second Setup boot disk (NTDLL.DLL and SMSS.EXE).
- BOOT.INI Modifications—To have BOOTSECT.DAT loaded to start the installation or upgrade process, the BOOT.INI file is modified and the following entry is added when using /B with Windows NT 3.5 Workstation:

  C:\WIN_NT.~BT\BOOTSECT.DAT="Windows NT 3.5 Workstation Installation/Upgrade"

  This entry is set to the default selection, and the "Timeout" value in the BOOT.INI is set to 5 seconds. As a result, the system will continue the install/upgrade process when it reboots.

Files Used by Setup

The *.INF Files Used by Setup

- TXTSETUP.INF
- FILELIST.INF
- SETUP.INF
- INITIAL.INF
- REGISTRY.INF

The *.INF File Formats

The TXTSETUP.INF file is functionally equivalent to the Windows 3.*x* SETUP.INF file. The TXTSETUP.INF contains the following sections:

Section	Description
[SourceDisks]	This section contains the source disks from which Windows NT Server 3.5 will be installed. When installing from a CD-ROM or over the network, there will be only two entries in this section.
[SetupData]	This section contains information on what product is being installed, and the installation requirements.
[debug]	Entries in this section can be changed to have the Setup program send Debug information to one of the system's COM ports.
[WinntDirectories]	This section contains the directories relating to the directory chosen by the user for the Windows NT installation, which are used to specify the directory files in which the various files are installed. Entries in this section are of the format <shortname> = <directory>, where <directory> must not start or end with \ unless it is the root directory.
[WinntFilesToDelete]	This section contains a list of files that will be deleted if they are present in the target installation directory structure. These entries are of the format <shortname>,filename. The <shortname> entry corresponds to the entries in the [WinntDirectories] section.
[BootDirectories]	This section is used only on *x*86-based systems. It is the root directory of the active partition. This entry has the same format as the [WinntDirectories] entries: <shortname> = <directory>.
[BootFilesToDelete]	This section is used only on *x*86-based systems. It specifies the files that will be deleted if present in C:\. These entries are of the format <shortname>,filename. The <shortname> entry corresponds to the entries in the [BootDirectories] section.
[msifs]	This section lists the installable file systems that Setup will install on the system.
[NoDeleteSource]	This section is used when a WINNT.EXE Setup is performed after the system has rebooted, when the Setup boot disk has started moving files around on the local hard disk. If a file is listed in this section, the file deletion is suppressed. The format of the entries in this section is <filename>=*xx*, where *xx* must be present but can be any value.
[Map.Computer] and [Computer]	These sections contain the information regarding the computer type selections that Setup allows. They define the shortname used by Setup to refer to the computer type in other sections.

(continued)

Section	Description
[Map.Display] and [Display]	These sections contain the information regarding the display type selections that Setup allows. In the [Display] section the entries are of the format: <string> = "Setup selection", <TXTSETUP.INF section for the files to be copied>, <shortname>, Xresolution, Yresolution, bits per pel, vrefresh, interlaced If the interlaced entry is –1, it is noninterlaced.
[Map.Mouse] and [Mouse]	These sections contain the information regarding the mouse selections that Setup allows. The format of the entries in the [Mouse] section is: <shortname> = "Setup selection", <TXTSETUP.INF section for the files to be copied>, <type>
[files.none]	This section is referred to when Setup does not have to copy any special files to support a piece of hardware.
[Map.Keyboard] and [Keyboard]	These sections contain the information regarding the keyboard selections that Setup allows. The format of the entries in the [Keyboard] section is: <shortname> = "Setup selection", <TXTSETUP.INF section for the files to be copied>, <type>
[SCSI.EISA], [SCSI.ISA], and [SCSI.MCA]	These sections contain the Setup information for the various SCSI adapters that Windows NT supports. The entries in these sections have the format: <shortname> = "Setup selection", <TXTSETUP.INF section for the files to be copied>, <shortname>, <shortname from the [WinntDirectories] section>
[SCSI.ISA.Load], [SCSI.EISA.Load], and [SCSI.MCA.Load]	These sections contain the load information for the various SCSI adapters that Windows NT supports. The entries in these sections have the format: <short disk name>,<shortname>
["Keyboard Layout"]	The entries in this section specify the shortname and the Setup selection for the Setup keyboard layout option. These entries have the form: <shortname> = "Setup selection"
[BootCode]	This section is used to install the Windows NT Boot Loader, boot sector on the various file systems. These entries have the format: <file system> = <short disk name>, <filename>, <boot sector size>

The Remaining TXTSETUP.INF File Entries

Most of the remaining entries in the TXTSETUP.INF file specify the files that have to be copied to support a specific hardware component. The section headings are of the form: [<shortname>] or [files.<shortname>]. The format of the entries in these sections is of the form:

<short disk name>, <filename>, <short [WinntDirectories] name>, <filename to rename the file to>

If the line ends in "", the file will retain the same name. For example, the entry: d2,haltest.dll,2,hal.dll will copy haltest.dll from the second disk to directory number 2 (specified in [WinntDirectories] section) as hal.dll.

The exceptions to the above are the following sections: [Files.KeyboardLayout], [IFSDLL], [Kernel], [MiscFiles], [ntdetect]. The entries in these sections all use the following formats: <shortname> = <short disk name>, <filename>, <short [WinntDirectories] name>, <filename to rename the file to>

TXTSETUP.OEM

This file is used by Original Equipment Manufacturers (OEMs) to install the correct files and Registry entries for their hardware devices. This file uses the hash (#) character to introduce comments. All strings with embedded spaces, commas, or hashes should be double-quoted, such as "Bill and Ted's Excellent Video Card".

This file uses the general format:

[section name]
key = value1, value2, ...

The TXTSETUP.OEM file contains the following sections:

[Disks]

This section lists all the disks in the disk set.

#

<description> is a descriptive name for a disk, used when prompting for a specific disk.

<tagfile> is a file whose presence allows Setup to recognize that the correct disk is inserted.

<directory> is where the files are located on the disk.

d1 = <description>,<tagfile>,<directory>

d2 = <description>,<tagfile>,<directory>

[Defaults]

This section lists the default selection for each "required" hardware component. If a line is not present for

a component, the default becomes the first item in the [<component_name>] section (see below).

#

<component_name> is one of computer, display, keyboard, mouse, SCSI.

<id> is a unique <within the component> string to be associated with an option.

<component_name> = <id>

.

.

[<component_name>]

This section lists the options available for a particular component.

#

<id> is the unique string for the option.

<description> is a text string, presented to the user in a menu.

<key_name> gives the name of the key to be created for the component in

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

<id> = <description>,<key_name>

.

.

[Files.<component_name>.<id>]

This section lists the files that should be copied if the user selects a particular component option.

#

<file_type> is one of driver, port, class, DLL, hal, inf, or detect (see below for more information).

<source_disk> identifies where the files are to be copied from, and must match an entry in the [Disks]

section.

<filename> is the name of the file. This is appended to the directory specified for the disk in the [Disks]

section to form the full path of the file on the disk.

<file_type> = <source_disk>,<filename>

.

.

[Config.<component_name>.<id>]

This section specifies values to be set in the registry for particular component options. Required values

in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\xxx key are created

automatically. This section is used to specify additional keys to be created in .....\Services*xxx* and values

in .....\Services*xxx* and Services*xxx**yyy*.

#

<key_name> is relative to the services node for this device. If it is empty, then it refers to the services

node. If specified, the key is created first.

<value_name> specifies the value to be set within the key.

<value_type> is a string, such as REG_DWORD. (See the Registry Terms section below for more

information on the possible <value_type>s.)

<value> specifies the actual value; its format depends on <value_type>

value = <key_name>,<value_name>,<value_type>,<value>...

.

.

The <file_type> in the [Files.<component_name>.<id>] section

- Driver—This is a valid type for all components, and the file is copied to *winnt_root*\SYSTEM32\DRIVERS.
- Port—This is a valid type for keyboard, mouse, and SCSI components and allows for a distinction between port and class drivers, but is equivalent to driver type. This file is copied to *winnt_root*\SYSTEM32\DRIVERS.
- Class—This is a valid type for keyboard and mouse components. If specified, this replaces the standard class driver. This file is copied to *winnt_root*\SYSTEM32\DRIVERS.
- DLL—This is a valid type for all components and is particularly useful for the GDI portion of a display driver. This file is copied to *winnt_root*\SYSTEM32.
- Hal—This is a valid type only for computer component. On *x*86-based systems, this file is copied to *winnt_root*\SYSTEM32\HAL.DLL. On ARC-compliant systems, this file is copied to \OS\NT\HAL.DLL on the system partition.
- INF—This is a valid type for all components and is used to copy a GUI inf file for use with system maintenance setup. This file is copied to *winnt_root*\SYSTEM32.
- Detect—This type is valid only on *x*86-based systems for the computer component. If specified, this replaces the standard *x*86 hardware recognizer (NTDETECT.COM). This file is copied to C:\NTDETECT.COM.

APPENDIX B

File Systems

The following tables outline the advantages and disadvantages of the NTFS, FAT, and HPFS file systems.

Table 1: NTFS

Advantages	Disadvantages
Supports complete Windows NT Server 3.5 security, so that you can specify who is allowed various kinds of access to a file or directory.	Recognized only by Windows NT. When the computer is running another operating system (MS-DOS or OS/2), that operating system cannot access files on an NTFS partition.
Keeps a log of activities to restore the disk in the event of power failure or other problems.	If drive C is formatted for NTFS, you cannot boot MS-DOS from your hard disk or use MS-DOS to access any files on the NTFS partition. But you can still run MS-DOS–based applications when using Window NT.
Supports file and directory names of up to 255 characters and supports extended file attributes. Automatically generates correct MS-DOS filenames so that files can be shared with MS-DOS users.	

Table 2: FAT

Advantages	Disadvantages
Allows access to files when your computer is running another operating system, such as MS-DOS or OS/2.	Files are not protected by the security features of Windows NT Server 3.5.
FAT is the most widely used file system for personal computers.	
	Less robust than NTFS; for example, no automatic disk-restoration features.

Table 3: HPFS

Advantages	Disadvantages
Ensures file compatibility if you want to switch between Windows NT and OS/2 on your hard disk.	Has not been widely adopted.
Supports long filenames.	Files are not protected by the security features of Windows NT Server 3.5.
	Does not auto-generate 8.3 filenames.
Provides better error correction than the FAT file system does.	MS-DOS– and Windows 3.1–based applications cannot access files with long filenames or with long directory names in their paths.

APPENDIX C

The Server Service Configuration Parameter Values

Server optimization level	**Parameter Values per Server RAM (MB)**							
Parameters	8	12	16	32	64	128	512	1024
Minimize Memory Used			*[MAX]*					
Init work items	4	6	8	8	8	8	8	8
Max work items	32	48	64	64	64	64	64	64
Raw work items	8	12	16	16	16	16	16	16
Max Paged Memory (MB)	4	6	8	8	8	8	8	8
Max NonPaged Mem (MB)	2	3	4	4	4	4	4	4
Thread Count Add	2	2	2	2	2	2	2	2
Blocking Threads	2	2	2	2	2	2	2	2
Balance				*[MAX]*				
Init work items	8	12	16	32	32	32	32	32
Max work items	64	96	128	256	256	256	256	256
Raw work items	16	24	32	64	64	64	64	64
Max Paged Memory (MB)	8	12	16	32	32	32	32	32
Max NonPaged Mem (MB)	4	6	8	16	16	16	16	16
Thread Count Add	2	2	2	5	5	5	5	5
Blocking Threads	2	2	2	4	4	4	4	4

Maximize Throughput ...						*[MAX]*		
Init work items	16	24	32	64	128	256	256	256
Max work items	128	192	256	512	1024	2048	4096	8192
Raw work items	32	48	64	128	256	512	512	512
Max Paged Memory (MB)	–1	–1	–1	–1	–1	–1	–1	–1
Max NonPaged Mem (MB)	–1	–1	–1	–1	–1	–1	–1	–1
Thread Count Add	2	4	5	8	8	8	8	8
Blocking Threads	2	3	4	8	8	8	8	8

APPENDIX D

Windows NT Security Data Structures

Security Descriptor (SD)

A Security Descriptor is a data structure that contains the security information associated with an object. This information is represented by Access Control Lists (ACLs) and Security Identifiers (SIDs) and can include an owner, primary group, discretionary ACL, and a system ACL. The Security Descriptor structure can be used to set and query an object's security attributes. All named objects, named and unnamed processes, threads, and token objects have a Security Descriptor associated with them.

One of the primary goals of the Windows NT security model is the definition of a standard set of security information that applies to all instances of objects. This security information includes the following components that are found in a Security Descriptor:

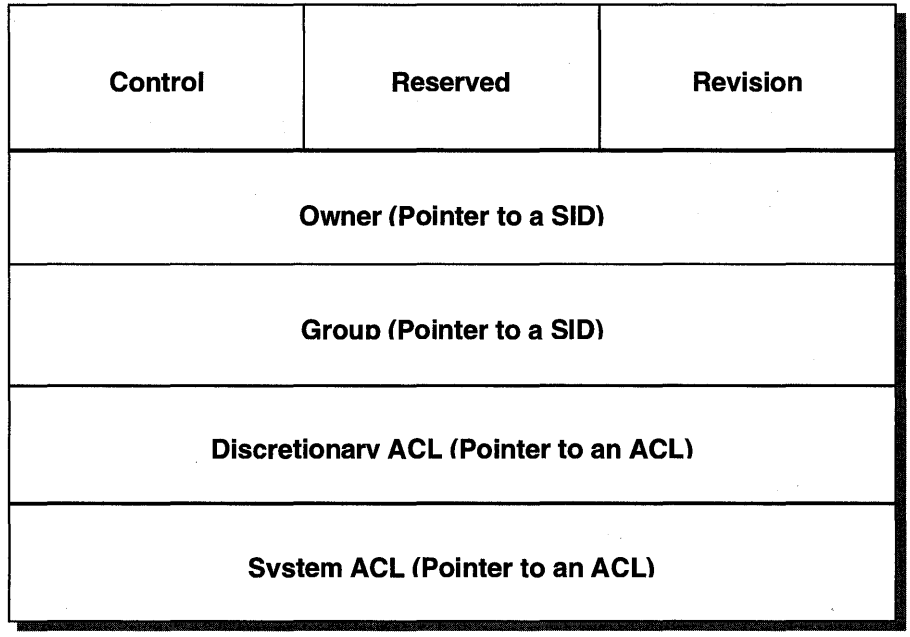
Owner This SID indicates the user or group account that owns the object.

Group This SID indicates which group the object is associated with. This is not necessary for security purposes, but it is useful for organizational purposes and is required to support POSIX.

Discretionary ACL This data structure is controlled by the owner of the object and identifies who can and cannot access the object.

System ACL This data structure is controlled by the security administrator and is used to control audit message generation.

The following diagram shows the structure of security descriptor data.



There are actually two methods that can be used for representing security data structures and their components (listed above).

- Absolute—This method uses a format in which the main body of the Security Descriptor contains pointers to the Security Descriptor components. (This is the method illustrated above.) This method allows each component to be allocated separately, which is useful when all or some of the components are already available.
- Self-Relative—This method uses a format in which the Security Descriptor data structure and all components are stored in a single contiguous block of memory. In this method, the components are pointed to using offsets from the beginning of the structure, rather than using memory addresses as in the Absolute method. This method is useful for storing, on secondary media, or transmitting Security Descriptors where absolute pointers would become invalid while offsets remain valid.

Security Identifier (SID)

The Windows NT security model makes extensive use of special identifiers, called Security Identifiers (SIDs), which are used to identify uniquely a user or group. A SID is a statistically unique number, that is, a SID value used to represent one user should never be used at a later date to represent another user. All SIDs are created using a combination of user information, time, date, and domain information.

SIDs are represented using the following format:

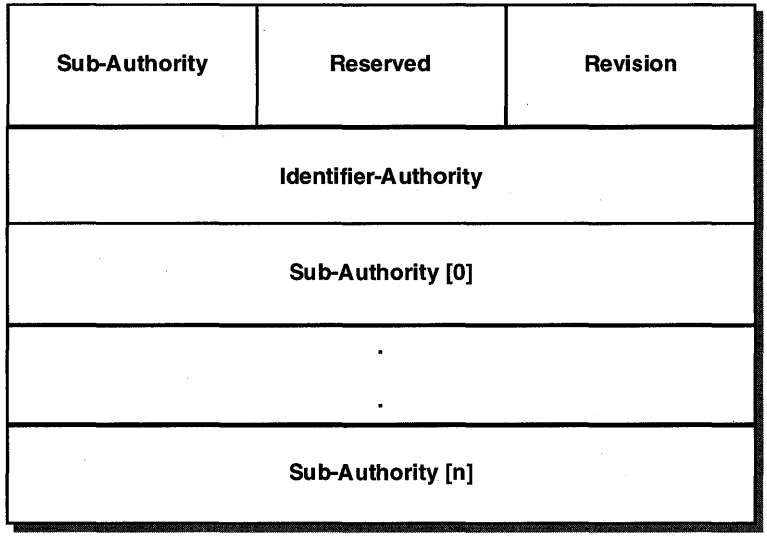
$S\text{-}1\text{-}X\text{-}Y_1\text{-}Y_2\text{-}.....\text{-}Y_n$

In this format, the prefix "S-1" indicates that this is a revision 1 SID and the "X" is the value representing the identifier authority. $Y_1\text{-}Y_2\text{-}.....\text{-}Y_n$ are values representing the SID's sub-authority values. For example, the string S-1-5-36 represents a revision 1 SID, with an identifier-authority value of 5 and a single sub-authority value of 36.

The SID is created from three 32-bit numbers, generated from the following three seeds:

- The computer name.
- The current time.
- The user-mode execution time of the current thread.

The following diagram shows the SID data structure.



The identifier authority value is probably the most important information contained in a SID, because this value identifies the agency that issued the SID; typically it represents a corporation or large organization.

On a Windows NT system there are some predefined, or what are referred to as "well known," SIDs. A "well known" SID is a SID whose value is constant across all Windows NT systems. In addition, there are some "well known" SIDs that are universal across all systems. For a listing of all universal and Windows NT "well known" SIDs, see the *Microsoft Windows NT Resource Guide*, Chapter 3, "Windows NT Security Model."

Locally Unique Identifier (LUID)

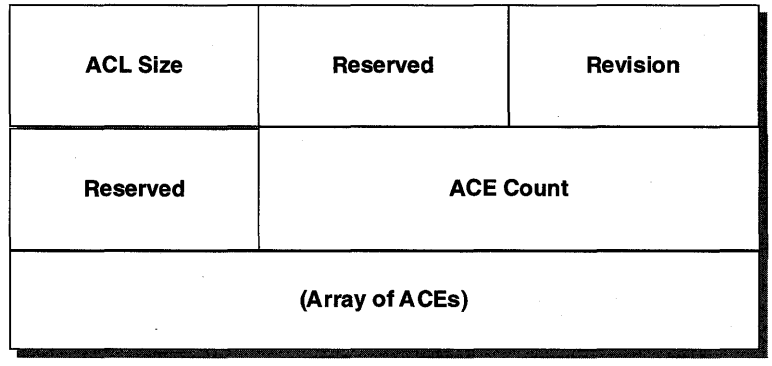
In Windows NT, privileges are used to acquire access to objects or services that normal discretionary access control does not provide. A privilege is represented by what is known as a Locally Unique Identifier (LUID). Each LUID is guaranteed to be unique only on the system on which it was generated. In addition, this uniqueness is guaranteed only until the next time the system is restarted. The data structure of a LUID is a large integer, but LUIDs are represented by character strings.

Similar to SIDs, there are also "well known" privileges, which have constant values. For a listing of some example "well known" privileges, see the *Microsoft Windows NT Resource Guide*, Chapter 3, "Windows NT Security Model."

Access Control Lists (ACL)

As discussed in the Windows NT Architecture course, an Access Control List (ACL) is a list of users and groups and their specific access permissions. Each entry in an ACL is known as an Access Control Entry (ACE). All protected objects have an ACL, which is pointed to by the object's Security Descriptor.

The following diagram shows the ACL data structure.



Access Control Entry (ACE)

Currently there are three defined ACE types:

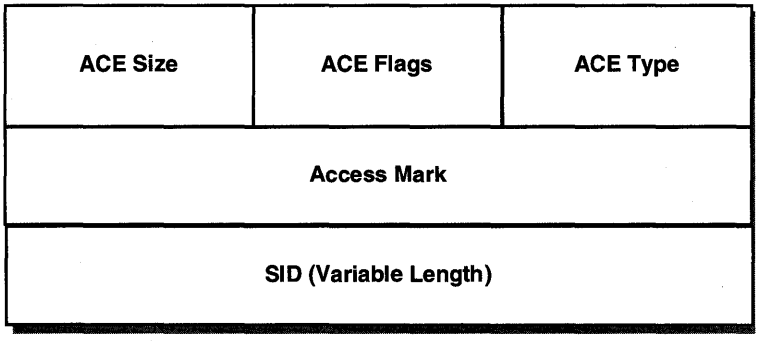
ACE type	Type of security
AccessAllowed	Discretionary Access Control
AccessDenied	Discretionary Access Control
SystemAudit	System security

- AccessAllowed—This ACE is used to grant access to a user or group of users. The user or group is identified by a SID in the ACE. In addition, the access to be granted by the ACE is also included in the ACE.
- AccessDenied—This ACE is used to deny access explicitly to a user or group. Once again, the user or group is identified in the ACE by a SID, and the access to be denied is also included in the ACE.
- SystemAudit—This ACE is used to generate a log of significant security events.

  Discretionary Access Control Lists (DACLs) are used to specify discretionary protection information. System Security ACLs are used to specify system-level security information.

Note There is an important distinction between a DACL that is empty (one with no ACEs) and an object without a DACL. When there is an empty DACL, no accesses are explicitly granted, so access is denied. When an object has no DACL, the object has no protection, so any access request is granted.

The following diagram shows the ACE data structure.



Access Mask

An Access Mask is a component of an ACE that contains the specific types, standard types, and generic types that define the access a user or a group has to an object.

- Specific types—Specific types contain the access mask information that is specific to the object associated with the mask, and they provide a fine granularity of protection when needed. When an object is defined, the specific types must be defined as well. There may be up to 16 specific access types per object type.
- Standard types—Standard types apply to all objects.
- Generic types—Generic types are mapped to the Specific and Standard types when access to an object is requested.

For More Information See Chapter 3, "Windows NT Security Model," in the *Microsoft Windows NT Resource Guide*.

APPENDIX E

Windows NT Server and Novell NetWare File and Directory Permissions and Rights

Windows NT permissions	NetWare rights
Full Control (All) (All)	S – Supervisor
Read (RX) (RX)	R – Read
Change (RWXD) (RWXD)	W – Write
Add (WX) (not in the spec)	C – Create
Change (RWXD) (RWXD)	E – Erase
Change (RWXD) (RWXD)	M – Modify
List (RX) (not in the spec)	F – File Scan
Change Permissions (P)	A – Access Control

File Rights

NetWare rights	Windows NT permissions
S – Supervisor	Full Control (All)
r– Read	Read (RX)
W – Write	Change (RWXD)
C – Create	
E – Erase	Change (RWXD)
M – Modify	Change (RWXD)
F – File Scan	
A – Access Control	Change Permissions (P)

File Attributes

NetWare	Windows NT
Ro – Read Only	R – Read Only
D – Delete Inhibit	R – Read Only
R – Rename Inhibit	R – Read Only
A – Archive	A – Archive
Sy – System	S – System
H – Hidden	H – Hidden
Rw – Read Write	Not Supported
C – Copy Inhibit	Inhibit Macintosh copy (not supported)
X – Execute Only	Not supported
P – Purge	Purge, works with salvage (not supported)
S – Shareable	All files are shareable
T – Transaction	No transaction tracking in Windows NT

Account Restrictions

NetWare	Windows NT
Account	See detail
Password	See detail
Station	Not transferred. NetWare 3.1*x* based on IPX address NetBios name would not work the same way.
Time	Rounded to hour from .5 hour
Intruder limits	Transferred
Disk quotas	Not transferred

Account (Detail)

Restriction	Policy	For each user	Not supported
Expiration Date		√	
Limit Concurrent Connections			√ (Unlimited users in Windows NT)
Account Disabled		√	

Password (Detail)

Restriction	Policy	For each user	Not supported
Required	√		
Minimum length	√		
Force periodic change		√	
Grace logins			√
Require unique		√	
User can change	√		

APPENDIX F

Introduction

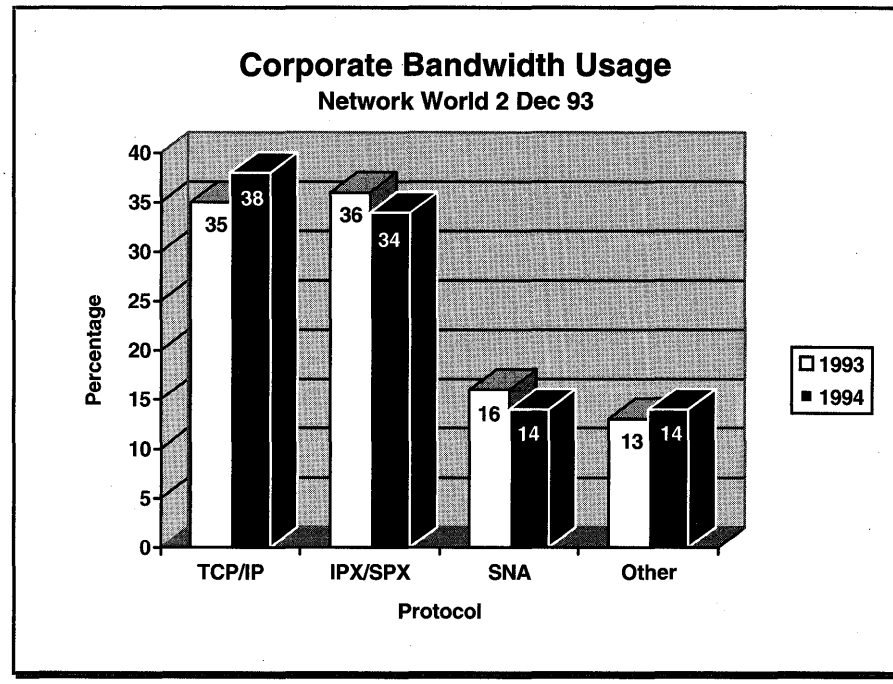
The Microsoft Windows NT Server 3.5 operating system includes key technologies which add value to both new and existing TCP/IP-based networks. In existing networks these new technologies simplify TCP/IP network administration, reduce administrative costs, and resolve common configuration problems. For new network installations they simplify the planning, configuration, and installation of the network, as well as server and client configurations. This paper begins with a review of TCP/IP and its benefits and shortcomings, and then introduces two key technologies: Dynamic Host Configuration Protocol (DHCP) and Windows Internet Naming Service (WINS).

TCP/IP Review

The Transmission Control Protocol and Internet Protocol (TCP/IP) is a wide-area network (WAN) protocol that provides the following features:

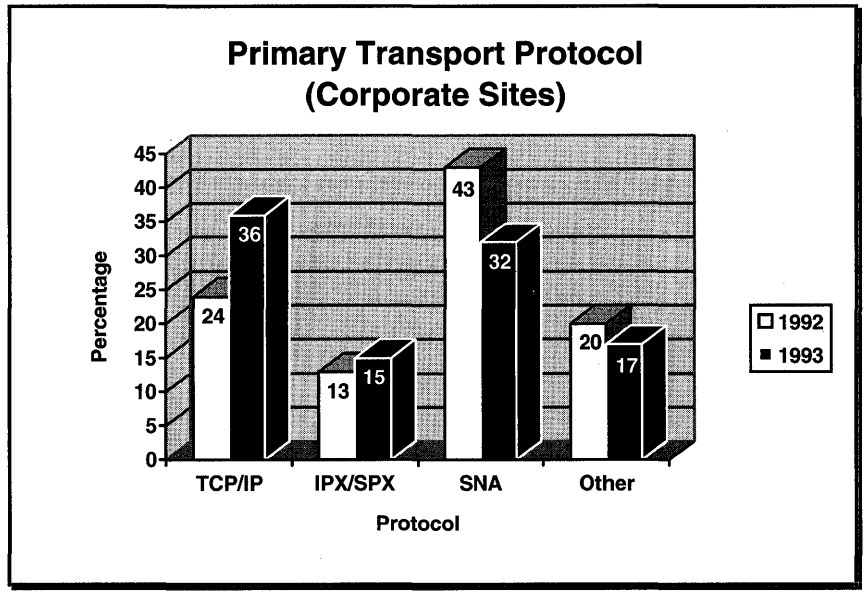
- Routable networking
- Network technology independence
- Scalable architecture
- Reliable delivery
- Universal interconnectivity
- Proven technology

Beyond the basic design features of TCP/IP, a network protocol must have broad-based support by both users and networking vendors. TCP/IP is the default protocol for the UNIX® environment, so it has gained wide acceptance among the UNIX community. Research on corporate bandwidth usage indicates that TCP/IP usage is on the rise, while IPX/SPX usage is declining slightly.



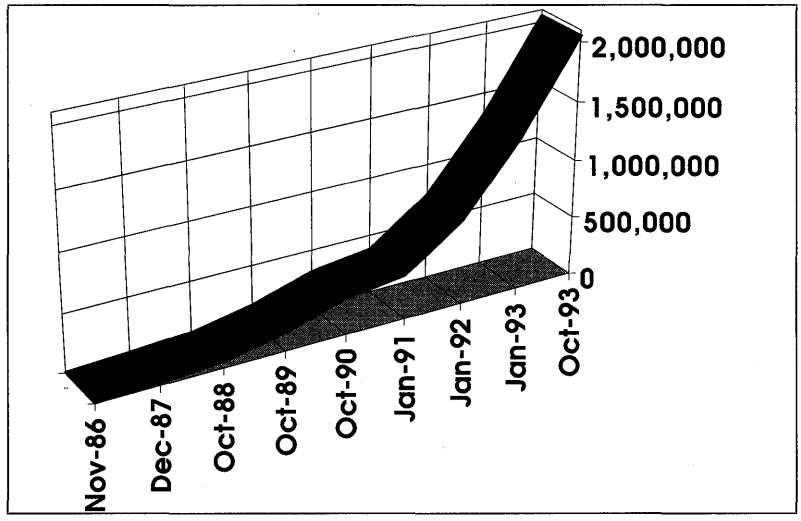
Corporate bandwidth usage, *Network World*, Dec. 2, 1993

TCP/IP plays a critical role in today's enterprise networking environment. As a primary transport, TCP/IP is the clear choice over IPX/SPX, and it is anticipated to become the primary transport protocol for corporate sites in 1994.



Primary transport protocol, *Datamation*, June 1, 1993

Perhaps the most significant indication of the widespread acceptance of TCP/IP is the rapid growth of the Internet. Based on the TCP/IP protocol, the Internet has exploded to over 2,000,000 nodes and 16,000 networks!



Number of total nodes on the Internet by year. Source: SRI International

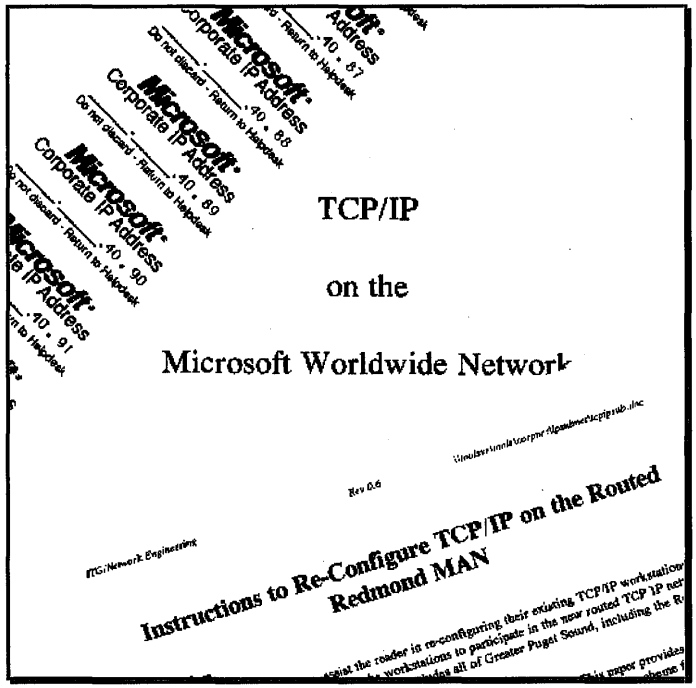
TCP/IP Shortcomings

Despite all the success of TCP/IP, however, it does have its shortcomings. There is a price to pay to address all the nodes that can participate in this large, scalable network.

TCP/IP Computer Configuration

Each computer running TCP/IP must have specific information to identify uniquely itself, the network that it is a member of, and the location for packets not bound for computers on the local network. This information is referred to as the TCP/IP address, subnet mask, and default gateway, respectively. Each of these addresses consists of a 32-bit number, typically represented in dotted decimal format. For example, in a typical TCP/IP configuration, the TCP/IP address might be 101.200.42.101, the subnet mask 255.255.0.0, and the default gateway 101.200.42.1.

Such requirements can create serious administrative headaches in a large corporate environment. For example, a department orders a new computer and it comes pre-installed with all the necessary software and hardware to connect to the corporate network. However, the computer cannot be attached to the network, nor can it access any TCP/IP-based networking resources, until the network administrator supplies the necessary client information. Furthermore, either a person from the "helpdesk" has to go to the computer physically and enter the appropriate information, or the user has to dig through documentation (written by MIS) on how to do it. The crucial factor here is whether the user can correctly enter the necessary client information instead of having a technician enter the information at a high hourly rate.

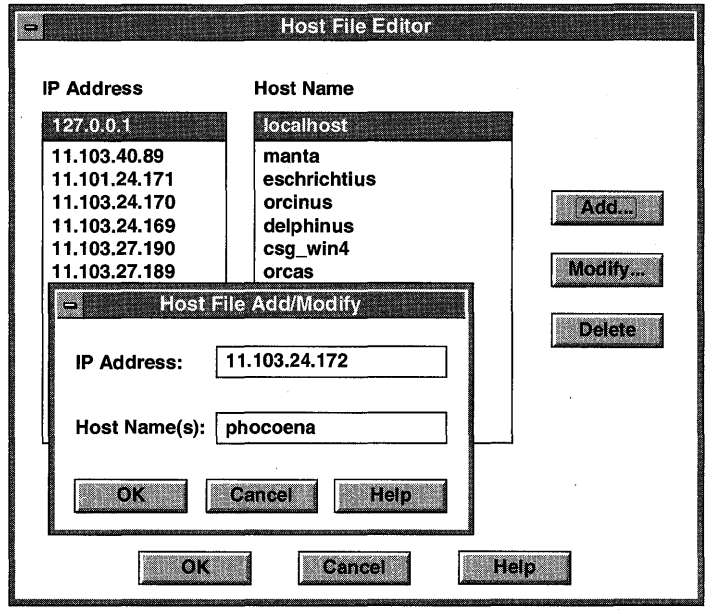


Before DHCP/WINS: TCP/IP documentation and IP address tags

Typical problems that occur in these environments are misconfigured computers, which cannot access the network due to incorrect addresses, and duplicate TCP/IP addresses. Duplicate addresses can occur when one user "assists" another by providing him or her with a configuration that "works," or when a computer is cloned and put on the network. Unfortunately, these types of problems are very difficult to detect, and require a resource-intensive analysis of network traffic to locate the computer with the duplicate TCP/IP address.

Accessing Network Resources

Consider the average user attempting to access information provided by a network resource. Typically, the user knows the name of the computer, such as ENGR_AIX, but not the computer's IP address. If the user is running an MS-DOS–based computer with NFS client support or FTP'ing to the computer, the user will reference the computer by name, e.g., (ENGR_AI), and the system will access a *host table* containing a mapping between the computer name and the IP address.



Host table information for an NFS client

The difficulty of the host table lies in its administration: who loads and maintains the information in these host tables? For typical NFS clients, the host table information resides on local computers, which means that either the *users* have to know enough about host files and TCP/IP addresses to update this information on their own, or someone from *MIS* has to maintain the information on a server, and have the updated file downloaded periodically.

Some corporate environments implement the Domain Name System (DNS), that is, server-based host table information, so that the user needs only to specify the address of the DNS server. However, this does not alleviate the matter of updating the information; it simply pushes the responsibility to the MIS department. Although DNS is server-based, it is not dynamic, so it must be manually updated whenever a computer name or IP address is changed.

Maintenance of TCP/IP Networks

The expense of administering a network is often considered a "fixed cost." To keep expenses down, companies must manage internal reorganization quickly and efficiently, minimizing the amount of time required by both the technician and the user who is waiting for his or her system to become part of the corporate network.

For example, with the typical naming structure, the DNS implementation of network addresses requires that each time a computer is renamed or physically moved to a new location, it must be reconfigured with both the new TCP/IP network address (to reflect its new subnet) and the DNS tables must be updated (to reflect the new client configurations).

Even a simple configuration change, such as a computer name, requires that the DNS tables be updated to locate the new computer on the network.

TCP/IP Limitations

- TCP/IP configuration information is complex and difficult to configure.
- Misconfiguration of TCP/IP addresses leaves a computer unable to communicate to TCP/IP resources, which can adversely affect other computers on the network.
- Network administrator must configure host tables manually.
- Changing a computer's name or moving the computer to another subnet requires updating the host tables.
- There is a need to make TCP/IP administration easier and more flexible for both the user and the network administrator.

Windows NT Advantages

- TCP/IP configuration information is issued automatically.
- Host table information is maintained dynamically in the WINS database.
- Users simply check a box to implement DHCP/WINS.

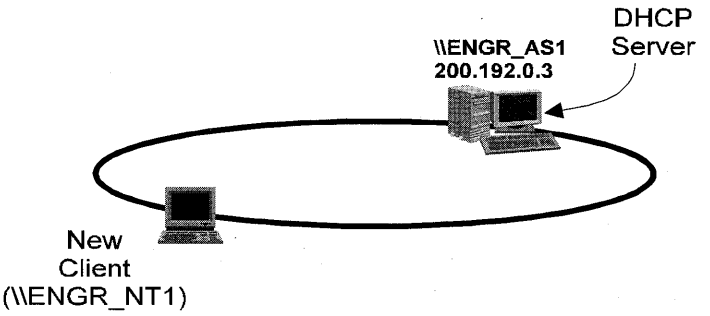
Dynamic Host Configuration Protocol (DHCP)

To address the problem of dynamic addressing in a TCP/IP environment, Microsoft looked at the available technologies, focusing on dynamic and open solutions to this problem. As a founding member of the Internet Society, Microsoft worked with the Internet Engineering Task Force (IETF) and other vendors to propose an open standard which would address the dynamic addressing problems of TCP/IP-based networks. As a result of this effort, standards were proposed, as documented in the Internet Request For Comments (RFCs) #1533, #1534, #1541, and #1542. These proposed standards document the basis for the work being done at Microsoft to provide scalable, dynamic TCP/IP addressing solutions in future versions of Microsoft systems products, both at the server and at the client level.

The goal of the TCP/IP projects at Microsoft is to provide 32-bit performance, the ease of configuration with TCP/IP that users have today with NetBEUI or AppleTalk®, and the ease of administration that can be provided with a dynamic and scalable TCP/IP addressing capability. Also, no workstation configuration is necessary, and users do not have to know anything about the computer's TCP/IP address.

An Example of How DHCP Works

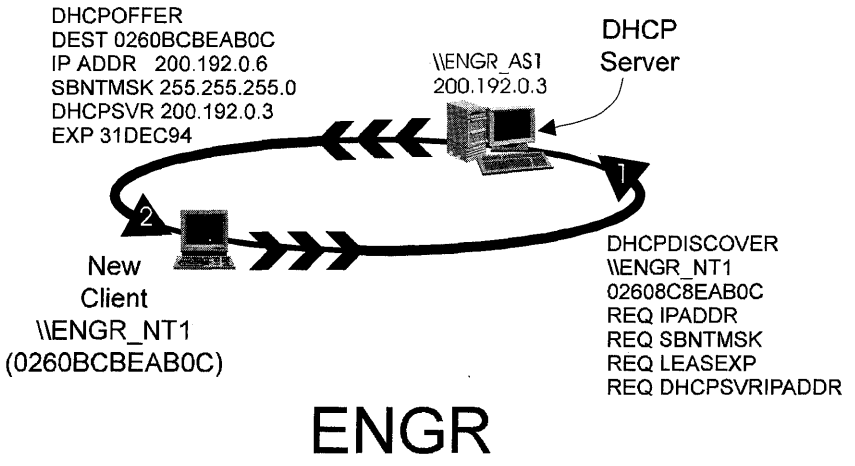
To explore how DHCP works we will consider "Exotic Excursions," a fictitious company with three Class C Internet addresses (200.192.0.x, 200.192.100.x, and 200.192.127.x). The following figure shows a simple network with one network server, and a single network client being added to the network.



DHCP server and new client

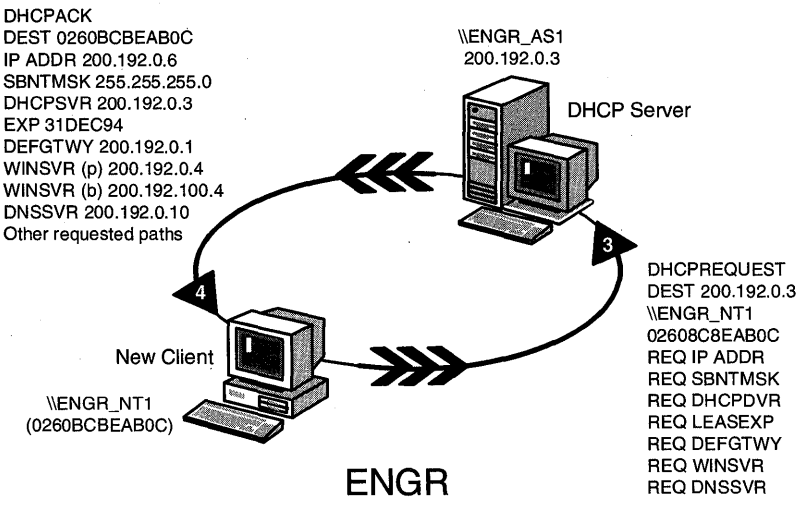
The Engineering department has a Windows NT Server Domain "ENGR" and a Windows NT Server–based computer, \\ENGR_AS1, with IP address of 200.192.0.2. The new client is a Windows NT–based computer with DHCP client support.

The Windows NT–based client computer starts Windows NT and issues a **DHCPDISCOVER** message (containing the MAC address and the computer name), which is picked up by the DHCP server. The DHCP server looks at the most recent table of available addresses, and, finding no references to that computer, offers an available address to the computer.



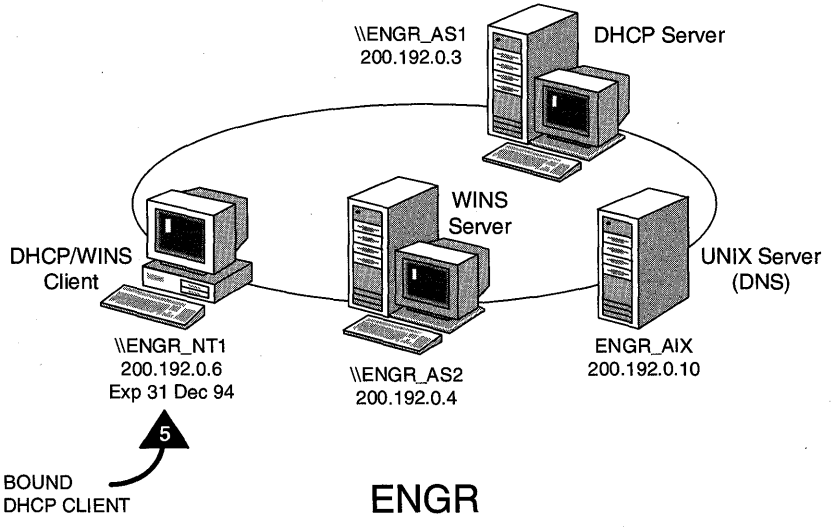
DHCP DISCOVER, DHCP OFFER messages

Any DHCP server receiving the request (even across a BOOTP-relay router) and having a valid configuration setting for the requesting computer can then check to see whether it has an address available. If there is an available address, the DCHP server will offer a **DHCPOFFER** response with the necessary configuration information and additional parameters, including the destination computer's network card address, the offered IP address, the appropriate subnet mask, the IP address of the offering DHCP server, the IP lease expiration date, and any other pertinent information specified in the additional parameters section of the original DHCPDISCOVER request.



DHCP REQUEST, DHCP ACK messages

The DHCP client collects the offers presented by the responding DCHP servers and selects the most appropriate configuration. The DHCP client then issues a **DHCPREQUEST** to the DHCP server accepting the offered address, and can request additional information (depending on the client's needs), including the default gateway, the WINS-based server IP address, and the DNS server IP address. The DHCP server responds with a **DHCPACK** message, assigning the IP lease and providing the requested information.



BOUND DHCP client

When the DHCP client receives the DHCPACK (acknowledge), the DHCP client completes the initialization process of the TCP/IP stack, becoming a *bound* DHCP client, and is able to use the leased IP address until the lease requires renewal.

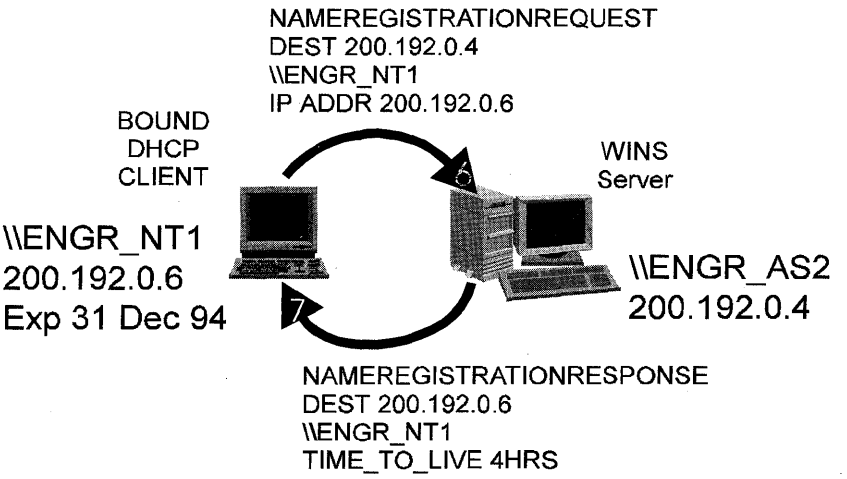
Now that the client computer has a valid IP address, let's turn to the process of registering the computer name on the network. In previous implementations of registering the network IP address and the computer name, the network administrator had to manually update the host's tables. Using the Windows Internet Naming Service (WINS), this process is handled at the system level by Windows NT Server.

Windows Internet Naming Service (WINS)

WINS is designed to address the problem of locating network resources in a TCP/IP-based Microsoft network by automatically configuring and maintaining the computer name and IP-address mapping tables, while serving basic functions such as preventing duplicate network names. WINS is a complementary service to DHCP and has a complete, centralized tool for administration and configuration of the WINS servers, static name tables, and replication information.

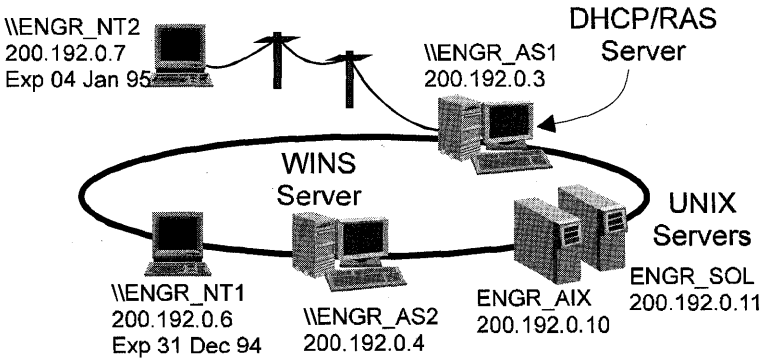
WINS Configuration

After the DHCP client is configured and bound, the client proceeds to register its name with the designated WINS server. The client issues a NAMEREGISTRATIONREQUEST message to the WINS-based server (a directed send) with the DHCP client's computer name and leased IP address.



Name registration with WINS server

The WINS-based server checks to see whether the requesting computer name is unique on the network, and responds with a positive or negative WINS name registration response message. If positive, the registration response will include the Time To Live (TTL) for the name registration. If negative, a duplicate name has been identified on the network (following an accepted challenge to the current owner), the name registration to the new DCHP client is declined, and the user is advised of the name conflict. We will discuss the renewal process for the IP address and the TTL for the name registration later. First, we want to expand our view of the Exotic Excursions computing environment, which now includes some additional hardware.



Expanded view of Exotic Excursions computing environment

Notice the changes from the initial configuration. The DNS server address that was passed back to the DHCP client is actually a UNIX server (ENGR_AIX) on the network. The Windows NT Server–based DCHP server is also a Remote Access Server with a dial-up (Point to Point) TCP/IP-based DHCP client (\\ENGR_NT2) that uses the same DHCP server as our newly bound DHCP client.

DHCP and WINS Renewal Process

DHCP and WINS are designed to be dynamic and scalable in their implementations, addressing the needs of highly dynamic and mobile corporations while providing centralized configuration and administration of TCP/IP-based Microsoft networks. To meet these requirements, the configuration confirmation for the clients is time-limited (with some exceptions), which means that the clients typically must update their information to the DHCP and WINS-based servers.

DHCP Renewals

DHCP clients receive an IP address with a lease period. When that lease period expires, the clients can no longer use the given IP address. The goal for the client is to negotiate the lease renewal periodically with their DHCP servers while enough time remains in the lease so that the lease does not expire in the process. By default (although the network administrator can change the defaults), the client will begin the renewal process when 50% of the lease time has expired. It will send a directed message to the DHCP server requesting a lease renewal. If allowed, the DCHP server will automatically renew the lease.

However, if the DHCP server no longer exists or the IP address of the DHCP server has changed, the client will broadcast a DHCPREQUEST when 87.5% of the lease has elapsed to look for *any* DHCP server. If no DHCP server can be located, the lease could expire, in which case the client discontinues the use of the IP address and begins the initialization process with a DHCPDISCOVER message.

DHCP Server Can Force Reinitialization

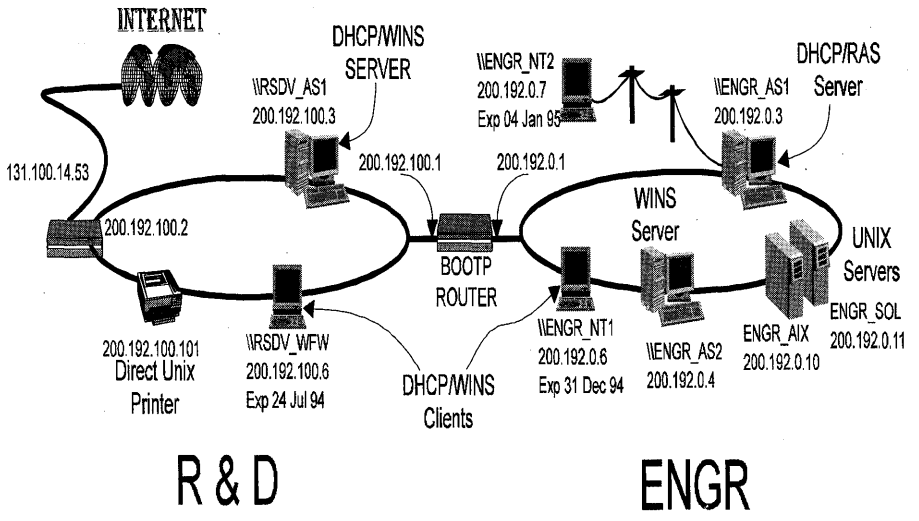
When a DHCP client contacts a DHCP server, the server might determine that the client is misconfigured (the computer has moved to a different subnet) or that the server can no longer honor the client's IP address. The DHCP server can issue a DHCPNAK (negative acknowledgment), forcing the DHCP client to reinitialize itself and request a new IP address. This can occur when the client computer has been moved between docking stations, and thus might be located on a different subnet. It will need a new IP address to successfully access the network resources wanted.

WINS Renewal

The renewal process for a WINS-based client is less obvious, as the NetBIOS over TCP/IP support (NBT) automatically registers the computer name with the WINS-based server when an NBT client process is started. Therefore, in many cases the renewal process is automatic, and the WINS-based server automatically reissues a new TTL with each NBT registration. With each new TTL, a timer is reset in the system to issue a NBT name registration with the WINS-based server, should the computer be in a state of inactivity and the timer expire.

The Big Picture

Now let's look at the Exotic Excursions environment with routers and multiple subnets.



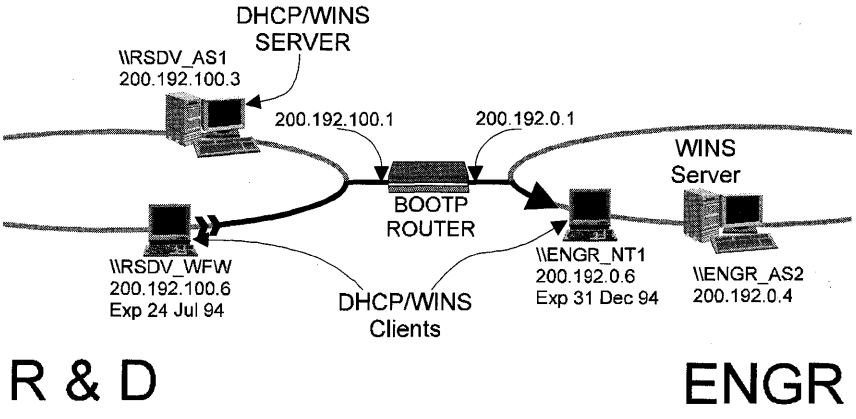
Network with routers and multiple subnets

Notice that there are a number of changes in the environment. There are two routers, two DHCP servers, and two WINS-based servers (one \\RSDV_AS1 is both a DHCP and a WINS-based server). Later, we will review the capabilities of the DHCP and WINS administrative tools, and reflect on how the tools and capabilities address the needs of a larger, more heterogeneous corporate environment.

Locating a Resource

What happens when a computer in the R&D domain wants to locate a resource in the ENGR domain? For the purpose of this example, \\RSDV_WFW wants to find the resources available on \\ENGR_NT1. To locate the computer's IP address, \\RSDV_WFW sends a NAMEQUERYREQUEST to its primary WINS server, \\RSDV_AS1, which it knows to be at 200.192.100.3. It requests that the server look in the database to find the entry for \\ENGR_NT1 and respond with the IP address of the computer wanted. The WINS-based server responds with a NAMEQUERYRESPONSE to \\RSDV_WFW with the computer's IP address, at which time the entry is cached at the requesting client computer.

Now that \\RSDV_WFW has the necessary IP address, it establishes a TCP connection, followed by a session message (request) to \\ENGR_NT1 (at 200.192.0.6), and the resource connection is established.



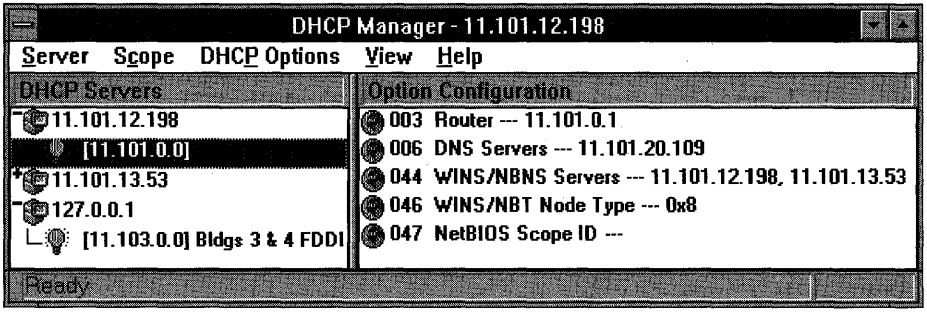
TCP connection

The Administrative Tools for DHCP and WINS

DHCP Administration

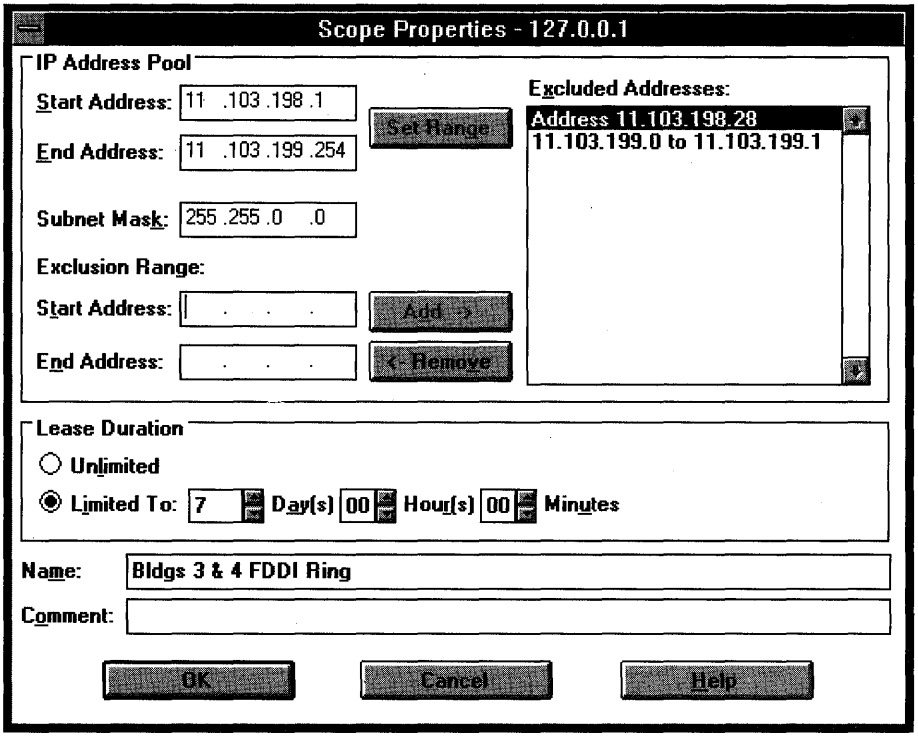
The DHCP administration tool is designed to organize the configuration of the network resources into logical groupings of computers on the same physical wire, the same as an Internet subnet or an equivalent network node on a private network. The administration tool allows the network administrator to define global and scope-specific configuration settings to identify routers.

In the example below, there are three scopes defined: 11.101.12.198, 11.101.13.53, and 127.0.0.1, which is the local computer. Focusing on the 11.101.0.0 scope, you can see the global default information.



Dynamic Host Configuration Protocol admin tool

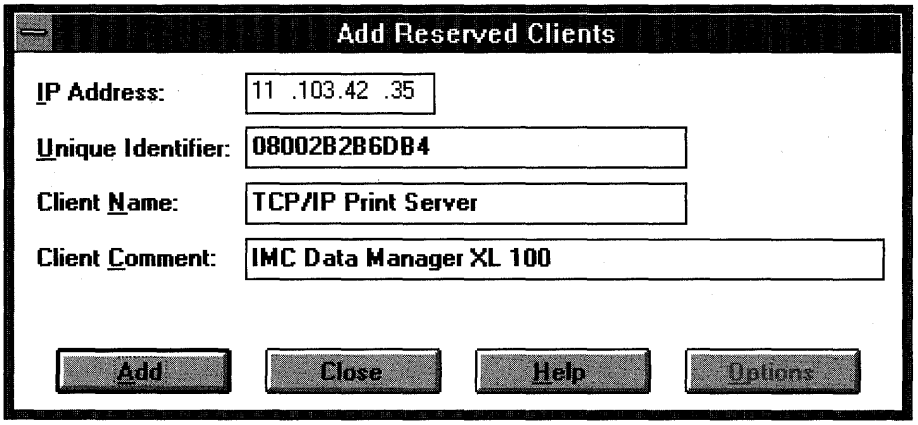
Each scope is defined by specific properties which are established by the DHCP administrator. The administrator defines the subnet ID, the subnet mask, and the primary DHCP server. The administrator also defines the pool of available IP addresses in that specific scope and any exclusion ranges to avoid, thereby allowing legacy systems to retain their established IP addresses.



DHCP Administrator Scope Properties dialog box

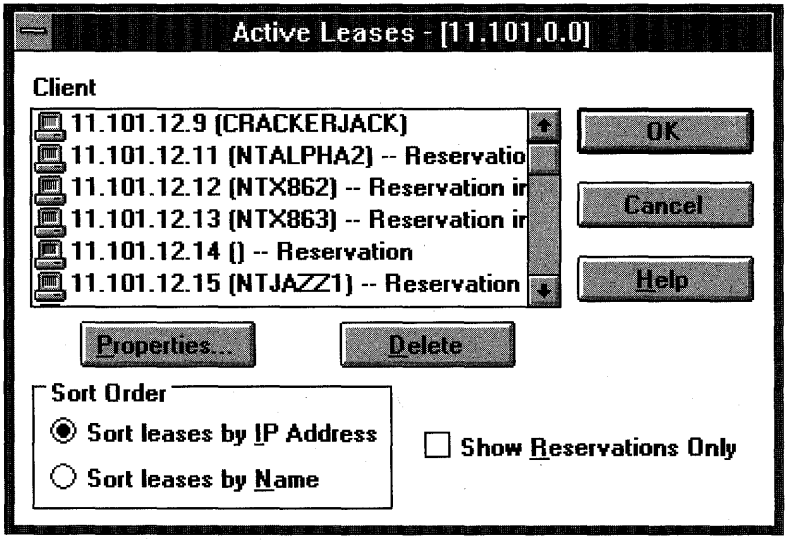
Each scope definition receives a name so that it can be easily identified by any network administrator, along with additional comments or questions.

In some cases, computers outside the Microsoft network can access computers that participate in the DHCP/WINS environment but do not have an easy way to inquire for the IP address of the server. Instead of forcing the user of the legacy computer to be manually updated with the dynamic address of the DHCP client, the DHCP administrator can elect to specify a *reserved client*. A reserved client is issued an infinite lease of the IP address; thus any legacy computer attempting to locate the DHCP client will be able to access the computer consistently via the now static IP address.



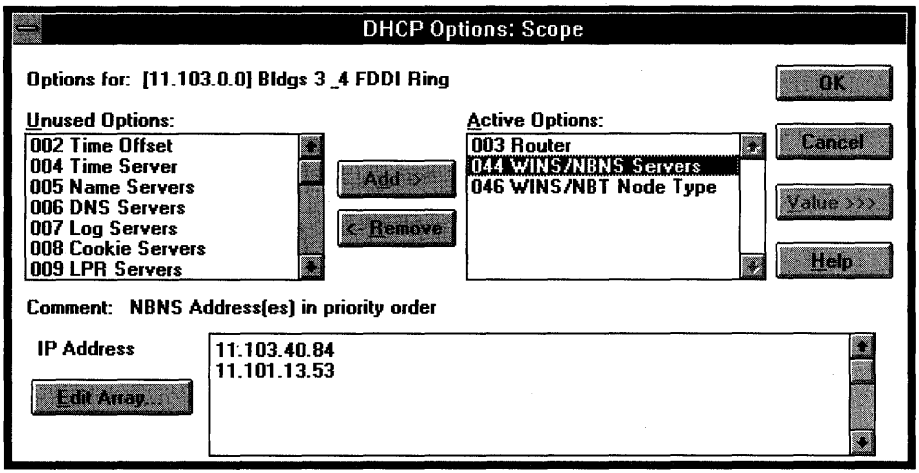
DHCP Administrator Add Reserved Clients dialog box

Another option with the DHCP Administrator tool is the ability to review the client lease information on a per-scope basis, allowing the administrator to review the outstanding leases and associate them with the client names and their MAC-layer addresses.



DCHP Administrator client lease review dialog box

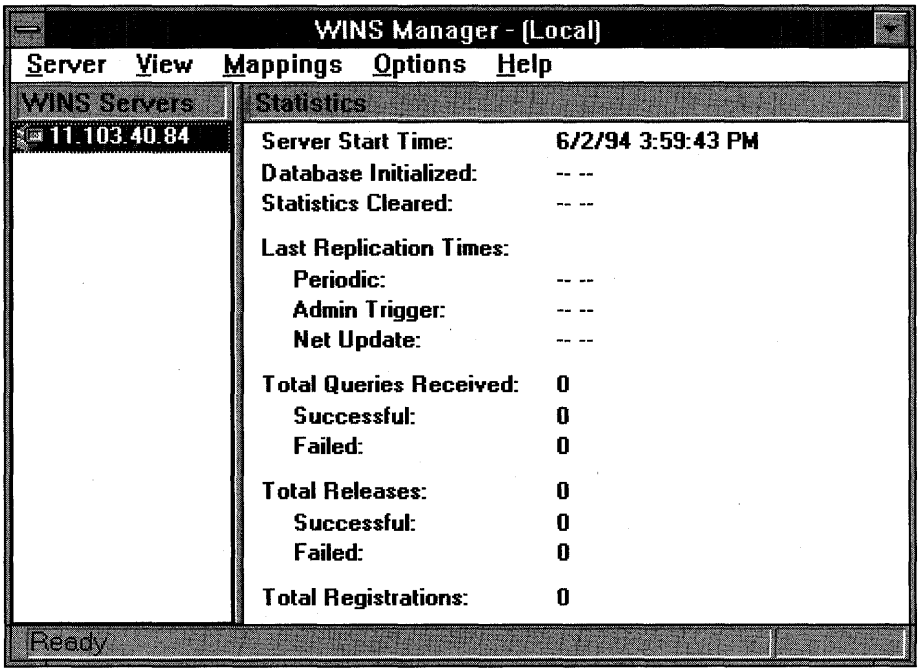
For each scope-member, options can be configured for the scope to provide additional configuration information to the scope members. The scope options contain an array of parameters that the DHCP administrator can configure. Notice that this same information can be set globally as well, by means of a similar Global Option Settings dialog box.



DHCP Scope Options dialog box

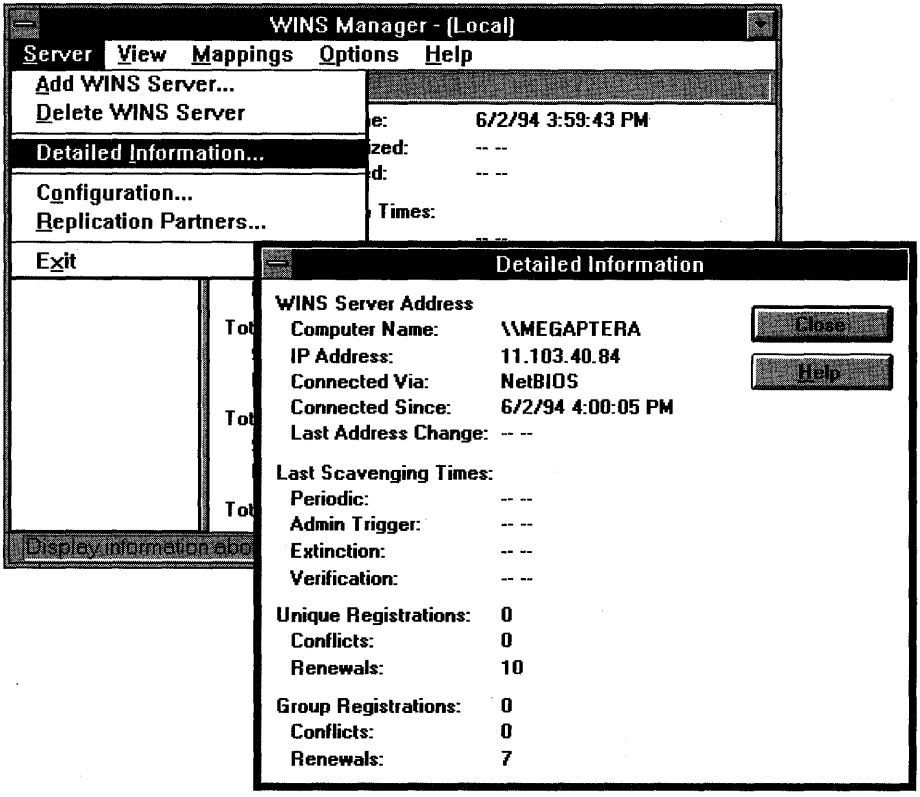
WINS Administration

The WINS administration tool is designed to help the network administrator configure the WINS-based servers and monitor activity. Notice that the information presented is very detailed in nature. Key pieces of information are the number of name queries received by the WINS-based server, and the number of successful and less-than-successful responses. In the example below, the Windows NT development team is running WINS-based clients, but when they perform a name query for computers outside the development team, the WINS-based server cannot locate the computer, resulting in a Query Failure. At the time this screen shot was taken, only about 1% of the total computers on the Microsoft network were WINS-based clients, hence the high number of failures.



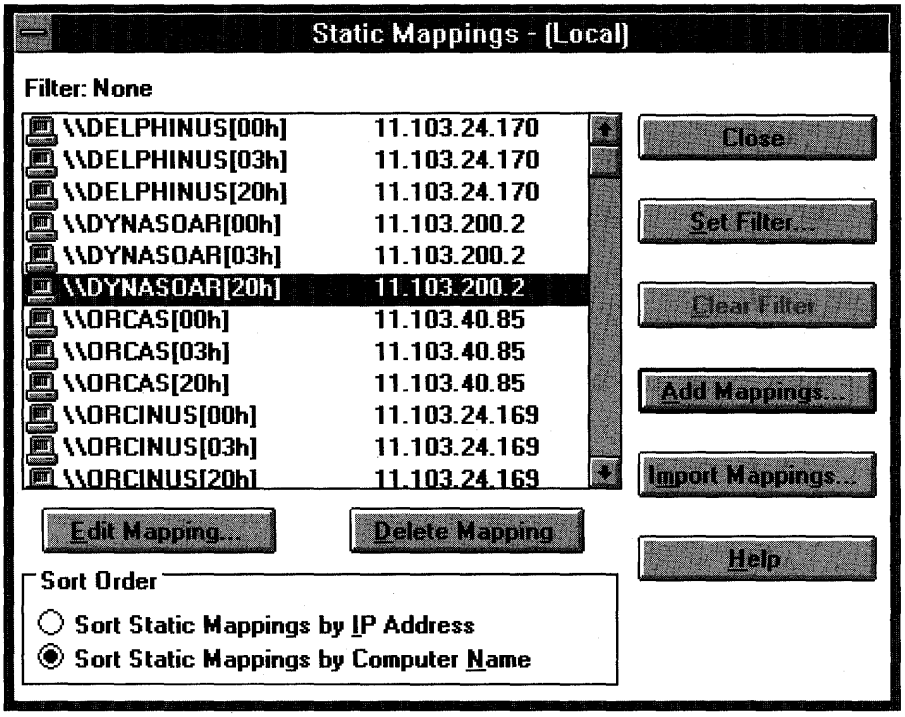
WINS Administrator tool

The WINS Administrator tool allows the configuration of various parameters for the WINS-based server, including which WINS-based server to focus on, the static mappings for the server, the replication information, and the database in use.



WINS Administration options

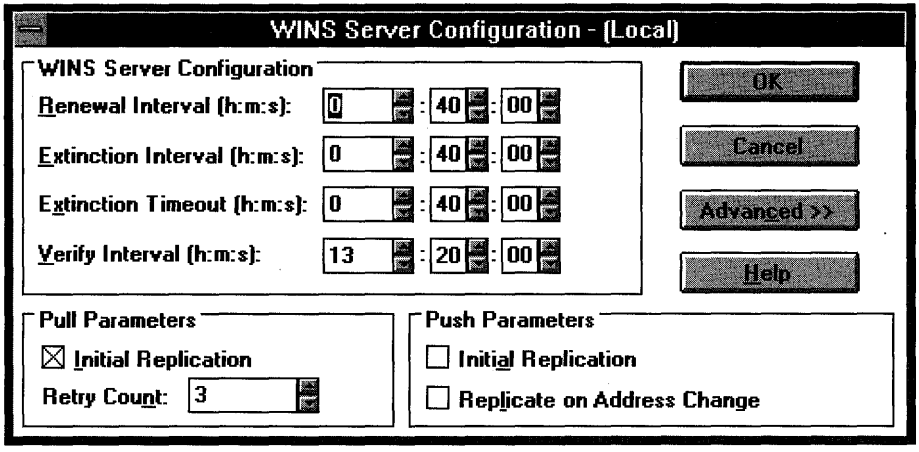
The Static Mapping options allows the network administrator to configure WINS mapping information manually for non-WINS clients, similar to the old host table information.



Static Mappings (Local) dialog box

This static mapping information can be entered individually for each computer, or it can be array-loaded from a file containing the necessary mappings. The latter minimizes the amount of work required to create an interoperative environment by importing the DNS host tables from the UNIX DNS server.

WINS-based servers specify the name registration TTL by specifying an Extinction Interval, which is defined by the administrator. Should an NBT client's reregistration not be received before the extinction time, the name will no longer be registered with the WINS server. Also, the replication process can be configured in this dialog, which will be discussed later.

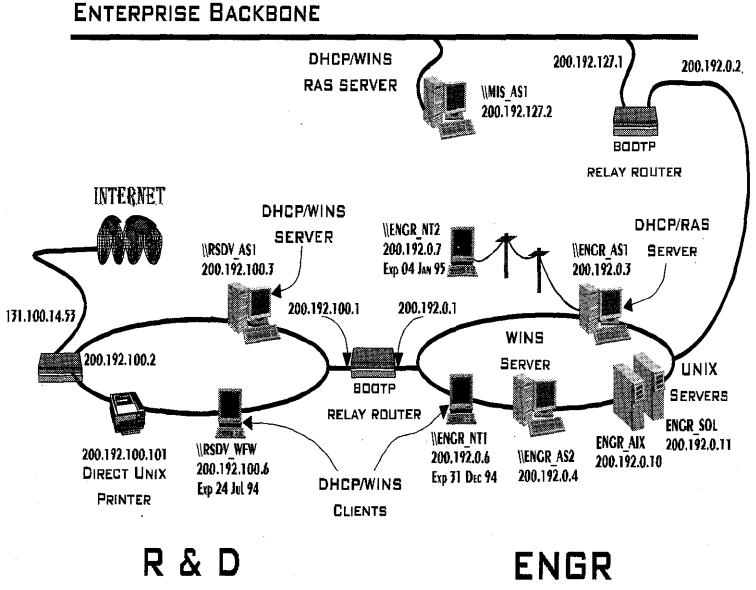


WINS Server Configuration dialog box

Error Handling with DHCP/WINS

Now let's take a look at how DHCP and WINS handle error conditions when the primary DHCP or WINS server is down.

The following configuration shows the expansion of the Exotic Excursions network to include the scope settings and the enterprise. Notice that the range of IP addresses has been split for both the ENGR and R&D scopes.



Exotic Excursions Enterprise Backbone

In the table below, the IP address ranges have been configured given an address range for the fourth octet of 1–254 for each scope (which is typical for a Class C address).

Type of Range	IP Address[1]	Lease Period
Fixed address: routers, DHCP, WINS servers	1–5	n/a
Primary DHCP server scope	6–120	2 weeks
Backup DHCP server scope	121–235	1 week
MIS tertiary DHCP server scope	236–245	1 day
Reserved for future use	245–254	n/a

For example, the DCHP Server \\ENGR_AS1 (the *primary* DHCP server for the ENGR scope) has available addresses 200.192.0.**6** through 200.192.0.**120** for DHCP clients in the ENGR scope. The backup DHCP server \\RSDV_AS1 has available addresses 200.192.0.**121** through 200.192.0.**235**. Therefore, if one DCHP server fails, either controller can support at least 115 DHCP clients in the ENGR scope.

DHCP Server //RSDV_AS1	DHCP Server //ENG_AS1	DHCP Server //MIS_AS1
R&D Scope	**R&D Scope**	**R&D Scope**
Primary WINS Server	Primary WINS Server	Primary WINS Server
200.192.100.3	200.192.100.3	200.192.100.3
Backup WINS Server	Backup WINS Server	Backup WINS Server
200.192.0.4	200.192.0.4	200.192.0.4
IP Address Pool	IP Address Pool	IP Address Pool
Start: 200.192.100.6	Start: 200.192.100.121	Start: 200.192.100.236
End: 200.192.100.120	End: 200.192.100.235	End: 200.192.100.245
Exclusion Range		
Start: 200.192.100.101		
End: 200.192.100.101		
R&D Scope	**R&D Scope**	**R&D Scope**
Primary WINS Server	Primary WINS Server	Primary WINS Server
200.192.0.4	200.192.0.4	200.192.0.4
Backup WINS Server	Backup WINS Server	Backup WINS Server
200.192.100.3	200.192.100.3	200.192.100.3
IP Address Pool	IP Address Pool	IP Address Pool

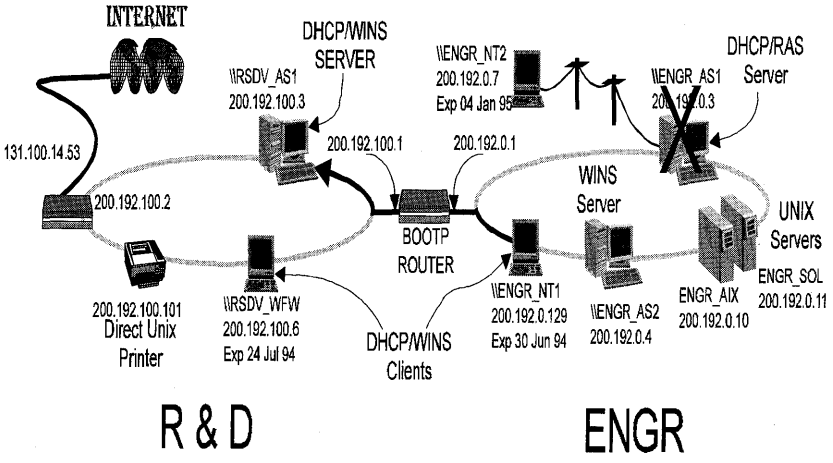
[1] IP address of the (200.192.x.y, where x ∈ {0,100,127})

Start: 200.192.0.121	Start: 200.192.0.6	Start: 200.192.0.236
End: 200.192.0.235	End: 200.192.10.120	End: 200.192.0.245

In many cases, however, both servers will regularly be online, and one computer might be offline only for a short time (for example, one day). Depending on the length of the lease period (for example, 3 months), only a few computers would need renewal during the period that the computer was offline. Therefore, you could have a smaller lease pool configured on the backup DHCP server than on the primary server, effectively providing better utilization of the available IP address space.

DHCP Server Is Offline

What if we are powering up \\ENGR_NT1, and our primary DHCP server (\\ENGR_AS1) is offline? If we remember that the DHCPREQUEST message can be relayed by BOOTP Relay routers, then the request is relayed across the router at 200.192.0.1 to \\RSDV_AS, which will respond, but with a different IP address. The scope for that subnet is different, so instead of \\ENGR_NT1 having the IP address of 200.192.0.6 that was provided by the R&D scope from the DHCP server \\ENGR_AS1, it now has the IP address 200.192.0.129, provided by the DHCP server \\RSDV_AS1.



Primary DHCP server offline

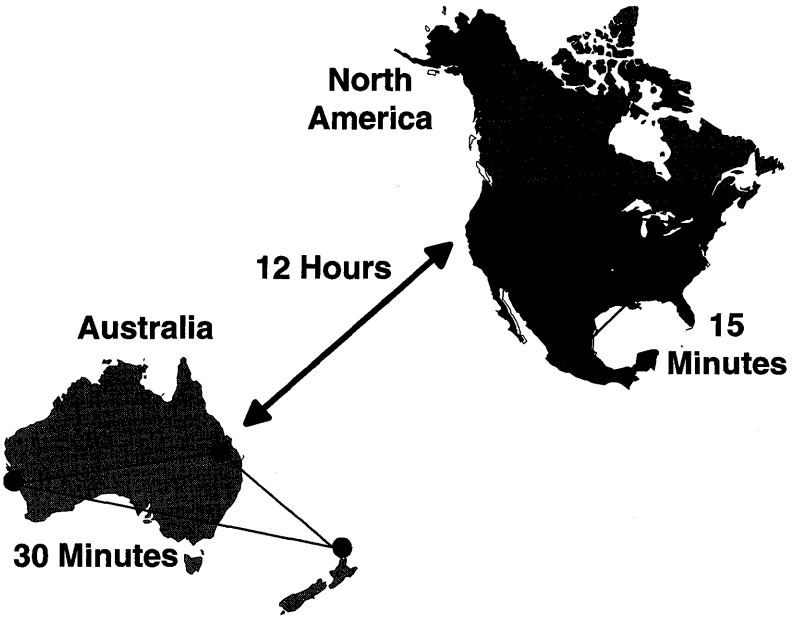
WINS Server Is Offline

If a WINS-based server is offline or otherwise unavailable, the DHCP client will contact the backup WINS-based server via the IP address that was returned during the DHCP REQUEST, DHCPACK process. WINS-based servers replicate their databases to the other known WINS-based servers on the network with the time interval specified by the network administrator.

WINS Server Replication

WINS-based servers maintain current databases via replication partners. Each WINS-based server is a push partner or pull partner with at least one other WINS-based server. A *pull partner* is a WINS-based server that pulls in database replicates. A *push partner* is a WINS-based server that sends replicas to its pull partner upon receiving a request. When the server's pull partner replicates the information, it pulls replicates by asking for all records with a higher version number than the last record stored from the last replication for that server. All mapping changes converge within the replication period for the entire WINS system.

Replication is triggered when a WINS-based server polls another server to get a replica based on an interval or time set by the administrator. Replication is also triggered when a WINS-based server reaches a threshold set by the administrator, which is a specified time or an update count for registrations and changes. In this case, the server notifies other servers that it has reached its threshold, and the other servers pull replicates. Replication pairs also have the advantage of specifying replication interval, so if servers are connected via slow links—such as international connections—you can specify specific replication intervals.



Replication of WINS-based server in U.S. and Australia

Therefore, in the above example, we would replicate WINS-based server data in the US every fifteen minutes, and in Australia every 30 minutes, but only every 12 hours between the US and Australia.

Summary

TCP/IP is a widely accepted, routeable WAN protocol that is unparalleled in its deployment worldwide as a de facto standard for wide-area networking. However, it has historically had high costs associated with the configuration and administration of network clients. Microsoft, as a member of the Internet Engineering Task Force (IETF), has been working with other IETF members to deploy dynamic IP addressing technology. The result is the Dynamic Host Configuration Protocol (DHCP), an open standard for TCP/IP-based networks.

Microsoft has also developed the Windows Internet Naming Service (WINS) which allows dynamic host table mapping from a computer's IP address to its respective NetBIOS name, thus eliminating the need to maintain the host tables in a network manually.

Microsoft networking, using DHCP and WINS functionality, provides easy administration on TCP/IP-based networks for computers running Windows for Workgroups 3.11 (and the future release, Windows 95), Windows NT Workstation, and Windows NT Server.

Glossary

A

account
See user account.

account policy
Controls the way passwords must be used by all user accounts in a domain, or in an individual computer.

acknowledgment
The process used to guarantee reliable end-to-end message delivery.

administrative alerts
Relate to server and resource use; warn about problems in areas such as security and access, user sessions, server shutdown because of power loss (when UPS is available), directory replication, and printing. When a computer generates an administrative alert, a message is sent to a predefined list of users and computers. *See also* Alerter service.

Alerter service
Notifies selected users and computers of administrative alerts that occur on a computer. Used by the Server and other services. Requires the Messenger service. *See also* administrative alerts.

American National Standards Institute (ANSI)
An organization dedicated to the development of trade and communications standards.

Application layer
The top (seventh) layer of the OSI model. This layer serves as the window for application processes to access network services. It represents the services that directly support user applications, such as software for file transfers, for database access, and for electronic mail.

ARC
Advanced RISC Computing. A standard developed by a consortium of hardware and software manufacturers. This standard specifies a computer that is similar to a PC but is based on a RISC processor.

archive bit
Used by backup programs to mark files after backing them up, using the normal or incremental backup types.

ArcNet®
A baseband, token-passing media-access network protocol created by the Datapoint Corporation. ArcNet runs on coaxial cable, twisted-pair cable, and fiber-optic cable and supports up to 255 nodes.

ASCII file
See text file.

associate
To identify a filename extension as "belonging" to a certain application so that when you open any file with that extension, the application starts automatically.

audit policy
For a domain or for an individual computer, defines the type of security events that are logged; determines what Windows NT will do when the security log becomes full.

auditing
Tracking activities of users by recording selected types of events in the security log of a server or a workstation.

authentication
Validation of a user's logon information. When a user logs on to an account on a Windows NT workstation, the authentication is performed by that workstation. When a user logs on to an account on a Windows NT Server domain, that authentication can be performed by any server in that domain. *See also* server, trust relationship.

B

backbone
The backbone, or trunk segment, is the main cable from which drop cables are connected to stations, repeaters, and bridges.

back end
In a client-server application, the part of the program that is executing on the server.

base I/O port
Specifies a channel through which information is transferred between your computer's hardware (such as your network card) and its CPU.

base memory address
Defines the address of the location in your computer's memory (RAM) that is used by the network adapter card. This setting is sometimes called the RAM start address.

backup domain controller
For Windows NT Server domains, refers to a computer that receives a copy of the domain's security policy and domain database, and authenticates network logons. *See also* primary domain controller.

batch program
An ASCII file (unformatted text file) that contains one or more Windows NT commands. A batch program's filename has a .BAT or .CMD extension. When you type the filename at the command prompt, the commands are processed sequentially.

bind
To associate two pieces of information with one another.

bit
Short for binary digit: either 1 or 0 in the binary number system. In processing and storage, a bit is the smallest unit of information handled by a computer. It is represented physically by an element such as a single pulse sent through a circuit or small spot on a magnetic disk capable of storing either a 1 or 0.

bit time
The time it takes each station to receive and store a bit.

BNC (British Naval Connector)
A connector for coaxial cable that locks when one connector is inserted into another and is routed 90 degrees.

boot loader
Defines the information needed for system startup, such as the location of the operating system's files. Windows NT automatically creates the correct configuration and checks this information whenever you start your system.

boot partition
The volume, formatted for an NTFS, FAT, or HPFS 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.

branch
A segment of the directory tree, representing a directory and any subdirectories it contains.

bridge
A device that allows you to join two local area networks, and allows stations on either network to access resources on the other. The bridge makes connections at the Data Link layer of the OSI model.

broadband
A system used to transmit the encoded signals over cable. A broadband system uses analog signaling and a range of frequencies. With analog transmission, the signals employed are continuous and nondiscrete. Signals flow across the physical medium in the form of electromagnetic or optical waves.

browse
To look through lists of directories, files, user accounts, groups, domains, or computers.

buffer
A temporary storage place for information.

built-in groups
The default groups provided with Windows NT and Windows NT Server. Built-in groups have been granted useful collections of rights and built-in abilities.

In most cases, a built-in group provides all the capabilities needed by a particular user. For example, if a domain user account belongs to the built-in Administrators group, logging on with that account gives a user administrative capabilities over the domain and the servers in the domain. To give a needed set of capabilities to a user account, assign it to the appropriate built-in group. *See also* group, User Manager, User Manager for Domains.

C

central file server
A network in which specific computers take on the role of a server with other computers on the network sharing the resources. *See also* Client-server.

check box
A small, square box in a dialog box that can be selected or cleared, representing an option that you can turn on or off. When a check box is selected, an X appears in the box.

choose
To pick an item that begins an action in Windows NT. You often choose a command on a menu to perform a task, and you choose an icon to start an application.

client
A computer that accesses shared network resources provided by another computer (called a server). *See also* client application, server, workstation.

client-server
A network in which specific computers take on the role of a server, with other computers on the network sharing the resources. *See also* central file server.

Clipboard
A temporary storage area in memory, used to transfer information. You can cut or copy information onto the Clipboard and then paste it into another document or application, or into the ClipBook. *See also* ClipBook.

ClipBook
Permanent storage of information you want to save and share with others. This differs from the Clipboard, which stores information temporarily. You can save the current contents of the Clipboard by using the ClipBook Viewer to copy it into your local ClipBook. You can then share that information, allowing others to connect to the ClipBook on your computer. *See also* Clipboard, ClipBook page.

ClipBook page
A unit of information pasted onto a local ClipBook. The ClipBook page is permanently saved. Information on a ClipBook page can be copied back onto the Clipboard and then pasted into documents. You can share ClipBook pages on the network.

Clipbook service
Supports the ClipBook Viewer application, allowing pages to be seen by remote ClipBooks.

Computer Browser service
Maintains an up-to-date list of computers and provides the list to applications when requested. Provides the computer lists displayed in the Select Computer and Select Domain dialog boxes, and (for Windows NT Server only) the lists in the Server Manager window.

computer name
A unique name of up to 15 uppercase characters that identifies a computer to the network. The name cannot be the same as any other computer or domain name in the network, and it cannot contain spaces.

configuration registry
A database repository for information about a computer's configuration.

connected user
A user accessing a computer or a resource over the network..

Control menu
A menu that contains commands you can use to manipulate a window.

Control-menu box
The icon at the left side of the title bar. This icon opens the Control menu for a window.

controller
See domain controller.

D

data frame
An organized, logical structure in which data can be placed.

datagram
A datagram is a basic messaging service. It provides connectionless data transfer when there is no association between the sender and receiver at the time the message is sent. Because the status of the receiver is unknown and no acknowledgments are sent, datagrams are considered unreliable. Datagrams allow messages to be broadcast to many stations at once.

Data Link layer
The second layer in the OSI model. It packages raw bits from the Physical layer into *data frames*.

DDE
See dynamic data exchange.

default printer
The printer that is used if you choose the Print command without first specifying which printer you want to use with an application. You can have only one default printer; it should be the printer you use most often.

default profile
See system default profile, user default profile.

dependent service
A service that requires the support of another service. For example, the Alerter service is dependent on the Messenger service.

desktop
The background of your screen, on which windows, icons, and dialog boxes appear.

destination directory
The directory to which you intend to copy or move one or more files.

destination document
The document into which a package or a linked or embedded object is being inserted. For an embedded object, this is sometimes also called the container document.

device contention
The way Windows NT allocates access to peripheral devices, such as a modem or a printer, when more than one application is trying to use the same device.

device driver
A program that enables a specific piece of hardware (device) to communicate with Windows NT. Although a device might be installed on your system, Windows NT cannot recognize the device until you have installed and configured the appropriate driver.

dimmed
Unavailable, disabled, or grayed. A dimmed button or command is displayed in light gray instead of black, and it cannot be chosen.

directory
Part of a structure for organizing your files on a disk. A directory can contain files and other directories (called subdirectories). *See also* directory tree.

directory entry
Any of the items shown in a directory listing. Each entry can be a file or another directory. The root directory is limited to 512 directory entries.

directory replication
The copying of a master set of directories from a server (called an export server) to specified servers or workstations (called import computers) in the same or other domains. Replication simplifies the task of maintaining identical sets of directories and files on multiple computers, because only a single master copy of the data must be maintained. Files are replicated whenever they are added to an exported directory and whenever a change is saved to the file. *See also* Directory Replicator service.

Directory Replicator service
Replicates directories, and the files in those directories, between computers. *See also* directory replication.

directory tree
A graphical display of a disk's directory structure. The directories on the disk are shown as a branching structure. The top-level directory is the root directory.

directory window
A File Manager window that displays the contents of a disk. The window shows both the directory tree and the contents of the current directory.

disabled user account
A user account that does not permit logons. The account appears in the user account list of the User Manager window and can be restored to enabled status at any time. *See also* user account.

disk configuration information
The Windows NT Registry includes information on the configuration of your disk(s): assigned drive letters, stripe sets, mirror sets, volume sets, and stripe sets with parity.

diskless workstations
Workstations that do not have a hard drive.

disk duplexing
Establishing a mirrored copy on a disk with a different controller.

disk mirroring
Maintaining a fully redundant copy of a partition on another disk.

disk striping
Writing data in stripes across a volume that has been created from areas of free space on from 2 to 32 disks.

domain
For Windows NT Server, a collection of computers that share a common domain database and security policy. Each domain has a unique name. *See also* workgroup.

domain controller
For a Windows NT Server domain, the server that authenticates domain logons and maintains the security policy and the master database for a domain. *See also* server.

domain database
See SAM database.

domain name
The name by which a domain is known to the network.

domain synchronization
See synchronize.

downloaded fonts
Fonts that you send to a printer either before or during the printing of a document. When you send a font to a printer, it is stored in the printing device's memory until it is needed.

drive icon
An icon in a directory window in File Manager that represents a disk drive on your system. Different icons depict floppy disk drives, hard disk drives, network drives, RAM drives, and CD-ROM drives.

drivebar
The horizontal bar in File Manager containing the drive icons.

dynamic data exchange
A form of interprocess communication (IPC) implemented in the Microsoft Windows family of operating systems. Two or more programs that support dynamic data exchange (DDE) can exchange information and commands.

E

embedded object
Presents information created in another application. Information in the embedded object does not exist in another file outside your document.

encapsulated PostScript (EPS) file
A file that prints at the highest possible resolution for your printing device. An EPS file can print faster than other graphical representations. Some Windows NT and non–Windows NT graphical applications can import EPS files.

end systems
Another name for workstations and servers. This term is often used in the context of wide area networks (WAN).

environment variable
A string consisting of environment information, such as a drive, path, or filename, associated with a symbolic name that can be used by Windows NT. You use the System option in Control Panel or the **set** command from the Windows NT command prompt to define environment variables.

event
Any significant occurrence in the system or in an application that requires users to be notified, or an entry to be added to a log.

Event Log service
Records events in the system, security, and application logs.

export path
In directory replication, a path from which subdirectories, and the files in those subdirectories, are automatically exported from an export server. *See also* directory replication.

export server
In directory replication, a server from which a master set of directories is exported to specified servers or workstations (called import computers) in the same or other domains. *See also* directory replication.

extended partition
Created from free space on a hard disk, an extended partition can be subpartitioned into zero or more logical drives. Only one of the four partitions allowed per physical disk can be an extended partition, and no primary partition need exist to create an extended partition.

extension
The period and up to three characters at the end of a filename. An extension usually indicates the type of file or directory.

external command
A command that is stored in its own file and loaded from disk when you use the command.

F

family set
A collection of related tapes containing several backup sets.

FAT
File Allocation Table; a table or list maintained by some operating systems to keep track of the status of various segments of disk space used for file storage.

file allocation table (FAT)
See FAT.

file system
In an operating system, the overall structure in which files are named, stored, and organized.

font set
A collection of font sizes for one font, customized for a particular display and printer. Font sets determine how text looks on screen and on paper.

frame
Data that is being transmitted is segmented into small units and combined with control information such as message start and message end. Each package of information is transmitted as a single unit called a frame.

frame preamble
Header information, added to the beginning of a data frame in the Physical layer.

frame type
The specifics of how the transmitted data is formatted and transmitted is controlled by the frame type. Examples of frame types are 802.2, 802.3, Ethernet II, and so on.

free space
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 that is not within an extended partition is available for the creation of a partition, with a maximum of four partitions allowed.

front end
In a client-server application, front end refers to the part of the program executing on the client computer.

full name
A user's complete name, usually consisting of the last name, first name, and middle initial. The full name is information that can be maintained by User Manager as part of the information identifying and defining a user account. *See also* user account.

G

gateway
A device used to connect dissimilar networks (networks using dissimilar protocols) so that information can be passed from one to the other. A gateway is at the Network layer of the OSI model.

global account
For Windows NT Server, a normal user account in a user's home domain. Most user accounts are global accounts. If there are multiple domains in the network, it is best if each user in the network has only one user account, in only one domain, and each user's access to other domains is accomplished by establishing domain trust relationships. *See also* local account.

global group
For Windows NT Server, a group that can be used in its own domain, servers and workstations of the domain, and trusting domains. In all these places it can be granted rights and permissions and can become a member of local groups. However, it can contain user accounts only from its own domain. Global groups provide a way to create handy sets of users from within the domain, available for use both inside and outside the domain.

Global groups cannot be created or maintained on Window NT workstations. However, for Windows NT workstations that participate in a domain, domain global groups can be granted rights and permissions at those workstations, and can become members of local groups at those workstations. *See also* group, local group.

group
In User Manager, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members, which makes groups a convenient way to grant common capabilities to collections of user accounts. For Windows NT, groups are managed with User Manager. For Windows NT Server, groups are managed with User Manager for Domains. *See also* built-in groups, global group, local group, user account.

group memberships
The groups to which a user account belongs. Permissions and rights granted to a group are also granted to its members. In most cases, the actions a user can perform in Windows NT are determined by the group memberships of the user account to which the user is logged on. *See also* group.

group name
A unique name that identifies a local or global group to Windows NT. A group's name cannot be the same as any other group name or user name in its own domain or workstation. *See also* global group, local group.

group window
In Program Manager, a window that displays the program item icons in a group.

H

hertz (Hz)
The unit of frequency measurement. Frequency measures how often a periodic event occurs, such as the manner a wave's amplitude, changes with time. One hertz equals one cycle per second. Frequency is often measured in kilohertz (KHz, 1000 Hz), megahertz (MHz), gigahertz (GHz, 1000 MHz), or terahertz (THz, 10,000 GHz).

high-performance file system
See HPFS.

home directory
A directory that is accessible to the user and contains files and programs for that user. A home directory can be assigned to an individual user or can be shared by many users.

host
Any device that is connected to the internetwork and uses TCP/IP.

host ID
The portion of the IP address that identifies a computer within a particular network ID.

host table
The HOSTS and LMHOSTS files, which contain mappings of known IP addresses mapped to host names.

HOSTS file
A local text file in the same format as the 4.3 Berkley Software Distribution (BSD) UNIX */etc/hosts* file. This file maps host names to IP addresses. In Windows NT, this file is stored in the *\systemroot*\SYSTEM32\DRIVERS\ETC directory.

HPFS High-performance file system (HPFS); primarily used with he OS/2 operating system version 1.2 or later. It supports long filenames but does not provide security.

hub
A unit that provides a common connection among computers in a star-configured network so that all of the computers can communicate with one another.

I

import computers
In directory replication, the servers or workstations that receive copies of the master set of directories from an export server. *See also* directory replication.

import path
In directory replication, the path to which imported subdirectories, and the files in those subdirectories, are stored on an import computer. *See also* directory replication.

Institute of Electrical and Electronic Engineers (IEEE) Project 802
A networking model developed by the Institute of Electrical and Electronic Engineers (IEEE). This project is called 802, for the year and month it began (February 1980). Project 802 defines LAN standards for the Physical and Data Link layers of the OSI model. The 802 project divides the Data Link layer into two sublayers: *Media Access Control* (MAC) and *Logical Link Control* (LLC).

intermediate systems
Equipment that provides a link, such as bridges, routers, and gateways.

internal command
Commands that are stored in the file CMD.EXE and that reside in memory at all times.

interrupt (IRQ)
An electronic signal sent to the computer's central processing unit.

interrupt request lines (IRQ)
Hardware lines over which devices can send signals to get the attention of the processor when the device is ready to accept or send information. Typically, each device connected to the computer uses a separate IRQ.

IPXODI.COM
The ODI version of the IPX/SPX protocol. Used in place of the standard IPX.COM, IPXODI.COM communicates between the LSL (Link Support Layer) and the applications.

K

kernel driver
A driver that accesses hardware.

L

link
The communication system connecting two LANs. Also, the equipment that provides the link, including bridges, routers, and gateways.

linked object
A representation or placeholder for an object that is inserted into a destination document. The object still exists in the source file and, when it is changed, the linked object is updated to reflect the changes.

Link Support Layer (LSL or LSL.COM)
This layer provides a foundation for the MAC driver to communicate with multiple protocols. LSL.COM performs functions similar to the protocol manager in NDIS.

list box
In a dialog box, a box that lists available choices, such as a list of all the files in a directory. If all the choices do not fit in the list box, there is a scroll bar.

local account
For Windows NT Server, a user account provided in a domain for a user whose global account is not in a trusted domain. Not required where trust relationships exist between domains. *See also* global account, user account.

local area network (LAN)
Computers connected in a geographically close network, such as in the same building or campus.

local group
For Windows NT, a group that can be granted permissions and rights only for its own workstation. However, a local group can contain user accounts from its own computer, and (if the workstation participates in a domain) user accounts and global groups both from its own domain and from trusted domains. Local groups provide a way to create handy sets of users from both inside and outside the workstation, to be used only at the workstation.

For Windows NT Server, a group that can be granted permissions and rights only for the servers of its own domain. However, it can contain user accounts and global groups both from its own domain and from trusted domains. Local groups provide a way to create handy sets of users from both inside and outside the domain, to be used only at servers in the domain. *See also* global group, group.

local printing device
A physical printing device that is directly connected to one of the ports on your computer.

logical drive
A subpartition of an extended partition on a hard disk.

Logical Link Control sublayer
The IEEE 802 project divides the Data Link layer into two sublayers. The Logical Link Control (LLC) layer is the upper sublayer that manages data link communication and defines the use of logical interface points (called Service Access Points [SAPs]), which other computers can refer to and use to transfer information from the LLC sublayer to the upper OSI layers.

logon hours
For Windows NT Server, a definition of the days and hours during which a user account can connect to a server. When a user is connected to a server and the logon hours are exceeded, the user is either disconnected from all server connections or is allowed to remain connected but denied any new connections.

logon script
Typically a batch file, a logon script runs automatically every time the user logs on. It can be used to configure a user's working environment at every logon, and it allows an administrator to affect a user's environment without managing all aspects of it. A logon script can be assigned to one or more user accounts.

logon script path
When a user logs on, the computer authenticating the logon locates the specified logon script (if one has been assigned to that user account) by following that computer's local logon script path (usually C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS) . *See also* logon script.

logon workstations
For Windows NT Server, the workstations from which a user is allowed to log on.

lost token
Refers to an error condition on a token ring network. This error causes an errant station to stop the token, causing a condition in which there is no token on the ring.

LPD (Line Printer Daemon)
A UNIX printing service. A daemon refers to a process that performs a particular system task.

M

mandatory user profile
For Windows NT Server, a user profile created by an administrator and assigned to one or more users. A mandatory user profile cannot be changed by the user and remains the same from one logon session to the next. *See also* personal user profile, user profile.

maximum password age
The period of time a password can be used before the system requires the user to change it. *See also* account policy.

Media Access Control (MAC)
The IEEE 802 standards divide the Data Link layer into two sublayers. The Media Access Control (MAC) sublayer communicates directly with the network adapter card and is responsible for delivering error-free data between two computers on the network.

Media Access Control (MAC) driver
The device driver located at the MAC sublayer. This driver is also known as the network adapter card driver or NIC driver. It provides low-level access to network adapters by supporting data transmission and some basic adapter management functions. These drivers also pass data from the Physical layer to transport protocols at the Network and Transport layers.

Messenger service
Sends and receives messages sent by administrators or by the Alerter service.

millions of bits per second (Mbps)
The unit of measure of supported transmission rates on the following physical media: coaxial cable, twisted-pair cable, and fiber-optic cable.

minimum password age
The period of time a password must be used before the user can change it. *See also* account policy.

minimum password length
The fewest characters a password can contain. *See also* Account policy.

monolithic protocol stack
A protocol driver that manages all functions of the MAC driver through the Transport layer in one protocol driver.

MS-DOS–based application
An application which is designed to run with MS-DOS, and which thus might not be able to take full advantage of all Windows NT features.

Multiple Link Interface Driver (MLID)
The part of the ODI interface that communicates between the adapter and the LSL. This is the hardware-dependent code created by the network adapter card manufacturer. This code usually carries the name of the supported adapter.

Multistation Access Unit (MAU)
The name for a token ring wiring concentrator. Also known as a *hub*.

N

named pipe
An interprocess communication mechanism that allows one process to communicate with another local or remote process.

Net Logon service
For Windows NT Server, performs authentication of domain logons, and keeps the domain's database synchronized between the domain controller and the other Windows NT Servers of the domain.

network
Two or more computers connected together by cables and running software enabling them to communicate with one another.

network adapter card
An expansion card or other device used to connect a computer to a local area network (LAN).

Network DDE DSDM service
The Network DDE DSDM (DDE share database manager) service manages shared DDE conversations. It is used by the Network DDE service.

Network DDE service
The Network DDE (dynamic data exchange) service provides a network transport and security for DDE conversations.

network device driver
Software that coordinates communication between the network adapter card and the computer's hardware and other software, controlling the physical function of the network adapter cards.

Network Device Interface Specification (NDIS)
A standard that defines an interface for communication between the MAC sublayer and protocol drivers. NDIS allows for a flexible environment of data exchange. It defines the software interface, called the *NDIS interface*. This interface is used by protocol drivers to communicate with the network adapter card.

network directory
See shared directory.

Network layer
The third layer in the OSI model. This layer is responsible for addressing messages and translating logical addresses and names into physical addresses. This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service, and other factors. It also manages traffic problems, such as switching, routing, and controlling the congestion of data packets on the network.

node
On a LAN, a device that is connected to the network and is capable of communicating with other network devices. For example, workstations, servers, and repeaters are called nodes.

non—Windows NT application
Refers to an application which is designed to run with Windows 3.*x*, MS-DOS, OS/2, or POSIX, but not specifically with Windows NT, and which might not be able to take full advantage of all Windows NT features (such as memory management).

NT
See Windows NT.

NT file system
See NTFS.

NTFS
An advanced file system designed for use specifically within the Windows NT operating system. It supports file system recovery, extremely large storage media, and various features for the POSIX subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes.

O

object
Any piece of information, created by using a Windows-based application with OLE capabilities, that can be linked or embedded into another document.

OLE
A way to transfer and share information between applications.

Open Data-Link Interface (ODI)
A specification defined by Novell and Apple to simplify driver development and to provide support for multiple protocols on a single network adapter. Similar to NDIS in many respects, ODI allows Novell NetWare drivers to be written without concern for the protocol that will be used on top of them.

Open Systems Interconnection (OSI) reference model
A seven-layer architecture that standardizes levels of service and types of interaction for computers exchanging information through a communications network. It is used to describe the flow of data between the physical connection to the network and the end-user application. This model is the best known and most widely used model for describing networking environments.

optical fibers
Fiber used to carry digital data signals in the form of modulated pulses of coherent light. An optical fiber consists of an extremely thin cylinder of glass, called the *core*, surrounded by a concentric sheath of glass, known as the *cladding*.

option button
A small round button that appears in a dialog box. Within a group of related option buttons, you can select only one button.

orphan
A member of a mirror set or a stripe set with parity that has failed in a severe manner, such as a loss of power or a complete head crash. When this happens, the fault tolerance driver determines that it can no longer use the orphaned member and directs all new reads and writes to the remaining members of the fault tolerance volume.

P

package
An icon that represents an embedded or linked object. When you choose the package, the application that was used to create the object either plays the object (such as a sound file) or opens and displays the object.

page
In ClipBook, one complete entry that has been pasted in. In memory, a fixed-size block.

paging file
See swap file.

partition
A portion of a physical disk that functions as though it were physically a separate unit. *See also* system partition.

password
A unique string of characters that must be entered before a logon or an access is authorized. A password is a security measure used to restrict logons to user accounts and access to computer systems and resources. For Windows NT, a password for a user account can be up to 14 characters long and is case-sensitive. *See also* account policy.

password uniqueness
The number of new passwords that must be used by a user account before an old password can be reused. *See also* account policy.

path
Specifies the location of a file within the directory tree. For example, to specify the path of a file named README.WRI located in the WINDOWS directory on drive C, you would type **c:\windows\readme.wri**.

peer-to-peer network
A network configuration in which devices operate on the same communications level. In other words, each station can operate as both a client and a server.

permission
A rule associated with an object (usually a directory, file, or printer) to regulate which users can have access to the object and in what manner. *See also* right.

persistent frame
An error condition on a token ring network. This error prevents a sending station from recognizing an acknowledgment data frame, which would then continue to circulate around the ring.

personal groups
In Program Manager, a program group you have created that contains program items. Personal groups are stored with your logon information and appear each time you log on. *See also* group.

personal user profile
For Windows NT Server, a user profile created by an administrator and assigned to one user. A personal user profile retains changes the user makes to the per-user settings of the Windows NT environment, and reimplements the newest settings each time that user logs on at any Windows NT workstation. *See also* mandatory user profile, user profile.

Physical layer
The first (bottommost) layer of the OSI model. This layer addresses the transmission of the unstructured raw bitstream over a physical medium (that is, the networking cable). The Physical layer relates the electrical/optical, mechanical, and functional interfaces to the cable. The Physical layer also carries the signals that transmit data generated by all the higher layers.

pipe
A portion of memory that can be used by one process to pass information along to another. It connects two processes so that the output of one can be used as the input to the other.

plotter font
A font created by a series of dots connected by lines. Plotter fonts can be scaled to any size and are most often printed on plotters. Some dot-matrix printing devices also support plotter fonts.

port
A connection or socket for connecting a device, such as a printing device, monitor, or modem, to your computer. Information is sent from your computer to the device through a cable.

POSIX
A family of standards for the UNIX operating system.

Presentation layer
The sixth layer of the OSI model. It determines the form used to exchange data between networked computers. It can be viewed as the network's translator. At the sending computer, this layer translates data from a format sent down from the Application layer into a commonly recognized intermediary format. At the receiving end, this layer translates the intermediary format into a format useful to that computer's Application layer. The Presentation layer also manages network security issues by providing services such as data encryption. It also provides rules for data transfer as well as data compression to reduce the number of bits that have to be transmitted.

primary partition
A portion of a physical disk that can be marked for use by an operating system. There can be up to four primary partitions (or up to three, if there is an extended partition) per physical disk. A primary partition cannot be subpartitioned.

printer driver
A program that controls how your computer and printer interact.

printer fonts
Fonts that are built into your printing device. These fonts are usually located in the printing device's read-only memory (ROM).

printer window
Displays information for one of the printers that you have installed or to which you are connected. For each printer, you can see what documents are waiting to be printed, who owns them, how large they are, and other information.

privileged processor mode
The portion of the Windows NT operating system that has direct access to system data and hardware.

process
As a noun, a program or part of a program; a coherent sequence of steps undertaken by a program—for example, an internal or external data-transfer operation, handling of an interrupt, or evaluation of a function.

As a verb, to manipulate data with a program.

program file
A file that starts an application or program. A program file has an .EXE, .PIF, .COM, or .BAT filename extension.

program group
In Program Manager, a collection of applications. Grouping your applications makes them easier to find when you want to start them.

program information file (PIF)
A file that provides information about how Windows NT should run a non–Windows NT application. PIFs contain such items as the name of the file, a startup directory, and multitasking options for applications running in 386 enhanced mode.

program item icon
An application, accessory, or document represented as an icon in a group window.

Project 802 topologies
802.3 defines standards for bus networks, such as Ethernet, that use a mechanism called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

802.4 defines standards for token-passing bus networks.

802.5 defines standards for token-passing ring networks.

The IEEE defined functionality for the LLC layer in Standard 802.2 and defined functionality for the MAC and Physical layers in Standards 802.3, 802.4, and 802.5.

protocol
A set of rules or standards designed to enable computers to connect with one another and to exchange information with as few errors as possible.

protocol driver
The protocol driver is responsible for offering four or five basic services to other layers in the network, while "hiding" the details of how the service is actually implemented. The services that the protocol driver performs include session management, datagram service, data segmentation and sequencing, acknowledgment, and possibly routing across a wide area network.

Q

quick format
Deletes the file allocation table and root directory of a disk but does not scan the disk for bad areas.

R

refresh
To update displayed information with current data.

Registry
See configuration registry.

remote administration
Administration of one computer by an administrator located at another computer and connected to the first computer over the network.

remote procedure call
RPC, a message-passing facility that allows a distributed application to call services available on various computers in a network. Used during remote administration of computers.

repeater
A device that regenerates signals so that they can travel on additional cable segments at their original strength.

replication
See directory replication.

resources
Any part of a computer system that can be shared, such as directories, printers, and CD-ROM drives.

right
Authorizes a user to perform certain actions on the system. Rights apply to the system as a whole, and are different from permissions, which apply to specific objects. *See also* permission.

root directory
See directory tree.

routers
Used to connect LANs. Routers allow the two networks to be administered independently yet to remain accessible to each other when communication is necessary. Routers connect networks at the Network layer of the OSI model.

RPC Locator service
The Remote Procedure Call Locator service allows distributed applications to use the RPC Name service. The RPC Locator service manages the RPC Name service database.

The server side of a distributed application registers its availability with the RPC Locator service. The client side of a distributed application queries the RPC Locator service to find available compatible server applications.

RPC service
The Remote Procedure Call service is the RPC subsystem for Microsoft Windows NT. The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.

RPC
See remote procedure call.

Remote Procedure Call service
See RPC service.

S

SAM
Security accounts manager. A Windows NT protected subsystem that maintains the SAM database and provides an application programming interface (API) for accessing the database.

SAM database
A database of security information that includes security information (such as user account names and passwords) and the settings of the security policies. For a Windows NT workstation, it is managed with User Manager. For a Windows NT Server domain, it is managed with User Manager for Domains.

Schedule service
Supports and is required for use of the **at** command. The **at** command can schedule commands and programs to run on a computer at a specified time and date.

screen buffer
The size reserved in memory for the command prompt display.

screen fonts
Fonts displayed on your screen. Soft-font manufacturers often provide screen fonts that closely match the soft fonts for your printing device. This ensures that your documents look the same on the screen as they do when printed.

scroll
To move through text or graphics (up, down, left, or right) in order to see parts of the file that cannot fit on the screen.

scroll bar
A bar that appears at the right or bottom edge of a window or list box whose contents are not completely visible. Each scroll bar contains two scroll arrows and a scroll box, which enable you to navigate through the contents of the window or list box.

security accounts manager
See SAM.

security database
See SAM database.

security ID
A unique name that identifies a logged-on user to the security system. Security IDs (SIDs) can identify one user or a group of users.

security identifier
See security ID.

security log
Records security events. It helps track changes to the security system and identify any possible breaches to security. For example, depending on the Audit settings in User Manager, attempts to log on to the system can be recorded in the security log. *See also* event.

security policies
For a Windows NT workstation, the security policies consist of the Account, User Rights, and Audit policies, and are managed with User Manager.

For a Windows NT Server domain, the security policies consist of the Account, User Rights, Audit, and Trust Relationships policies, and are managed with User Manager for Domains.

segment
A segment is the length of cable between two terminators. A segment can also refer to messages that have been broken up into smaller units by the protocol driver.

selection cursor
The marking device that shows where you are in a window, menu, or dialog box and what you have selected. The selection cursor can appear as a highlight or as a dotted rectangle around text.

server
For Windows NT, refers to a computer that provides shared resources to network users. *See also* client.

For Windows NT Server domains, refers to a computer that receives a copy of the domain's security policy and domain database and authenticates network logons. *See also* domain controller.

Server Manager
In Windows NT Server, an application used to view and administer domains, workgroups, and computers.

Server service
Provides RPC (remote procedure call) support, and file, print, and named pipe sharing.

service
A process that performs a specific system function and often provides an application programming interface (API) for other processes to call. Windows NT services are RPC-enabled, meaning that their API routines can be called from remote computers.

Session layer
The fifth layer of the OSI model. This layer allows two applications on different computers to establish, use, and end a connection called a *session*. This layer performs name recognition and the functions needed to allow two applications to communicate over the network, such as security functions. The Session layer provides synchronization between user tasks. This layer also implements dialog control between communicating processes, regulating which side transmits, the time and duration of transmission, and so on.

session management
Establishing, maintaining, and terminating connections between stations on the network.

sequence information
Enables the protocol driver on the receiving end to reassemble data frames in the right order.

share
To make resources, such as directories, printers, and ClipBook pages, available to network users.

share name
The name of a shared resource.

shared directory
A directory to which network users can connect.

shared network directory
See shared directory.

shared page
In ClipBook, a page that has been made available for others to access.

shared resource
Any device, data, or program that is used by more than one other device or program. For Windows NT, any resource that is made available to network users, such as directories, files, printers, and named pipes.

shortcut key
A key or key combination, available for some commands, that you can press to carry out a command without first selecting a menu. Shortcut keys are listed to the right of commands on a menu.

SID
See security ID.

single server
See central file server.

source directory
The directory that contains the file or files you intend to copy or move.

source document
The document in which a linked or embedded object was originally created.

split bar
Divides a directory window into two parts: the directory tree is displayed on the left, and the contents of the current directory are on the right.

status bar
A line of information related to the application running in the window. Usually located at the bottom of a window. Not all windows have a status bar.

string
A data structure composed of a sequence of characters, usually representing human-readable (alphanumeric) text.

subdirectory
A directory within a directory.

subsystem
A separate process that provides API services to other programs.

swap file
A special file on your hard disk. With virtual memory under Windows NT, some of the program code and other information is kept in RAM while other information is temporarily swapped to virtual memory. When that information is required again, Windows NT pulls it back into RAM and, if necessary, swaps other information to virtual memory. Also called a paging file.

symbolic link
A mechanism for indirectly referring to an object name. A symbolic link lets a user create a filename or directory name that, when used, is translated by the operating system into a different file or directory name. It is a simple method for allowing users to share a file or the contents of a directory indirectly, creating a cross-link between different directories in the usually hierarchical directory structure.

synchronize
To replicate the domain database from the domain controller to one server of the domain, or to all the servers of a domain. This is usually performed automatically by the system, but can also be initiated manually by an administrator.

syntax
The order in which you must type a command and the elements that follow the command. Windows NT commands have up to four elements: command name, parameters, switches, and values.

system default profile
For Windows NT Server, the user profile that is loaded when Windows NT is running and no user is logged on. When the Welcome dialog box is visible, the system default profile is loaded. *See also* user default profile, user profile.

system partition
The volume that contains the hardware-specific files needed to load Windows NT. *See also* partition.

T

Task List
A window that shows all running applications and enables you to switch between them. You can open Task List by choosing Switch To from the Control menu or by pressing CTRL+ESC.

text file
A file containing only letters, numbers, and symbols. A text file contains no formatting information, except possibly linefeeds and carriage returns. A text file is an ASCII file.

text-only file
An ASCII file that contains no formatting.

thread
An executable entity that belongs to one and only one process. It comprises a counter, a user mode stack, a kernel mode stack, and a set of register values. All threads in a process have equal access to a program's address space, object handles, and other resources.

time-out
If a device is not performing a task, the amount of time the computer should wait before detecting it as an error.

time slice
The amount of processor time allocated to an application, usually measured in milliseconds.

toolbar
A series of shortcut buttons providing quick access to commands. Usually located directly below the menu bar. Not all windows have a toolbar.

Transport layer
The fourth layer of the OSI model. It ensures that messages are delivered error-free, in sequence, and with no losses or duplications. This layer repackages messages for their efficient transmission over the network. At the receiving end, the Transport layer unpacks the messages, reassembles the original messages, and sends an acknowledgment of receipt.

trust
See trust relationship.

trust relationship
Trust relationships are links between domains that enable pass-through authentication, in which a user has only one user account in one domain, yet can access the entire network. User accounts and global groups defined in a trusted domain can be given rights and resource permissions in a trusting domain, even though those accounts do not exist in the trusting domain's database. A trusting domain honors the logon authentications of a trusted domain.

twisted-pair cable
A cable that consists of two insulated strands of copper wire twisted together. A number of twisted-wire pairs are often grouped together and enclosed in a protective sheath to form a cable. Unshielded twisted-pair cable is commonly used for telephone systems.

U

uninterruptible power supply (UPS)
See UPS.

UPS
Uninterruptible power supply: a battery-operated power supply connected to a computer to keep the system running during a power failure.

UPS service
Manages an uninterruptible power supply connected to a computer. *See also* UPS.

user account
Consists of all the information that defines a user to Windows NT. This includes such things as the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the system and accessing its resources. For Windows NT, user accounts are managed with User Manager. For Windows NT Server, use accounts are managed with User Manager for Domains. *See also* group.

user account database
See SAM database.

user default profile
For Windows NT Server, the user profile that is loaded by a server when a user's assigned profile cannot be accessed for any reason, when a user without an assigned profile logs on to the computer for the first time, or when a user logs on to the Guest account. *See also* system default profile, user profile.

User Manager
A Windows NT workstation tool used to manage the security for a workstation. Administers user accounts, groups, and security policies.

User Manager for Domains
A Windows NT Server tool used to manage security for a domain or an individual computer. Administers user accounts, groups, and security policies.

user mode
The portion of the Windows NT operating system that does not have direct access to system data and hardware; it must access system data and hardware through the privileged processor mode.

user name
A unique name identifying a user account to Windows NT. An account's user name cannot be the same as any other group name or user name in its own domain or workstation. *See also* user account.

user profile
Configuration information can be retained on a user-by-user basis, and it is saved in user profiles. The information includes all the per-user settings of the Windows NT environment, such as the desktop arrangement, personal program groups and the program items in those groups, screen colors, screen savers, network connections, printer connections, mouse settings, window size and position, and more. When a user logs on, the user's profile is loaded and the user's Windows NT environment is configured according to that profile.

User Profile Editor
For Windows NT Server, a tool used to create, edit, and save personal user profiles, mandatory user profiles, the user default profile, and the system default profile. *See also* user profile.

user right
See right.

user rights policy
Manages the assignment of rights to groups and user accounts.

V

virtual memory
Space on a hard disk that Windows NT uses as if it were actually memory. Windows NT does this through the use of swap files. The advantage of using virtual memory is that you can run more applications at one time than your system's physical memory would otherwise allow. The drawbacks are the disk space required for the virtual-memory swap file and the decreased execution speed when swapping is required.

volume
A partition or collection of partitions that have been formatted for use by a file system.

W

wide area network (WAN)
Computer networks using long-range telecommunications links, allowing the computers to be networked over long distances.

wild card
A character that represents one or more characters. The question mark (?) wildcard can be used to represent any single character, and the asterisk (*) wildcard can be used to represent any character or group of characters that might match that position in other filenames.

Windows NT Workstation
The portable, secure, 32-bit, preemptive multitasking member of the Microsoft Windows operating system family.

Windows NT Server
A superset of Windows NT Workstation, Windows NT Server provides centralized management and security, advanced fault tolerance, and additional connectivity.

workgroup
For Windows NT, a workgroup is a collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name. *See also* domain.

workstation
In general, a powerful computer having considerable calculating and graphics capability. For Windows NT, computers running the Windows NT operating system are called workstations, as distinguished from computers running Windows NT Server, which are called servers. *See also* server, domain controller.

Workstation service
Provides network connections and communications.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

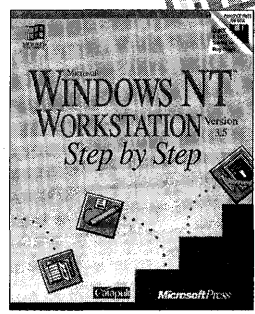
X

Step by Step books from Microsoft Press

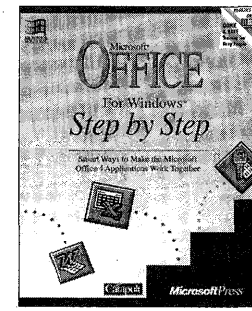
The Intelligent Choice for Self-Training

"Each chapter contains a clear statement of objectives, an appropriately conservative estimate of the time it will take you to complete, and a summary at the end to recap your progress. The lessons are well illustrated and point out both the mouse and keyboard commands needed to perform the various operations"

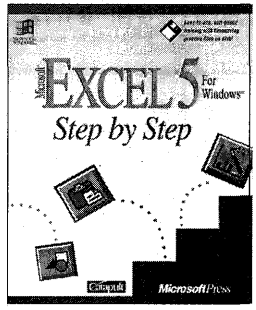
PC Magazine



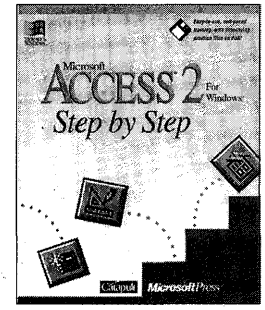
Microsoft® Windows NT™ Workstation Step by Step
ISBN 1-55615-695-2 $29.95 ($39.95 Canada)



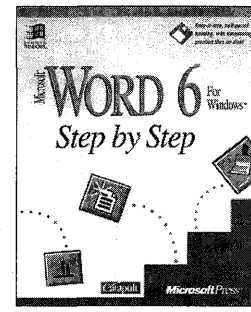
Microsoft® Office for Windows® Step by Step
ISBN 1-55615-648-0 $29.95 ($39.95 Canada)



Microsoft® Excel 5 for Windows® Step by Step
ISBN 1-55615-587-5 $29.95 ($39.95 Canada)



Microsoft® Access 2 for Windows® Step by Step
ISBN 1-55615-593-X $29.95 ($39.95 Canada)



Microsoft® Word 6 for Windows® Step by Step
ISBN 1-55615-576-X $29.95 ($39.95 Canada)

The *Step by Step* book-and-disk packages are the fastest way to master Microsoft® applications. Geared for time-sensitive individuals, books in the *Step by Step* series offer excellent self-paced instruction including disk-based tutorials, follow-along lessons, and practice exercises. And the information comes from Microsoft—so you can be assured of technical accuracy.

When it comes to intelligent training, training that thousands of individuals and hundreds of corporations are choosing, Microsoft Press® *Step by Step* books are the natural choice.

Microsoft® Press

Microsoft Press® books are available wherever quality books are sold and through CompuServe's Electronic Mall—**GO MSP**.
Call **1-800-MSPRESS** for more information or to place a credit card order.*
Please refer to **BBK** when placing your order. Prices subject to change.
*In Canada, contact Macmillan Canada, Attn: Microsoft Press Dept., 164 Commander Blvd., Agincourt, Ontario, Canada M1S 3C7, or call 1-800-667-1115.
Outside the U.S. and Canada, write to International Coordinator, Microsoft Press, One Microsoft Way, Redmond, WA 98052-6399 or fax +(206) 936-7329.

Learn to configure, optimize, troubleshoot, and integrate networks with the Microsoft® Windows NT™ Server network operating system version 3.5—and prepare for the Microsoft Certified Professional exam at the same time—with this in-depth course.

Objectives

Upon course completion, you will be able to install and configure Windows NT Server as a primary domain controller, backup domain controller, or a server in a domain; set up replication; implement hard disk fault tolerance; analyze domain models and implement related trust relationships; install and configure TCP/IP using DHCP; install and configure the Gateway Service for NetWare®; install and configure Microsoft Network Client Software; implement browsing in a wide area network domain; and resolve bottlenecks in a system's performance.

Topics Covered

- Comparing workgroup and domain models
- Installing Windows NT Server: defaults, preinstallation considerations, upgrade issues, and deinstallation
- Managing domains: Server Manager, User Manager for Domains, User Profile Editor, and the Net Logon Service
- Implementing import and export directory replication
- Protecting server data: RAID levels, sector sparing, and fault tolerance
- Establishing trust relationships, including pass-through authentication
- Using global and local groups to manage users
- Analyzing the four domain models: single, master, multiple master, and complete trust
- Interoperating with MS-DOS® and Microsoft Windows® for Workgroups
- Using TCP/IP with Windows NT Server, including DHCP and the Windows Internet Naming Service (WINS)
- Integrating Novell® NetWare with Windows NT Server, including NWLink, and the Gateway Service for NetWare (GSNW)
- Browsing for network resources: Domain Master browsers, synchronization, multiple domains, and WAN browsing
- Optimizing Windows NT Server for performance

Prerequisites

This kit teaches operational and support details of the Microsoft Windows NT Server network operating system. It assumes that you have successfully completed the *Support Fundamentals for Microsoft Windows NT* course (either instructor-led or self-paced) or have equivalent knowledge of Windows NT Server.

NOTE: The accompanying disks include supplementary utilities for the Windows NT operating system. To install them, you must have Windows NT Workstation or Windows NT Server already installed.

Version 3.5

1294 Part No. 098-57538

Microsoft Press