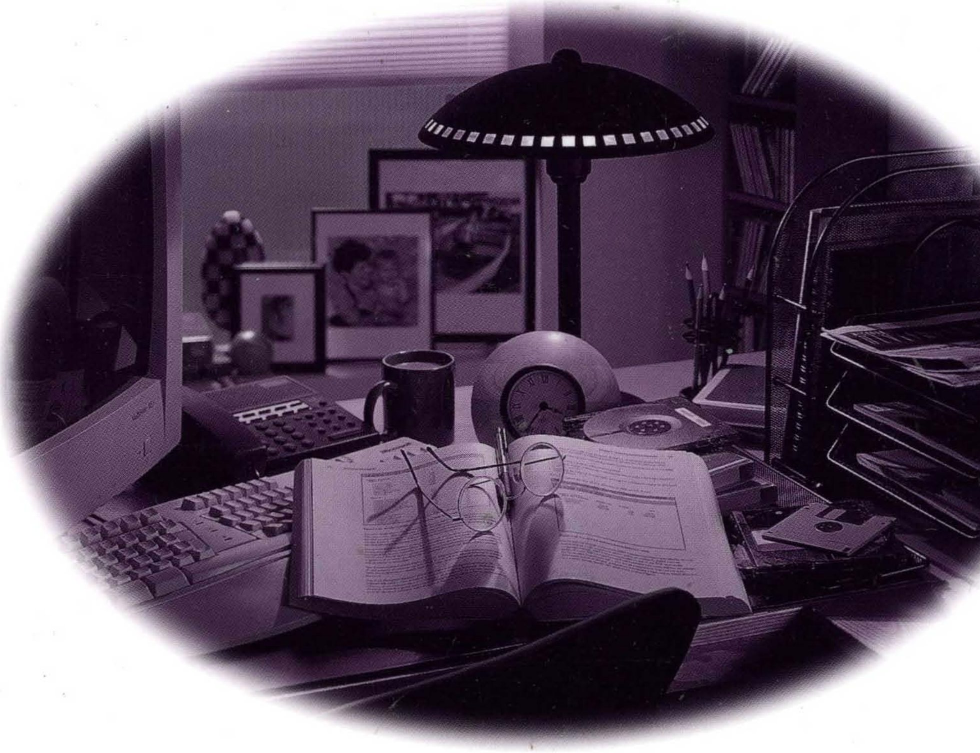
Microsoft®
Windows NT®



Microsoft® Windows NT® Network Administration

Hands-On, Self-Paced Training for Administering Version 4.0

Microsoft® Press

Microsoft®

Windows NT® Network Administration

Microsoft® Press

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

Library of Congress Cataloging-in-Publication Data pending.

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 WCWC 2 1 0 9 8 7

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

A CIP catalogue record for this book is available from the British Library.

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 and Instructional Designer: Susan Greenberg
Instructional Design and Technical Writing contributors: Kate Knight, Tom Parker
Technical Contributors: Ryan Calafato, Jonathan Corners, Andrew Mason
Graphic Artist: Kimberly Jackson
Graphics Contributor: Julie Stone
Multimedia Producers: Susan Greenberg, Beverly Hare
Assistant Multimedia Producer: Sandra Alto
Interactive Lab Developer: Wendy Wahl
Multimedia Development: Digital Post & Graphics
Video Compression and Processing: "E.J." John Erickson, Brian Snyder
Web Page Design and Development: Kate Knight, Nikki McCormick
Web Page Graphic Design: Becky Johnson
Editor: Laurie Pritchard
Production Support: Irene Barnett
Indexers: Jane Dow, Barbara Sherman
Manufacturing Support: Bo Galford
Product Managers: Dean Murray, Robert Stewart, Elaine Stovall

Acquisitions Editor: Eric Stroo
Project Editor: Stuart Stuple

Contents

Chapter 10 Monitoring Resources 363

Chapter 11 Backing Up and Restoring Files 393

FOREWORD

Microsoft Windows NT Network Administration

If you're buying garden gloves or an apron, one size can fit all. But your best business suit has to fit you like it fits no one else. That's because, while simple solutions are adequate for simple needs, your sophisticated needs generally require equally sophisticated solutions.

When Microsoft first introduced the Microsoft® Windows NT® operating system four years ago, it was managed in relatively simple network installations and a single, simple training course sufficed to educate IT professionals—who almost always had other, primary responsibilities—in its use. What a difference a few years can make. Today, Windows NT is the market-leading network operating system and the fastest-growing, as well. It has scaled up to support the enterprise needs of the largest corporations and, now, the new needs of intranets and the Internet.

With all this growth in the market for Windows NT, a single training course is no longer enough. At Microsoft, we build courses around specific job titles, to ensure that they're relevant for the professionals who will take them. Over the past few years, Windows NT has become important enough to most corporate users to warrant a specific, new job title: the Windows NT administrator. But those Windows NT administrators didn't have a Windows NT course just for them.

The self-study course you're holding in your hands responds to this need of Windows NT administrators. And Windows NT administrators have responded to it, in return. When the instructor-led version of this course was introduced in July, 1996, Windows NT administrators made it one of Microsoft's ten most popular courses in just two months.

And no wonder. The only thing that's growing as fast as the market for Windows NT products is the market for trained professionals to manage them. Microsoft has boosted the population of IT professionals trained on Windows NT to more than 400,000 last year and the demand continues unabated. At the end of 1996, ComputerWorld rated Windows NT administration as the fifth-hottest skill for IT professionals.

Windows NT administrators have also flocked to this course because it teaches them exactly what they need to know to make the best decisions with Windows NT. Microsoft believes in customizing each of its courses with hands-on, relevant training geared to the specific, daily needs of a single job title. This course in Windows NT administration is no exception. Forget time-consuming histories of the computer industry or the development of Windows NT. The course starts with the information you need to be more effective—and to be seen as more effective by current or prospective managers, employers, customers, or clients. After just the first chapter, you'll understand the key differences between the two Windows NT products, the tools available to administer them, and the key components of the Windows NT network.

Our emphasis on providing practical, hands-on information to help you make the best decisions about implementing Windows NT has also led to another innovation: This course is our first to be integrated with *best practices*. Windows NT administrators want to know the options available to them, but they also want to know the best option for their specific circumstances. Best practices information meets this need, based on advice from the world's leading Windows NT administrators, developers, and solutions providers, as well as from Microsoft's own Windows NT team. What's the best way to ensure the security of user accounts and disk resources? To implement a plan for backing up files? To make file and print resources available to network users? Whatever your needs, you'll find best practices tips and checklists to meet them.

As a professional in technology education management, I'm delighted to have played a key role in spurring the creation of this path-breaking course. But my enthusiasm runs even deeper, because I began my career as an IT administrator. So, I know that this is the type of information that today's IT professionals need, presented in the way that they need it. Hundreds of thousands of IT professionals already agree. I hope that very soon, you will too.

Nancy Lewis
General Manager, Training and Certification Worldwide
February 7, 1997

About This Book

Welcome to *Microsoft Windows NT Network Administration.* This book provides the knowledge and skills necessary to perform post-installation and day-to-day Windows NT administration tasks in single-domain and multiple-domain networks. It also helps prepare you to meet the certification requirements to become a Microsoft Certified Professional.

The "About This Book" provides important Setup procedures that will prepare your computer for the lessons. Read through "About This Book" thoroughly before you start the lessons. All lessons depend on the completion of the Setup procedures in "About This Book."

The chapters in this book are divided into lessons. Most lessons include hands-on procedures to practice or demonstrate key concepts and skills. At the end of each lesson is a summary of key points, and when appropriate, references to additional information on the lesson material or related topics. At the end of each chapter is a review of the critical points made throughout the chapter.

Intended Audience

This book is intended for those who administer Microsoft Windows NT Server and Windows NT Workstation, and for those who are on the Microsoft Certified Systems Engineer Windows NT 4.0 Track.

Prerequisites

- Working knowledge of an operating system, such as Microsoft MS-DOS®, UNIX, Microsoft Windows® version 3.*x*, Windows for Workgroups, Windows 95, or Windows NT.
- Proficiency using the Windows 95 or Windows NT version 4.0 interface, including the ability to use Windows Explorer to locate, create, and manipulate folders and files, to create shortcuts, and to configure the desktop environment.
- Working knowledge of major networking components, including clients, servers, local area networks (LAN), network adapter cards, drivers, protocols, and network operating systems.
- Knowledge of basic computer hardware components, including computer memory, hard disks, central processing unit (CPU), communication and printer ports, display adapters, and pointing devices.

Finding the Best Starting Point for You

The modular design of this book offers you considerable flexibility in customizing your learning. You can go through lessons in almost any order, skip lessons, and repeat lessons later to review certain skills. Lessons in each chapter build on concepts presented in previous lessons, so you may want to back up if you find that you do not understand the concepts and terminology used in a particular lesson. If the steps in one lesson require that you have completed the steps in an earlier lesson, you are told of this fact at the start of the lesson.

The following table recommends starting points depending on your Windows NT experience.

If you	Follow this learning path
Are preparing to take the Microsoft Certified Professional Exams (70–67, *Implementing and Supporting Microsoft Windows NT Server 4.0*, and 70–73, *Implementing and Supporting Microsoft Windows NT Workstation 4.0*)	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapters 1–3 and Chapters 5–6. Work through the other chapters in any order.
Want to learn key Windows NT concepts and skills	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapters 1–3 and Chapters 5–6.
Want to set up and maintain user accounts	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapters 1–4.
Want to make files available to network users	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapter 5.
Want to secure disk resources	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapters 5–6.
Want to set up a network print server	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapters 7–8.
Want to back up network files	Read "Getting Started" and complete the procedures in "Setup Procedures" (both located later in "About This Book"). Next, work through Chapter 11.
Need information on a specific topic related to Windows NT	Refer to the table of contents or index in this book, or refer to Windows NT Help.
Need to know the definition of a Windows NT term	Refer to the glossary in Windows NT Help or at the end of this book.

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.

Features of This Book

- Each chapter opens with an "About This Chapter" section, which provides an overview of the chapter content.
- Following "About This Chapter," each chapter contains a "Before You Begin" section, which describes the prerequisites and setup required for the chapter.
- Whenever possible, lessons contain procedures that give you an opportunity to build your skills. All procedures are identified through the following procedural convention: ▶
- The "Lesson Summary" provides a summary of the key points of the lesson. Use this summary to gage whether you understood the important concepts of the lesson.
- 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 that is referred to covers product documentation, online locations, or both.
- The "Review" section at the end of each chapter is available to test what you have learned in the lesson.
- The "Answer Key" section contains all of the questions and corresponding answers for each chapter. Each question is referenced by page number.
- The "Glossary" presents a set of definitions for the technical terms that appear in this book and some related terms.

Notational Conventions

- Dialog box names, options, menu names, and menu commands appear in **bold** type.
- Characters or commands that you type appear in **bold lowercase** type (unless what you type is case-sensitive).
- *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 or folders appear in Title Caps, except when you are to type them directly. Unless otherwise indicated, you can use lowercase letters when you type a folder name or file name in a dialog box or at the command prompt.

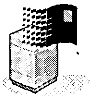
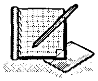
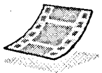
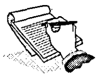
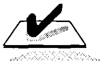
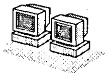
- File name extensions appear in all lowercase.
- Square brackets [ ] are used in syntax statements to enclose optional items. For example, [*file_name*] in command syntax indicates that you can choose to type a file name with the command. Type only the information within the brackets, not the brackets 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 make the menu bar active, 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 that is listed next to the particular menu command, such as CTRL+C for the **Copy** command.
- 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.

Icons

The following table describes the icons that are used throughout this book.

Icon	Description
	Identifies content that applies only to computers running Windows NT Server.
	Indicates a hands-on procedure for you to complete. If this symbol does not appear next to a section with steps, it is not intended as a hands-on procedure.
	Indicates instructions for starting a video. Videos are located on the Supplemental Material compact disc in an .avi format.
	Identifies content useful in planning.
	Indicates a best practice. A best practice is the way of performing a task that Microsoft recommends you follow.
	Calls out cautions or warnings. Cautions indicate a possible loss of data. Warnings indicate possible damage to hardware.
	Identifies content that is useful in identifying and troubleshooting problems.
	Indicates questions for you to answer. Sometimes the questions reference an illustration that you need to examine. Other times, the questions are for the purpose of reviewing and reinforcing key concepts.
	Indicates that two computers are required to complete the procedure. Procedures that have this icon are not required to meet the lesson objectives. Instead, they provide additional practice.

Notes

The following list describes the notes that appear throughout this book:

- Notes marked **Tip** contain explanations of possible results or alternative methods of performing a task. These tips may be suggested as best practices.
- Notes marked **Important** are items that 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.

Chapter and Appendix Overview

This self-paced training combines text, hands-on procedures, videos, and review questions to teach you how to administer Windows NT Workstation and Windows NT Server.

The self-paced training book is divided into the following chapters and appendix:

- Chapter 1, "Introduction to Administering Windows NT," provides you with a foundation of knowledge useful for all chapters in this book. It includes an overview of Microsoft Windows NT Server and Windows NT Workstation, describes the administrative differences between them in a workgroup and a domain, and discusses directory services, the Windows NT Server services that provide a single user logon, centralized administration, and access to domain resources. It also introduces you to the administrative tasks and tools that you will use throughout this book and the essential tasks that all users perform when using Windows NT. The hands-on procedures guide you through Windows NT basics.
- Chapter 2, "Setting Up User Accounts," introduces you to the three types of user accounts and provides you with a planning strategy for implementing them. The hands-on procedures give you an opportunity to plan and create your own user accounts.
- Chapter 3, "Setting Up Group Accounts," provides you with a groups planning strategy and procedures for creating groups. The hands-on procedures give you an opportunity to plan and implement local and global groups for a network.
- Chapter 4, "Administering User and Group Accounts," presents tasks related to maintaining existing accounts and streamlining administrative tasks, including creating template accounts, modifying multiple accounts at one time, planning and implementing an account policy, maintaining domain controllers, and troubleshooting user logon problems. The hands-on procedures give you an opportunity to implement and practice each task.
- Chapter 5, "Securing Network Resources with Share Permissions," explains how to share folders and how to assign permission for gaining access to the shared folders to user and group accounts. The hands-on procedures give you an opportunity to plan and share folders and to secure them with permissions.
- Chapter 6, "Securing Network Resources with NTFS Permissions," explains how NTFS permissions secure local resources, and how when combined with share permissions, NTFS permissions secure resources from users who connect to resources over the network. The hands-on procedures give you an opportunity to plan and implement NTFS permissions, and to troubleshoot common permission-related problems.

- Chapter 7, "Setting Up a Network Print Server," introduces you to Windows NT printing. It explains procedures and guidelines for setting up and configuring a network print server. The hands-on procedures give you an opportunity to implement and practice these tasks.
- Chapter 8, "Administering a Network Print Server," presents the post-installation and configuration print server administration tasks, including tasks related to managing documents and printers, and identifying printing problems. In the hands-on procedures, you will have an opportunity to perform many of these tasks on your own printer.
- Chapter 9, "Auditing Resources and Events," introduces auditing and provides guidance in planning and implementing a domain Audit policy. The hands-on procedures give you an opportunity to plan and implement an Audit policy, to set up auditing on files and printers, and to use Event Viewer to view audited events and archive security logs.
- Chapter 10, "Monitoring Resources," provides an overview of Server Manager and Windows NT Diagnostics and shows you how to use them to obtain key information about network and computer resources. The hands-on procedures guide you through viewing computer properties; viewing user sessions, shared resources, and resources in use; setting administrative alerts; sending messages to users; and gathering information about a computer configuration to use for inventory tracking and troubleshooting.
- Chapter 11, "Backing Up and Restoring Files," describes planning strategies for backing up files on your network and shows you how to use Windows NT Backup to back up and restore files. In the hands-on procedures, you use a Backup Simulation program to back up and restore files. This program simulates Windows NT Backup.
- Appendix A, "Planning Worksheets," provides completed planning worksheets for use with the planning exercises in Chapters 2, 3, 5, 6, and 11. Use them to check your answers or use them as guides for implementing tasks.

Getting Started

This self-paced training contains hands-on procedures to help you learn how to administer Windows NT Workstation and Windows NT Server. To complete these procedures, you must have the following:

- One computer running Windows NT Server version 4.0 configured as a domain controller, with an audio board and headphones or speakers; a CD-ROM drive; and a VGA or higher-resolution monitor, minimum of 256 color support.

Note There are a few procedures in this book that require two computers to complete them. Using a second computer is optional; it is not required to meet the lesson objectives.

It is recommended that you set up a domain controller on its own network specifically for this self-paced training because, to complete the lessons in this book, you will need to make changes to the domain controller that can affect other network users. However, you can use a domain controller on an existing network.

You can use the evaluation copy of Windows NT Server that is included with this book to set up a domain controller. The evaluation copy can be installed in a separate directory on an existing Windows NT–based computer. The evaluation copy is good for 120 days from the date that you install it. To install it, you need the following:

- On Intel and compatible systems: 486/33 MHz or higher, Pentium, or Pentium PRO processor, and 125 megabytes (MB) of free hard disk space.

  –or–

  On RISC-based systems: RISC processor compatible with Windows NT Server version 4.0, and 160 MB of free hard disk space.
- 16 MB of memory (RAM)
- VGA, Super VGA, or video graphics adapter compatible with Windows NT Server 4.0
- CD-ROM drive

Note All hardware must be on the Microsoft Windows NT 4.0 hardware compatibility list (HCL).

- Use of the built-in Administrator account on the domain controller or any user account on the domain controller with administrative privileges (one that is a member of the Administrators group).

  If you install the evaluation copy of Windows NT Server that is included with this book, an Administrator account will be created for you.

- A volume formatted with the Windows NT File System (NTFS). If you plan on using an existing domain controller and it does not already have an NTFS volume, see your network administrator before you convert one.

  If you do not have an NTFS volume and are prevented from creating one (for example, if Windows 95 is running on the same computer), you will still be able to complete most lessons in this book. However, you will not be able to complete the lessons in Chapter 7, "Securing Network Resources with NTFS Permissions" or Chapter 9, "Auditing Resources and Events."

Cross-References to Windows NT Documentation

You will find references to Windows NT documentation and Windows NT Help throughout this book. These references point you to more information about the task at hand.

- Microsoft Windows NT Server *Concepts and Planning* explains how to implement and optimize Windows NT Server. It is designed for new and experienced administrators of small networks and advanced users of operating systems. The online version of Microsoft Windows NT Server *Concepts and Planning* is included on the Windows NT Server compact disc.
- The *Microsoft Windows NT Server Resource Kit* (for version 4.0) provides detailed information on implementing Windows NT Server in larger networks.
- The *Microsoft Windows NT Workstation Resource Kit* (for version 4.0) provides detailed information on the Windows NT Workstation operating system, plus topics that are either new for version 4.0 or that reflect issues that Microsoft Technical Support Engineers consider timely and important.
- Windows NT Help, available online when you install Windows NT, provides references and how-to information for all Windows NT tasks.

Setup Procedures

The following information is a checklist of the tasks that you need to perform to prepare your computer for the lessons in this book. If you do not have experience installing Windows NT or another network operating system, you may need help from an experienced network administrator. As you complete a task, mark it off in the check box. Step-by-step instructions for each task follow.

□ Create Windows NT Server Setup disks. These disk are required to install the evaluation copy of Windows NT Server. If you plan on completing the lessons in this book on an existing domain controller, skip this procedure.

□ Install the evaluation copy of Windows NT Server (provided with this book), and configure it as a domain controller. If you plan on completing the lessons in this book on an existing domain controller, skip this procedure.

Note The installation information provided will help you prepare a computer for use with this book. It is not intended to teach you installation. For comprehensive information on installing Windows NT Server, see the *Microsoft Windows NT Technical Support* self-paced training, also available from Microsoft Press.

□ Install the self-paced training files. These files are required to complete the lessons. You need 6 MB of free disk space to install them.

□ Assign the *Log on locally* user right to the Everyone group. This will ensure that all user accounts required to complete the lessons in this book have the ability to log on the computer.

□ Create a user account named User1 with a password of **secret** (all lowercase) to prepare for the lessons in Chapter 1.

□ Share the Users and Profiles folders to prepare for the lessons in Chapter 2. The Users and Profiles folders are created when you install the self-paced training files.

□ Install Microsoft Internet Explorer 3.*x*. Internet Explorer 3.*x* is required only so that you can view the Web page on the Supplemental Material compact disc. It is not required to complete the lessons in this book. Skip this procedure if you already have Internet Explorer 3.*x* installed.

□ Install the Intel Video drivers required to play the instructional videos included on the Supplemental Material compact disc.

□ Set the color palette and desktop area for your monitor so that you can view the instructional videos included on the Supplemental Material compact disc. You only need to complete this procedure if you do not configure the color and resolution when you install the evaluation copy of Windows NT Server.

▸ To create Windows NT Server Setup disks

In this procedure, you create the three Setup disks that are required to install the evaluation copy of Windows NT Server. To complete this procedure, you need three blank, formatted disks.

Note This procedure requires that you have an operating system installed that provides the ability to access the CD-ROM drive on that computer.

1. Insert the Microsoft Windows NT Server compact disc into the CD-ROM drive.

   If a Windows NT CD-ROM windows appears, close it.

2. Go to a command prompt (If you are using a computer running Windows 95 or Windows NT, click the **Start** button, point to **Programs**, and then click **Command Prompt**.) and type one of the following commands:

   On a computer running MS-DOS, Windows 3.1, Windows for Workgroups, or Windows 95, type the following command, and then press ENTER.

   cd_drive\i386\winnt /ox**

   where *cd_drive* is the appropriate letter for your CD-ROM drive.

   –or–

   On a computer running Windows NT, type the following command, and then press ENTER.

   *cd_drive***\i386\winnt32 /ox**

   where *cd_drive* is the appropriate letter for your CD-ROM drive.

   The Windows NT 4.00 Upgrade/Installation dialog box appears, prompting for the location of the Windows NT Server files.

3. If the path to your compact disc does not already appear, type *cd_drive***:\i386** and then click **Continue**.

4. When prompted, label a blank disk as *Windows NT Server Setup Disk #3,* insert the disk into drive A, and then click **OK**.

   Setup prepares Disk #3.

5. When prompted, label a blank disk as *Windows NT Server Setup Disk #2,* insert the disk into drive A, and then click **OK**.

   Setup prepares Disk #2.

6. When prompted, label a blank disk as *Windows NT Server Setup Boot Disk,* insert the disk into drive A, and then click **OK.**

   Setup prepares the boot disk.

   When Setup has finished preparing the disks, the command prompt appears.
7. Close the Command Prompt window.
8. Remove the compact disc from the CD-ROM drive.

▸ **To install the evaluation copy of Windows NT Server**

Note If your computer is part of a part of a larger network, verify with your network administrator that the computer name, domain name, and IP address information does not conflict with network operations. If they will conflict, ask the network administrator to provide alternative values.

1. With the Windows NT Server Setup Boot Disk in drive A, restart the computer.
2. When prompted, insert Setup Disk #2, and at the subsequent prompts, insert Setup Disk #3, and then insert the CD-ROM.
3. Read the online instructions carefully. For many of the instructions, you can accept the default settings.
4. When prompted, supply the following configuration information.

When prompted for	Do this
A response to whether you are upgrading or installing a new version (fresh copy)	If you are installing the evaluation copy of Windows NT Server on the same computer as another version of Windows NT, type **N** for new version.
Partition information	Select a partition that has enough free disk space to install Windows NT Server.
File system information	Select **Leave current file system intact.**
A location to install Windows NT files	If you are installing the evaluation copy of Windows NT Server on the same computer as another version of Windows NT, type a different name (for example, \NTEval or \120Eval). Otherwise, accept \Winnt. (The location that you specify will be referred to in the lessons as *systemroot.*)

(continued)

When prompted for	Do this
Your name and organization	Type your name and your organization's name.
The CD key	Type **040** followed by **0048126**
The licensing mode	In the **Per Server for** box, type **10** for the maximum number of client access licenses provided with the evaluation copy of Windows NT Server.
A name for your computer	Type a name that is unique to your network.
The server type	Click **Primary Domain Controller**.
The Administrator account password	Type a password for the default Administrator account. Keep in mind that passwords are case-sensitive.
A response to the floating-point workaround (only appears on Pentium-based computers that have floating-point arithmetic problems)	Click **Do not enable the floating-point workaround**.
Emergency repair disk	Click **No, do not create an emergency repair disk** (you may want to create an Emergency Repair Disk for your computer, but it will not be used in this book).
The components to install	Click **Games** (required for some lessons). The default components should remain selected.
How this computer should participate on a network	If your computer is on a network, make sure **Wired to the network** is selected.
Install Microsoft Internet Information Server	Click to clear.
Setup to start searching for a Network Adapter	Click **Start Search**. If Setup cannot detect the installed network adapter or if your computer does not have a network adapter, click **Select from list**. If your computer does not have a network adapter, under **Network Adapter**, click **MS Loopback Adapter**. Otherwise, select your network adapter.
Network protocols	Accept **TCP/IP Protocol** and **NWLink IPX/SPX Compatible Transport**.

(continued)

When prompted for	Do this
TCP/IP setup. Do you wish to use DHCP?	Click **Yes** if your computer is connected to a network that has a DHCP server. (Check with your network administrator if you are unsure.) Otherwise, click **No**.
An IP address (appears if there is no DHCP server)	Type **131.107.2.200** (If your computer is on a network, check with the network administrator to verify that this IP address does not conflict with an existing IP address.)
A subnet mask (appears if there is no DHCP server)	Type **255.255.255.0** (If your computer is on a network, check with the network administrator for a valid subnet mask.)
A default gateway (appears if there is no DHCP server)	If your computer is on a network, check with the network administrator for a valid default gateway to use. Otherwise, leave it blank.
A name for your domain	Type a name that is unique to your network.
Time zone information	Specify your time zone.
The display properties	Set the **Color Palette** for 256 colors. Set the **Desktop Area** for 800 x 600 pixels.

5. When prompted, restart the computer.

Important If you do not have an NTFS volume, you need to convert a file allocation table (FAT) volume to NTFS. If your computer dual-boots with MS-DOS or Windows 95, do not convert the MS-DOS or Windows 95 system volume or you will no longer be able to boot those operating systems. For instructions on how to convert a volume from FAT to NTFS, see "Convert Command" in Windows NT Help.

▸ **To install the self-paced training files**

1. Log on as Administrator.
2. Insert the Supplemental Material compact disc into the CD-ROM drive.
3. In the root of the compact disc, double-click Setup.exe.

   A **Microsoft Windows NT Network Administration Setup** dialog box appears.
4. Click **Continue.**
5. In the **Name** box, type your name.

6. In the **Organization** box, type the name of your organization (optional), and then click **OK**.
7. Click **OK** to confirm that the Name and Organization information was entered correctly.

   A **Microsoft Windows NT Network Administration Setup** dialog box appears.
8. Under **Folder**, verify that the path points to a volume formatted with NTFS.

   If the path points to a volume formatted with FAT, click **Change Folder**, and then in the **Path** box, type *drive*:**\Program Files\Admin Training** (where *drive* is the drive letter of your NTFS volume) and then click **OK**.

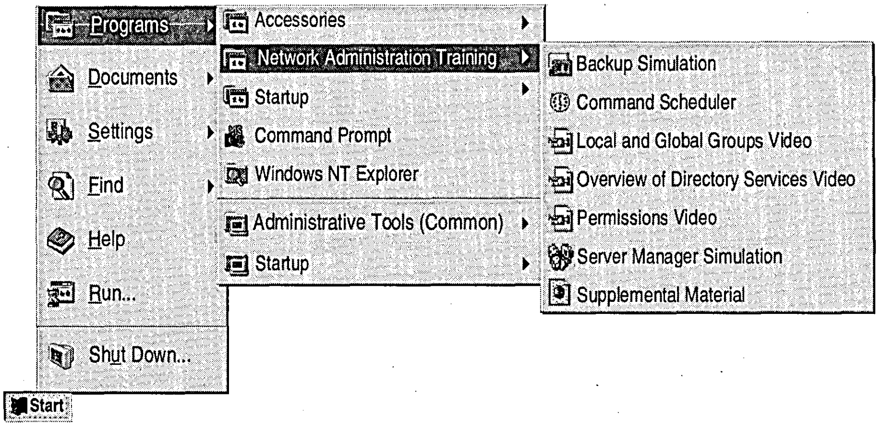
   If you are prompted to create the destination folder, click **Yes**.
9. Click the **Setup** button.

   Setup checks for free disk space and then copies the Admin Training folder to the specified path.

   The LabFiles folder is copied to the root of the drive that you specified. For example, if you specify D:\Program Files\Admin Training in the **Path** box, LabFiles will be located in D:\LabFiles. The LabFiles folder contains the folders and files required to complete the lessons in this book. You may want to record the drive location here.

10. When Setup has completed successfully, click **OK**.

    The Setup program installed the required files on your hard disk, created a **Network Administration Training** menu, and then added shortcuts to the files on the **Network Administration Training** menu.



The following list describes the shortcuts that appear on the **Network Administration Training** menu:

- *Backup Simulation* is a Microsoft® Visual Basic program that simulates Windows NT Backup, but does not require a tape drive in your computer. This program is required to complete Chapter 11, "Backing Up and Restoring Files," to simulate backing up and restoring files on your hard disk.
- *Command Scheduler* is a *Microsoft Windows NT Server Resource Kit* utility (for version 4.0) that schedules batch and executable files to start a process, such as a backup, at a specified time. This utility is required to complete Chapter 11, "Backing Up and Restoring Files."
- *Local and Global Groups Video* is a six minute instructional video that defines local and global groups and explains how they are used in single-domain and multiple-domain networks. This video is required to complete Chapter 3, "Setting Up Group Accounts."
- *Overview of Directory Services Video* is a five minute instructional video that describes the components in a Windows NT network and the role of user accounts in Windows NT Directory Services. This video is required to complete Chapter 1, "Introduction to Administering Windows NT."
- *Permissions Video* is a five minute instructional video that shows the effective permissions when shared folder and NTFS permissions are combined. This video is required to complete Chapter 6, "Securing Network Resources with NTFS Permissions."
- *Server Manager Simulation* program is a Visual Basic program that simulates promoting and synchronizing multiple domain controllers in Server Manager using a single computer. This program is required to complete Chapter 4, "Administering User and Group Accounts."
- *Supplemental Material* is a Web page on the Supplemental Material compact disc. This Web page provides information on the Microsoft Certified Trainer program (including the *Administering Microsoft Windows NT 4.0* self-administered assessment), course materials, and key Web sites. To open the Web page, in the root of the Supplemental Material compact disc, double-click Open.htm.

Note The videos are the only files that are not installed on your hard disk. The menu shortcuts for the videos require that the Supplemental Material compact disc be in the CD-ROM drive. The videos can also be started directly from the Web page on the Supplemental Material compact disc.

▸ To assign the Log on locally user right to the Everyone group

1. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **User Manager for Domains**.

   The User Manager for Domains window appears.

2. On the **Policies** menu, click **User Rights**.

   The **User Rights Policy** dialog box appears.

3. In the **Right** box, click **Log on locally**, and then click **Add**.

   The **Add Users and Groups** dialog box for your domain appears.

4. Under **Names**, click **Everyone**, and then click **Add**.

   The Everyone group appears under **Add Names**.

5. Click **OK** to return to the **User Rights Policy** dialog box.

   The Everyone group appears under **Grant To**.

6. Click **OK** to apply your changes and to return to the User Manager for Domains window.

7. On the **User** menu, click **Exit**.

▸ To create a user account named User1 with a password of secret

- Click the **Start** button, click **Run**, and then in the **Open** box, type *drive*:**\labfiles\chapter1.cmd** (where *drive* is the drive letter that you specified when you ran the Setup.exe file to install the self-paced training files).

▸ To share the Users and Profiles folders

1. Click the **Start** button, point to **Programs**, and then click **Command Prompt**.

2. Type **net share users=***drive*:**\labfiles\users** and then press ENTER (where *drive* is the drive letter that you specified when you ran the Setup.exe file to install the self-paced training files).

   A message appears stating that "Users" was shared successfully.

3. Type **net share profiles=***drive*:**\labfiles\profiles** and then press ENTER (where *drive* is the drive letter that you specified when you ran the Setup.exe file to install the self-paced training files).

   A message appears stating that "Profiles" was shared successfully.

4. Close the Command Prompt window.

▸ To install Internet Explorer 3.*x*

1. In Windows NT Explorer, expand the IE_Setup folder on the Supplemental Material compact disc, and then double-click Msie30.exe.
2. When prompted to continue, click **Yes**.

   The **Internet Explorer License Agreement** dialog box appears.
3. Read through the license agreement, and then click **I Agree** to accept its terms.

   The Setup program copies files to your hard disk.
4. When prompted to restart your computer, click **Yes**.
5. Once your computer has restarted, log on as Administrator.

▸ To install the Intel Video drivers required to play the videos

1. In Windows NT Explorer, expand the Videos\Codec\32bit folder on the Supplemental Material compact disc.
2. Double-click Setup.exe.

   A **Welcome** dialog box appears.
3. Click **Next**.

   The **Software License Agreement** dialog box appears.
4. Read through the agreement, and then click **Yes** to accept its terms.

   The **Select Components** dialog box appears. **Windows NT system** is selected.
5. Click **Next**.

   The files are copied to the *systemroot*\System32 folder.
6. When prompted, if you would like to read the README file, click **Yes**; otherwise, click **No**.
7. Close all windows.

▸ To set the color palette and desktop area for your monitor

Complete this procedure only if you did not configure this information during installation.

1. Right-click a blank area of your desktop, and then on the menu that appears, click **Properties**.
2. In the **Display Properties** dialog box, click the **Settings** tab.
3. Under **Color Palette**, click **256**.

4. Under **Desktop Area**, move the slider to **800 x 600** pixels (if it is supported), and then click **Test**.
5. When prompted to test the new settings, click **OK**.

   A bitmap appears for five seconds, and then you are asked if you saw the test bitmap properly.
6. If you did see the bitmap properly, click **Yes**, and then click **OK**. Otherwise, click **No** and reset your the desktop area to 640 x 480 pixels.

Cleanup Procedures

Use the following procedures to remove user accounts, group accounts, and files that are created specifically for use in the lessons in this book.

Removing User and Group Accounts

Most chapters use batch files (Chapter*x*.cmd, where *x* is the chapter number) to create user or group accounts necessary to complete the chapter lessons. Account names include the number of the corresponding chapter. For example, User1 is created for use in Chapter 1. User5 is created for use in Chapter 5. This was done so that chapters do not depend on the completion of other chapters and can be done out of sequence.

After you complete all of the lessons in a chapter, you may want to remove the accounts that you create in the "Before You Begin" section of each chapter. You can do this at any time—when you finish all of the lessons in a chapter or when you finish all of the chapters.

▸ **To remove accounts created at the beginning of a chapter**

1. Log on as Administrator.
2. Insert the Supplemental Material compact disc into the CD-ROM drive.
3. Start Windows NT Explorer, and expand the Cleanup folder.

   The following files appear:

   DeleteChapter1.cmd
   DeleteChapter3.cmd
   DeleteChapter4.cmd
   DeleteChapter5.cmd
   DeleteChapter6.cmd
   DeleteChapter7.cmd
   DeleteChapter8.cmd
   DeleteChapter9.cmd
   DeleteChapter10.cmd
   DeleteChapter11.cmd

4. Double-click the DeleteChapter*x*.cmd file (where *x* is the chapter number) that corresponds to the chapter.

Note The DeleteChapter*x*.cmd files only remove the account or accounts that are created by running the corresponding Chapter*x*.cmd files. They do not remove any user or group accounts that you created as part of a lesson.

Removing Self-Paced Training Files

If you want to remove all files and shortcuts that were created when you installed the self-paced training files, you use Add/Remove Programs in Control Panel.

▸ **To remove the self-paced training files**

1. Click the **Start** button, point to **Settings**, and then click **Control Panel.**

   The Control Panel window appears.

2. Double-click the Add/Remove Programs icon.

   The **Add/Remove Programs Properties** dialog box appears.

3. On the **Install/Uninstall** tab, click **Microsoft Windows NT Network Administration**, and then click **Add/Remove**.

   The **Microsoft Windows NT Network Administration Setup** dialog box appears.

4. Click **Remove All.**

   A message appears asking if you want to remove Windows NT Network Administration.

5. Click **Yes**.

   The **Network Administration Training** menu is removed from the **Programs** menu, and all related files are removed from your hard disk, including the LabFiles folder (which does not appear on the **Network Administration Training** menu).

6. When a message appears stating that the process has successfully completed, click **OK**.

7. Click **OK** to close the **Add/Remove Programs Properties** dialog box.

8. Close Control Panel.

The Microsoft Certified Professional Program

The Microsoft Certified Professional (MCP) program provides the best method to prove your command of current Microsoft products and technologies. Anyone who must prove his or her technical expertise with Microsoft products should consider the program, including systems engineers, product developers, support technicians, system and network administrators, consultants, and trainers.

The Four Certifications

The following table describes the four certifications, based on specific areas of technical expertise.

Certification	Description
Microsoft Certified Product Specialist (MCPS)	MCPSs demonstrate in-depth knowledge of at least one Microsoft operating system. Candidates may pass additional Microsoft certification exams to further qualify their skills with Microsoft BackOffice™ integrated family of server products, development tools, or desktop programs.
Microsoft Certified Systems Engineer (MCSE)	MCSEs are qualified to effectively plan, implement, maintain, and support information systems in a wide range of computing environments with Windows NT Server and Microsoft BackOffice products.
Microsoft Certified Solution Developer (MCSD)	MCSDs are qualified to design and develop custom business solutions with Microsoft development tools, technologies, and platforms, including Microsoft Office and Microsoft BackOffice.
Microsoft Certified Trainer (MCT)	MCTs are instructionally and technically qualified to deliver Microsoft Official Curriculum through Microsoft Authorized Technical Education Centers.

Certification Requirements

The certification requirements differ for each certification and are specific to the products and job functions addressed by the certification. To become a Microsoft Certified Professional, you must pass rigorous certification exams that provide a valid and reliable measure of technical proficiency and expertise.

The following table describes exam requirements.

Certification	Exam requirements
Microsoft Certified Product Specialist (MCPS)	Pass one operating system exam. In addition, individuals seeking to validate their expertise in a desktop program must pass the appropriate elective exam.
Microsoft Certified Systems Engineer (MCSE)	Pass four operating system exams and two elective exams.
Microsoft Certified Solution Developer (MCSD)	Pass two core technology exams and two elective exams.
Microsoft Certified Trainer (MCT)	Required to meet instructional and technical requirements specific to each Microsoft Official Curriculum course that they are certified to deliver.[1]

MCSE Track

This book supports the MCSE Windows NT 4.0 track. To complete this track, we recommend that you do the steps outlined in the following table.

Step	Pass this exam	Preparation
1	70–58, *Networking Essentials*	Course 683, *Networking Essentials—Self-Paced Training Kit*
2	*Administering Microsoft Windows NT 4.0* self-administered assessment	Course 803, *Administering Microsoft Windows NT 4.0*
3	70–67, *Implementing and Supporting Microsoft Windows NT Server 4.0* and any client exam[2], such as exam 70–73, *Implementing and Supporting Microsoft Windows NT Workstation 4.0* or exam 70–63, *Implementing and Supporting Microsoft Windows 95*	Course 803, *Administering Microsoft Windows NT 4.0* Course 687, *Supporting Windows NT Core Technologies* Course 564, *Microsoft Windows 95 Training—Self-Paced Training Kit*

[1] *Inside the United States and Canada, call (800) 636-7544 for more information on becoming a Microsoft Certified Trainer. Outside the United States and Canada, contact your local Microsoft subsidiary.*

[2] *For a complete list of client and elective exams, see the Microsoft Training and Certification Web site at http://www.microsoft.com/train_cert/ or the Certification section of the Web page provided on the Supplemental Material compact disc.*

(*continued*)

Step	Pass this exam	Preparation
4	70–68, *Implementing and Supporting Microsoft Windows NT Server 4.0 in the Enterprise*	Course 689, *Supporting Windows NT Server 4.0 Enterprise Technologies*
5	Two elective exams	Elective exams are available for the following: Microsoft SQL Server™, BackOffice Internet-related products, Microsoft SNA Server, Microsoft Exchange Server, Microsoft Systems Management Server, and TCP/IP.

Important Microsoft Official Curriculum (MOC) courses help you to prepare for Microsoft Certified Professional (MCP) exams. However, no one-to-one correlation exists between MOC courses and MCP exams.

Administering Microsoft Windows NT 4.0 Self-Administered Assessment

The *Administering Microsoft Windows NT 4.0* self-administered assessment is a computer-based test.

▸ To learn more about the assessment

- If you have completed the Setup procedures in "About This Book," see the Readme file located in the *drive*:\Program Files\Admin Training\Assess folder (where *drive* is the location that you specified for the installation of the self-paced training files).

  –or–

  If you have not completed the Setup procedures in "About This Book," see "Assessment" in the "Certification" section of the Supplemental Material compact disc.

▸ To start the assessment

- If you have completed the Setup procedures in "About This Book," in Windows NT Explorer, expand *drive*:\Program Files\Admin Training\Assess folder (where *drive* is the location that you specified for the installation of the self-paced training files), and then double-click Lnchtst.exe.

  –or–

  If you have not completed the Setup procedures in "About This Book," copy the Assess folder from the Supplemental Material compact disc to your hard disk, and then in the Assess folder, double-click Lnchtst.exe.

Note Passing this self-administered assessment does not satisfy any requirements for the Microsoft Certified Professional program, nor does performance on this test guarantee or directly correlate to the success that you may have on any Microsoft certification exam. Unlike the Microsoft certification exams, this assessment is not professionally validated. If you plan to pursue Microsoft certification, see the "Certification" section of the Web page included with this book.

CHAPTER 1

Introduction to Administering Windows NT

About This Chapter

This chapter provides you with a foundation of knowledge that is useful for all chapters in this book. It includes an overview of Microsoft® Windows NT® Server and Windows NT Workstation, describes the administrative differences between them in a workgroup and a domain, and discusses directory services, the Windows NT Server services that provide a single user logon, centralized administration, and access to domain resources. It also introduces you to the administrative tasks and tools that you will use throughout this book and the essential tasks that all users perform when using Windows NT.

The hands-on procedures guide you through Windows NT basics.

Before You Begin

To complete the lessons in this chapter, you must have completed the Setup procedures located in "About This Book."

Lesson 1: Introduction to Windows NT

Windows NT is a multipurpose network operating system that can act as both a client and a server in a network environment. Windows NT refers to two different products—Windows NT Workstation and Windows NT Server.

This lesson provides an overview of Windows NT Server and Windows NT Workstation and the key administrative differences between them.

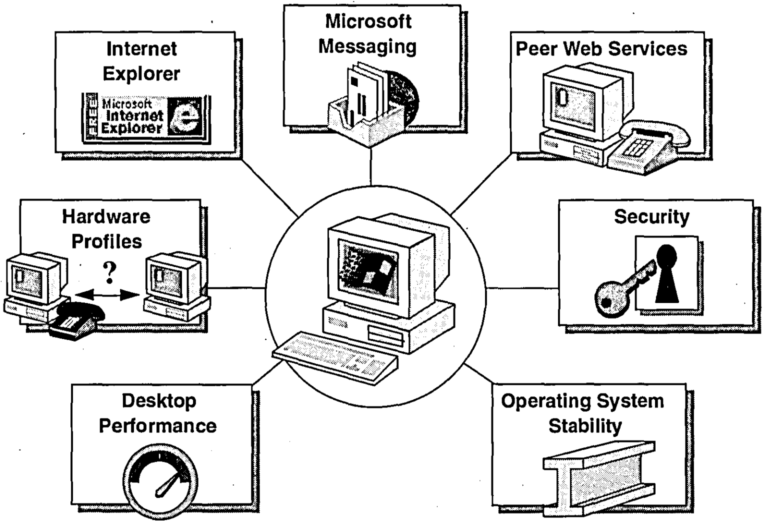
After this lesson, you will be able to:

- Explain the key differences between Microsoft Windows NT Workstation and Windows NT Server.
- Describe the difference between a workgroup model and a domain model, and understand what the administrative differences are between these two models.

Estimated lesson time: 10 minutes

What Is Windows NT Workstation?

Windows NT Workstation is optimized for use as a high performance, secure network client and corporate desktop operating system. Windows NT Workstation can be used alone as a desktop operating system, networked in a peer-to-peer workgroup environment, or used as a workstation in a Windows NT Server domain environment. Windows NT Workstation can be used with the Microsoft BackOffice™ family of products to access resources from all of the BackOffice products.

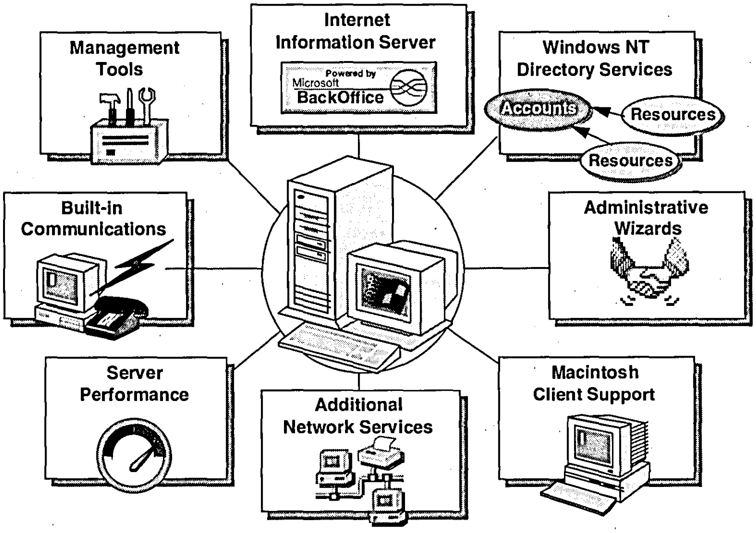


Windows NT Workstation offers the following advantages:

- *Desktop performance.* Supports preemptive multitasking for all programs. Windows NT Workstation supports multiple processors for true multitasking performance. For example, if you run a multithreaded program such as Microsoft Word, you can work on one document while another document prints.
- *Hardware profiles.* Creates and maintains a list of hardware configurations specific to a computer. For example, if you use a laptop computer and docking station at work, you can use a hardware profile to configure the laptop for use with the docking station. When you take the laptop computer home, you can use a different hardware profile with a configuration for dial-in networking.
- *Microsoft Internet Explorer.* Provides a fast and simple-to-use browser that is compatible with existing standards.
- *Microsoft messaging.* Receives and stores electronic mail, including files and objects created in other programs.
- *Peer Web services.* Provides a personal Web server, optimized to run on Windows NT Workstation version 4.0.
- *Security.* Provides local security for files, folders, printers, and other resources. Users must be authenticated by either the local computer or a domain controller in order to gain access to any resources on the computer or network.
- *Operating system stability.* Supports each program in its own memory address space. This means that malfunctioning programs will not affect other programs or the operating system.

What Is Windows NT Server?

Windows NT Server is optimized for use as a file, print, and application server that can handle tasks for organizations ranging from small workgroups to enterprise networks.



Windows NT Server offers the following advantages:

- *Server performance.* Windows NT Server version 4.0 is tuned for file, print, and application server performance. The retail version of Windows NT Server supports up to four processors in a symmetric multiprocessing environment. Original Equipment Manufacturers' (OEM) implementations of Windows NT Server support up to 32 processors in a symmetric multiprocessing environment.
- *Built-in communications.* Salespeople, home-based employees, traveling workers, and other mobile users connect to Windows NT Server 4.0 using Remote Access Service (RAS), a feature that lets remote users dial-in to the network. Windows NT provides support for 256 inbound RAS sessions.
- *Management tools.* Task Manager and Network Monitor simplify the day-to-day administration of your network server. Task Manager monitors programs, tasks, and key performance metrics of Windows NT Server 4.0, providing detailed information on each program and process running on the system. With this information, you can quickly terminate elements that are not responding, resulting in improved system reliability.

  Network Monitor examines network traffic to and from the server at the packet level and captures it for later analysis, making it easier to troubleshoot potential network problems.

- *Internet Information Server (IIS).* The integration of IIS with Windows NT Server 4.0 means that Web server installation and management are simply another part of the operating system. In addition, with IIS version 2.0 you can remotely administer your Web site from any Microsoft Windows®-based computer with a Web browser. IIS provides a fast, powerful, and secure platform for offering Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Gopher service.
- *Administrative Wizards.* Task-oriented Administrative Wizards make server management easier than ever. Wizards group the common server management tools such as User Manager for Domains and Server Manager, and walk you through the steps required to add users, create and manage groups of users, manage file and folder access for network clients, and so on.
- *Macintosh client support.* This feature provides file and print sharing services for Macintosh clients.
- *Additional network services.* These additional network services include multiprotocol routing (MPR), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Windows Internet Name Service (WINS).
- *Windows NT Directory Services.* A directory database provides a single network logon, a single point of administration, and the ability for users to access resources throughout the network.

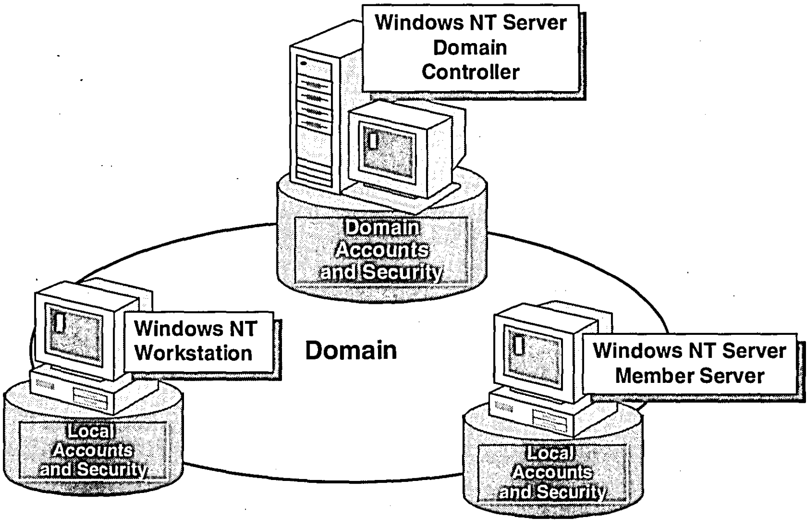
Administrative Differences

A Microsoft Windows NT–based network can be set up using either a domain model or a workgroup model. Both Windows NT Server and Windows NT Workstation can participate in either of these two models. The administrative differences between the two products depend on the model.

Domain Model

A domain model has at least one computer running Windows NT Server configured as a domain controller. A domain is a logical grouping of computers that share common security and user account information. This information is stored in the domain controller's master directory database.

Note Windows NT Server can also be configured as a member server (a non-domain controller). A member server does not validate domain logon attempts. It maintains a local directory database just as computers running Windows NT Workstation do.

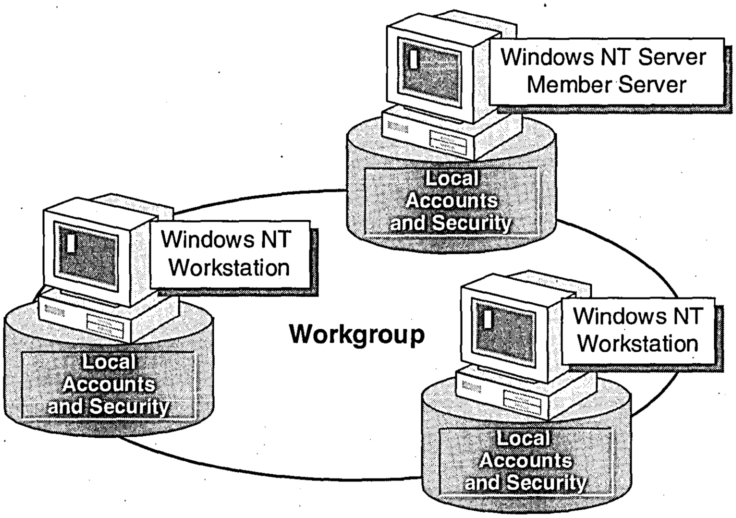


All computers running Windows NT maintain a directory database; however, it is the domain controller's master directory database that provides a central location for administering user accounts and resource security for the domain. In a domain, each user requires only one account and password to gain access to network resources. If a user changes his or her password, the change is automatically reflected throughout the domain.

Workgroup Model

A workgroup model is a Windows NT–based network that does not have a Windows NT Server domain controller. A workgroup is often referred to as a peer-to-peer network because all computers share files and printers as equals, or *peers*.

In a workgroup model, administration of user accounts and resource security is not central to any one computer. Instead, each computer running Windows NT Workstation or Windows NT Server (configured as a member server) maintains its own user accounts and resource security information in a local directory database. This means that user accounts are created on every computer that the user will access either locally or over the network.



In this model, resource administration tasks are distributed to each computer in the network. For example, each time a user changes his or her password, the user must change the password at every computer where that user has an account. To administer a computer in a workgroup, changes are made on each computer. This can be a time-intensive endeavor.

Lesson Summary

The following information summarizes the key points in this lesson:

- Windows NT Server is optimized for use as a file, print, and application server.
- Windows NT Workstation is optimized for use alone as a desktop operating system, as a networked computer in a peer-to-peer workgroup environment, or as a workstation in a Windows NT Server domain environment.
- A domain is a logical grouping of computers that share common security and user account information. The domain model provides centralized administration of user accounts and resource security.
- A workgroup is a network that does not have a Windows NT Server domain controller. Windows NT Workstation and Windows NT Server member servers are administered on an individual basis.

For more information on	See
New programs and features in Windows NT	Windows NT Help.
Windows NT procedures	Windows NT Help.
Windows NT Workstation	The Microsoft World Wide Web site at http://www.microsoft.com/ntworkstation/
Windows NT Server	The Microsoft World Wide Web site at http://www.microsoft.com/ntserver/
BackOffice family of products	The Microsoft World Wide Web site at http://www.microsoft.com/backoffice/

Lesson 2: Overview of Windows NT Directory Services

Directory services is one of the services provided by Windows NT Server. Directory services provides users with a single user name and password, and allows access to resources throughout the network. It provides administrators with the ability to view and manage users and network resources from any computer on the network. This lesson provides an instructional video on directory services, which focuses on a Windows NT environment and the role that user accounts play in it.

After this lesson, you will be able to:

- Describe the components in a Windows NT network and the role of user accounts in Windows NT Directory Services.
- Describe the function of primary and backup domain controllers, and the role of member servers.
- Explain the function of a trust relationship between domains.

Estimated lesson time: 10 minutes

The five minute video describes the components in a Windows NT network and the role of user accounts in Windows NT Directory Services. In addition, the video defines key terminology that is used throughout this book. The complete video script is available under "Course Materials" on the accompanying Supplemental Material compact disc.

► **To start the video from the Start menu**

1. Insert the Supplemental Material compact disc into the CD-ROM drive.
2. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Overview of Directory Services Video.**

► **To start the video from the compact disc**

1. Start Windows NT Explorer.
2. In the root of the Supplemental Material compact disc, double-click Open.htm.
3. Click the center of the screen to continue to the home page.
4. Click **Course Materials.**

5. Under **Contents**, click **Overview of Windows NT Directory Services.**
6. Follow the instructions in the text box to install the required DLL files and to start the video.

Note If you completed the Setup procedures described in "About This Book," or if you have run a video on this computer before, you do *not* need to install the DLL files.

▶ To review the video

The following study guide highlights the main points of the video. Complete the guide as you view the video, or use the guide as a follow-up test (recommended).

1. Name three benefits of Windows NT Server Directory Services.

   ____

   ____

2. Name the three Windows NT Server configurations.

   ____

   ____

3. How many primary domain controllers can there be in each domain? How many backup domain controllers?

   ____

   ____

4. How does a domain differ from a peer-to-peer network?

   ____

   ____

5. Name the logical link that combines domains into one administrative unit.

   ____

   ____

Lesson Summary

The following information summarizes the key points in this lesson:

- Directory services is one of the services provided by Windows NT Server.
- A domain is the administrative unit of directory services.
- A domain consists of one or more domain controllers that maintain a common directory database.
- Directory services provides users with a single user account and password. This means that users can log on to the domain from any computer on the network and have access to resources throughout it.
- Directory services also provides administrators with the ability to view and manage users and network resources from any computer on the network.

For more information on	See
Directory services	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.
Security	Chapter 5, "Securing Network Resources with Share Permissions" and Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.

Lesson 3: Logging On to Windows NT

Although resources are protected at several levels by different processes, overall access to a domain or a computer is protected by logon security. This lesson introduces the process of logging on to the domain or a local computer.

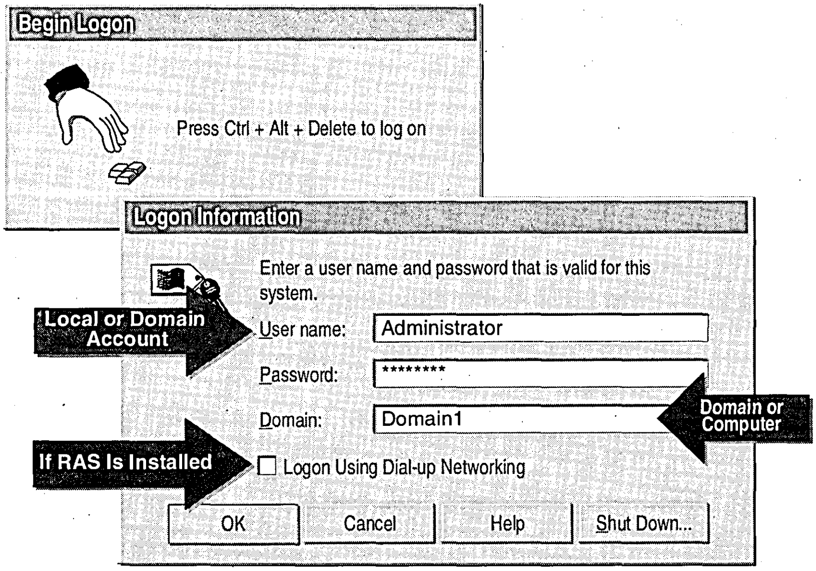
After this lesson, you will be able to:

- Log on to the domain or local computer.
- Describe the authentication process in a domain and workgroup.

Estimated lesson time: 10 minutes

To gain access to any part of the operating system, users must first identify themselves to the domain or the computer through the logon process.

Each time you start a computer running Windows NT, you are prompted to press CTRL+ALT+DELETE to log on.



Begin Logon

Press Ctrl + Alt + Delete to log on

Logon Information

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

User name: Administrator

Password: ********

Domain: Domain1

□ Logon Using Dial-up Networking

The following table describes the **Logon Information** dialog box options.

Option	Description
User name	Enter the unique user account that was assigned by an administrator. To log on to a domain, this account must reside in the directory database on domain controllers. To log on to the local computer, this account must reside in the directory database of the local computer.
Password	Enter the password assigned to the user name. Passwords are case-sensitive. The password appears on the screen as asterisks (*) to protect it from onlookers.
Domain	To log on to the domain, select the name of the domain. When a user logs on to the domain, the domain controller's directory database is checked for a valid match. The account is validated if the user name, password, and domain name match the domain controller's directory database. To log on to the local computer, select the name of the computer. When a user logs on to a local computer, the local computer's directory database is checked for a valid match. The account is validated if the user name, password, and computer name match the local directory database. A user can only log on to a local computer with a user name that resides in the local computer's directory database. Member servers and computers running Windows NT Workstation have a local Administrator and a Guest account by default. Other local accounts must be created.
Logon Using Dial-up Networking	When Remote Access Service (RAS) is installed, selecting this check box allows a user to log on to a remote network using RAS.
Shut Down	Closes all files, saves all operating system data, and prepares the computer to be safely turned off. On Windows NT Server, this button is disabled to prevent an unauthorized user from shutting down the server.

Logging On

To log on, the information that the user supplies in the **User name** and **Password** boxes must be either a valid domain user account or a local user account, depending on whether the user is logging on to the domain or the local computer.

In the **Domain** box, the user selects either the name of a domain or the name of the local computer to which he or she is logging on.

- If the computer is participating in a domain, the **Domain** box contains both the computer name and the domain name, as well as any domains trusted by the computer account's domain. The **Domain** box lists every domain where user accounts can be authenticated. To log on to a domain, the user selects the name of the domain where the user account resides.
- If the computer is participating in a workgroup, the **Domain** box contains only the local computer name. The user name and password must reside in the local computer's directory database. This is the only place where user accounts can be authenticated.

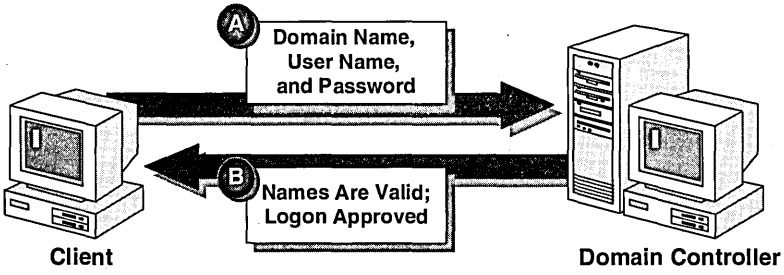
Important A user cannot log on to either the domain or the local computer from any computer running Windows NT Server, unless that user has been assigned the *Log on locally* user right by an administrator or has administrative privileges for the server. This feature helps to secure the server.

The Validation Process for a Domain Account

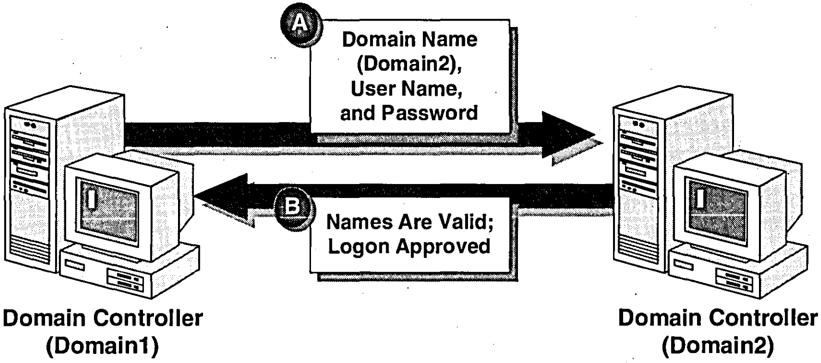
When the user clicks **OK**, the computer sends the domain name, user name, and password to a domain controller. The domain controller first checks the domain name, and then checks the user name and password against that domain's directory database.

One of the following three processes occurs:

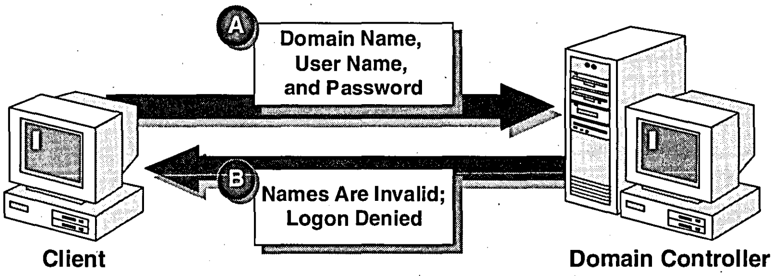
- If the domain name is correct and the user name and password match a domain account, the server notifies the computer that the logon is approved.


A
Domain Name, User Name, and Password
B
Names Are Valid; Logon Approved
Client
Domain Controller

- If the domain name is different and the domain controller recognizes the domain as a trusted domain, the domain controller passes the information to the appropriate domain, which authenticates the logon and sends the information back to the original domain controller.


A
Domain Name (Domain2), User Name, and Password
B
Names Are Valid; Logon Approved
Domain Controller (Domain1)
Domain Controller (Domain2)

- If the domain name is different and the domain controller does not recognize the domain, the controller denies domain access.


A
Domain Name, User Name, and Password
B
Names Are Invalid; Logon Denied
Client
Domain Controller

A Windows NT–based client keeps track of the last 10 successful logon attempts. This means that if the user account cannot be validated by a domain controller, but has been validated from that client within the last 10 previous successful logon attempts, the user will still have access to the local computer.

The Validation Process for a Local Account

When the user clicks **OK**, the computer checks the computer name, and then checks the user name and password against the local directory database. If the names match, the user account is validated and the user gains access to local resources. If the user account in not validated, the user does not gain access to the computer.

▸ **To log on to your domain**

1. Press CTRL+ALT+DELETE.

   The **Welcome** dialog box appears.

2. In the **User name** box, type **user1** (your domain user account name). By default, the account name that was last used to log on appears in this box. If this is the first time logging on, the default Administrator account appears in this box.
3. In the **Password** box, type **secret** (the password that is assigned to the account). Keep in mind that passwords are case-sensitive, and note that for security reasons, the password appears as asterisks to shield the password from onlookers.
4. In the **Domain** box, select your domain (where your account was created). By default the domain or computer name that was last used to log on appears in this box.
5. Click **OK**.

Using CTRL+ALT+DELETE to Prevent Trojan Horse Attacks

By requiring the user to press CTRL+ALT+DELETE to display the **Begin Logon** dialog box, Windows NT provides an important safeguard against Trojan horse programs. A Trojan horse program is an MS-DOS®-based program that tries to trick users into typing their user ID and password. The Trojan horse program then captures and saves the user's user name and password, giving the Trojan horse programmer access to the network.

Because most operating systems use CTRL+ALT+DELTE to restart a computer, it is difficult for programs to stay resident during a CTRL+ALT+DELETE keystroke operation. To ensure effective security, educate your users to always press CTRL+ALT+DELETE before logging on at a computer, even if the logon window already appears on the screen. The reason to always press CTRL+ALT+DELETE is to guarantee that you are providing your user name and password only to the operating system itself.

Lesson Summary

The following information summarizes the key points in this lesson:

- To log on, each user must supply a valid domain user account or a local user account.
- If a user supplies a valid domain user account, the user name and password are validated by the domain controller.
- If a user supplies a valid local user account, the user name and password are validated by the local computer.
- A user cannot log on from any computer running Windows NT Server unless that user has been assigned the Log on locally user right or the user has administrative privileges.

For more information on	See
User accounts	Chapter 2, "Working with User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 2, "Setting Up User Accounts," in this book.
User rights	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 2, "Working with User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
The Administrators group	Chapter 2, "Working with User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 3, "Setting Up Group Accounts," in this book.

Lesson 4: Windows NT Administrative Tasks and Tools

This lesson presents an overview of Windows NT administrative tasks and introduces the administrative tools. You will use many of these tools in the hands-on exercises that accompany the lessons throughout this book.

After this lesson, you will be able to:

- Describe the tasks required for administering Windows NT Workstation and Windows NT Server.
- Describe the functions of the Windows NT administrative tools for Windows NT Server and Windows NT Workstation.

Estimated lesson time: 10 minutes

Windows NT Administrative Tasks

Administering Windows NT involves both post-installation and day-to-day maintenance tasks. Administrative tasks for Windows NT Workstation and Windows NT Server are similar; however, the tools included with each product vary.

Administrative tasks can be grouped into the five categories described in the following table.

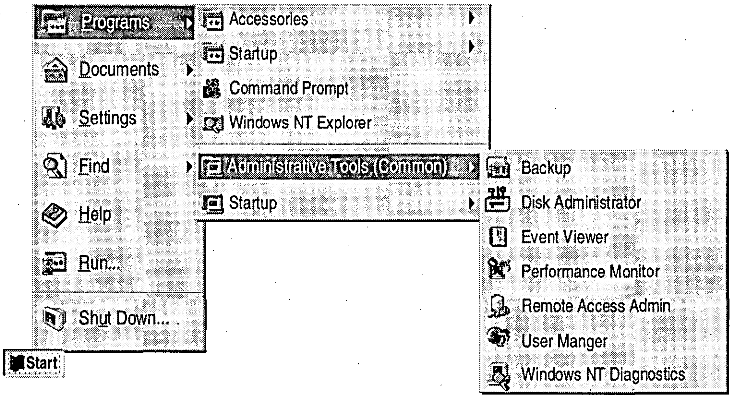
Administrative category	Specific tasks
User and group account administration	Planning, creating, and maintaining user and group accounts to ensure that each user can log on to the network and gain access to necessary resources.
Security administration	Planning, implementing, and enforcing a security policy to ensure protection of data and shared network resources, including folders, files, and printers.
Printer administration	Setting up local and network printers to ensure that users can connect to and use printer resources easily. Troubleshooting common printing problems.
Monitoring network events and resources	Planning and implementing a policy to audit network events so that you can find security breaches. Monitoring and controlling resource usage.
Backing up and restoring data	Planning, scheduling, and performing regular backups to ensure quick restoration of critical data.

The structure of this book maps to these five categories. The tasks in each category are described in detail in the corresponding chapters of this book.

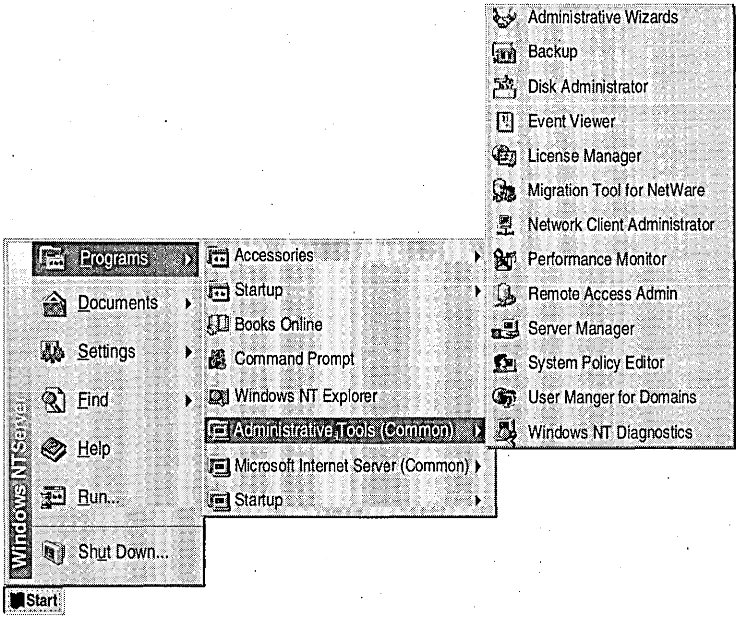
Windows NT Administrative Tools

Both Windows NT Server and Windows NT Workstation include administrative tools. The Windows NT Workstation administrative tools are only used to administer the local computer. The Windows NT Server Administrative Tools are used to administer any computer in the domain.

The following illustration shows the administrative tools that are installed on a computer running Windows NT Workstation.



The following illustration shows the administrative tools that are installed on a computer running Windows NT Server.



The following table describes the administrative tools that will be used throughout this book. Administrative Wizards, User Manager for Domains, and Server Manager are available on Windows NT Server only. User Manager is installed on Windows NT Workstation only. All other administrative tools are installed on computers running Windows NT Server and those running Windows NT Workstation.

Tool	Function
Administrative Wizards	The administrative wizards are Windows NT Server tools that guide you through tasks, such as creating user accounts, creating and modifying group accounts, setting permissions on files and folders, and setting up network printers.
User Manager for Domains	User Manager for Domains is a Windows NT Server tool that enables you to establish, delete, or disable domain user accounts. You can also set security policies and add user accounts to groups.
User Manager	User Manager is a Windows NT Workstation tool that enables you to establish, delete, or disable local user and group accounts.
Server Manager	Server Manager is a Windows NT Server tool that enables you to view and manage computers and domains.
Event Viewer	In Windows NT, an event is any significant occurrence in the system or in a program that requires you to be notified. Event Viewer notifies you and/or puts the event in a log. It provides information about errors, warnings, and the success or failure of a task, such as a user logon attempt.
Windows NT Diagnostics	Windows NT Diagnostics displays and prints system configuration information, such as data about memory, drives, and installed services.
Backup	Backup is a tool used to back up information to your local tape drive. Backing up your computer protects your data from accidental loss and media failures.

Using Windows NT Server Client-based Tools

You can install the Windows NT Server client-based tools on any computer running Microsoft Windows 95 or Windows NT Workstation. This gives an administrator the ability to perform domain administration from a client. This is useful in networks where the server is locked in a room and is not easily accessible.

The client-based tools are located on the Windows NT Server compact disc in the Clients\Srvtools folder.

- To install the tools on a computer running Windows NT Workstation, run Setup.bat from the Clients\Srvtools\Winnt folder, and then create a shortcut to each tool. The following tools that are useful for performing tasks covered in this book are installed in the *systemroot*\System32 folder.
  - Usrgmgr.exe (User Manager for Domains)
  - Srvmgr.exe (Server Manager)
- To install the tools on a computer running Windows 95, see the Readme.txt file in the Clients\Srvtools\Win95 folder.

▸ To open Administrative Tools

In this procedure, you view the Administrative Tools on a computer running Windows NT Server.

1. Click the **Start** button, point to **Programs**, and then point to **Administrative Tools.**

   Notice all of the tools in the Administrative Tools group. To learn more about each tool, click a tool, and then on the **Help** menu, click **Contents.**

2. Click **Administrative Wizards** to view the wizards.

   The following table describes the wizards.

This wizard	Is used to
Add User Accounts	Create new user accounts.
Group Management	Create and modify group accounts.
Managing File and Folder Access	Set permissions on files and folders.
Add Printer	Set up printers that are connected to your computer or are on a network.
Add/Remove Programs	Install or remove programs from your computer.
Install New Modem	Set up modems that are connected to your computer.
Network Client Administrator	Install or update network client.
License Compliance	Check licensing for installed programs.

3. Click **Close.**

Lesson Summary

The following information summarizes the key points in this lesson:

- The Windows NT Workstation administrative tools are only used to administer the local computer.
- The Windows NT Server administrative tools are used to administer any computer in the domain.
- Windows NT Server Administrative Tools (with the exception of the Administrative Wizards) can be installed from the Windows NT Server compact disc on any computer running Windows NT Workstation or Windows 95.

For more information on	See
Each tool in the Administrative Tools group	Help provided in each tool.
User Manager and User Manager for Domains	Chapter 2, "Working with User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*. Chapter 2, "Setting Up User Accounts," in this book. Chapter 3, "Setting Up Group Accounts," in this book.
Event Viewer	Chapter 9, "Auditing Resources and Events," in this book. Chapter 9, "Monitoring Events," in Microsoft Windows NT Server *Concepts and Planning*.
Server Manager	Chapter 4, "Administering User and Group Accounts," in this book. Chapter 10, "Monitoring Resources," in this book.
Windows NT Diagnostics	Chapter 10, "Monitoring Resources," in this book. Chapter 7, "Protecting Data," in Microsoft Windows NT Server *Concepts and Planning*.
Backup	Chapter 11, "Backing Up and Restoring Files," in this book. Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.
Installing client-based network administration tools	Chapter 11, "Managing Client Administration," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 5: The Windows NT Security Dialog Box

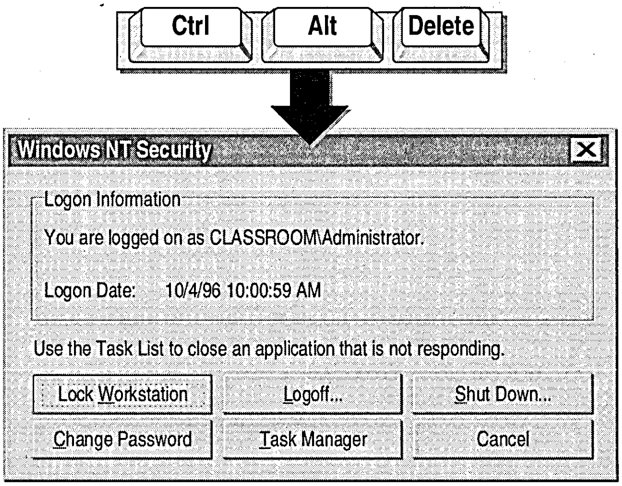
Once you are logged on, you can use the CTRL+ALT+DELETE key sequence, also referred to as the *secure attention sequence*, to access the **Windows NT Security** dialog box. You can use the **Windows NT Security** dialog box to perform key tasks.

After this lesson, you will be able to:

- Lock a workstation.
- Change your password.
- Use Task Manager.
- Log off Windows NT.
- Log on as a different user.
- Shut down the computer.

Estimated lesson time: 20 minutes

The **Windows NT Security** dialog box provides easy access to important security options. You will need to educate your users to use the features provided in this dialog box.



You are logged on as CLASSROOM\Administrator.

Logon Date: 10/4/96 10:00:59 AM

Use the Task List to close an application that is not responding.

The following table describes the **Windows NT Security** dialog box options.

Option	Function
Lock Workstation	Secures the computer without logging off. All programs remain running. Lock your workstation when leaving your workstation momentarily. The user who locks the workstation must unlock it by entering the valid password. If a user forgets the password, an administrator can unlock the workstation, log the user off the system, and then reassign a new password.
Change Password	Allows a user to change the user account password. The user must know the old password before a new one can be created. This prevents users from changing other users' passwords. This is the only way for users to change their passwords. Administrators should require users to change their passwords regularly and should set password restrictions as part of account policy.
Logoff	Logs off the current user, but leaves Windows NT running. This means that network users can still connect to and use shared resources on the computer. Always log off when you no longer need to use the computer.
Task Manager	Lists the current programs that are running. Task Manager gives you a summary of overall CPU and memory usage and a quick view of how each program, program component, or system process is using CPU and memory resources. Task Manager is also used to switch between programs and to stop a program that is not responding.
Shut Down	Closes all files, saves all operating system data, and prepares the computer to be safely turned off.
Cancel	Closes the **Windows NT Security** dialog box.

▶ To lock your workstation

1. Press CTRL+ALT+DELETE.

   The **Windows NT Security** dialog box appears.

2. Click **Lock Workstation.**

   The Workstation Locked window appears, indicating that the workstation is in use, but locked, and can only be opened by an administrator or by the authenticated user.

3. Press CTRL+ALT+DELETE.

   The **Unlock Workstation** dialog box appears.

4. In the **Password** box, enter your password, and then click **OK** to unlock your workstation.

▸ To change your password

1. Press CTRL+ALT+DELETE.

   The **Windows NT Security** dialog box appears.

2. Click **Change Password.**

   The **Change Password** dialog box appears.

   Notice that the **User name** and **Domain** boxes show the current user account and domain.

3. In the **Old Password** box, enter the current password.
4. In the **New Password** and **Confirm New Password** boxes, enter the new password, and then click **OK.**

   Your password change is confirmed.

5. Click **OK** to return to the **Windows NT Security** dialog box.
6. Click **Cancel.**

▸ To close a program from Task Manager

In this procedure, you open WordPad and then close it using Task Manager. Use this procedure anytime a program has stopped responding.

1. Click the **Start** button, point to **Programs**, point to **Accessories**, and then click **WordPad.**

   WordPad opens.

2. Press CTRL+ALT+DELETE.

   The **Windows NT Security** dialog box appears.

3. Click **Task Manager.**

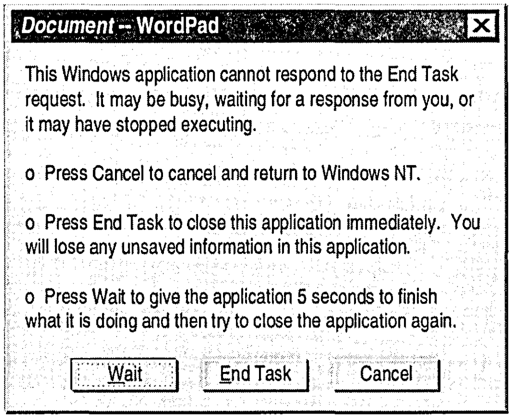
   The Windows NT Task Manager window appears.

4. Click the **Applications** tab, if it is not already the default.

   A list of open program appears.

5. Under **Task**, click **WordPad**, and then click **End Task**.

   If the program has stopped responding, the following message appears.



Document -- WordPad

This Windows application cannot respond to the End Task request. It may be busy, waiting for a response from you, or it may have stopped executing.

o Press Cancel to cancel and return to Windows NT.

o Press End Task to close this application immediately. You will lose any unsaved information in this application.

o Press Wait to give the application 5 seconds to finish what it is doing and then try to close the application again.

   If you did not get a chance to save changes to a document before your program stopped responding, click **Wait**. Clicking **Wait** gives the program five seconds to respond. If the program does respond, this message disappears and you are returned to your program. If your program still does not respond, click **End Task** to close the program.

   Important When Task Manager closes a program, all unsaved data is lost.

6. Exit Task Manager.

▸ **To log off**

1. Press CTRL+ALT+DELETE.

   The **Windows NT Security** dialog box appears.

2. Click **Logoff.**

   A message appears, stating that this will end your Windows NT session.

3. Click **OK.**

Note Another method to log off is to click the **Start** button, click **Shut Down**, and then click **Close all programs and log on as a different user**.

▸ To shut down your workstation

1. Press CTRL+ALT+DELETE.

   The **Windows NT Security** dialog box appears.

2. Click **Shut Down**.

   The **Shutdown Computer** dialog box appears. The default is **Shutdown and Restart**.

3. Click **OK** to shut down, or click **Cancel** to return to the **Windows NT Security** dialog box.

Lesson Summary

The following information summarizes the key points in this lesson:

- Use the CTRL+ALT+DELETE key sequence to gain access to the **Windows NT Security** dialog box.
- Using the **Windows NT Security** dialog box is the only way that users can change their passwords.
- Educate all users to lock their workstations anytime they leave them, to log off their workstations when they no longer need to use the computer, and to shut down their computers before turning them off.
- Use Task Manager as a troubleshooting tool anytime a program stops responding.

For more information on	**See**
Task Manager	Task Manager Help.

Best Practices

The following checklist provides best practices for ensuring security and safety. Educate your users to do the following:

☐ Always press CTRL+ALT+DELETE before logging on at a computer, even if the logon window already appears on the screen. This will ensure effective security and prevent Trojan horse attacks.

☐ Use the **Shut Down** command to safely prepare the computer to be turned off. This ensures that Windows NT will close all open files, save system settings, update the user environment settings, and avoid file corruption.

☐ Keep passwords absolutely secret. This ensures each user that no one else can access her computer and network resources by using her password.

☐ Enable the password protection on the computer's screen savers. This ensures that workstations will lock automatically when left unattended.

☐ Lock computers when stepping away from a workstation. The user's programs remain open, but the operating system remains locked until the user who locked the workstation unlocks it by entering a valid password.

☐ Log off computers when leaving a workstation. When a user logs off the system, all of the user's open files are closed. Windows NT remains running, however, so that another user can log on.

Additionally, for convenience:

☐ Install the Windows NT Server Administrative Tools (from the Clients\Srvtools folder on the Windows NT Server compact disc) on a client computer running the Windows NT Workstation or Windows 95 client, so that domain administration can be done from the client, allowing the server to be locked in a room for additional security.

Note If you want to remove the User1 user account that was created for use in this chapter only, log on as Administrator, and then double-click DeleteChapter1.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. What is the primary difference between Windows NT Server and Windows NT Workstation?

2. Which of the following describe a workgroup? (Circle all that apply.)
   a. A workgroup has only computers running Windows NT Workstation.
   b. A workgroup is a peer-to-peer network.
   c. A workgroup has at least one Windows NT Server domain controller.
   d. A workgroup does not have a Windows NT Server domain controller.
   e. Resource administration tasks are distributed to each computer in the network.

3. Which of the following describe a domain? (Circle all that apply.)
   a. A domain is a logical grouping of computers that share common security and user account information.
   b. A domain has at least one Windows NT Server member server.
   c. A domain has at least one Windows NT Server domain controller.
   d. A domain does not have a Windows NT Server domain controller.
   e. Resource administration is centralized at the domain controller.

4. Which of the following accurately describe differences between a domain controller and a member server? (Circle all that apply.)
   a. A domain controller is a computer running Windows NT Server that validates user logons for the domain.
   b. A domain controller maintains the master directory database for the domain.
   c. A member server is a computer running Windows NT Server that does not validate user logons for the domain.
   d. A member server is often used as an application server.

5. What key sequence is used to log on to the computer or a domain and to access the **Window NT Security** dialog box?

Answer Key

Procedure Answers

Page 11

▶ **To review the video**

1. Name three benefits of Windows NT Server Directory Services.

   Single user logon, universal access to resources, and centralized administration.

2. Name the three Windows NT Server configurations.

   Primary domain controller, backup domain controller, and member server.

3. How many primary domain controllers can there be in each domain? How many backup domain controllers?

   Each domain must have one and *only* one primary domain controller. A domain can have more than one backup domain controller.

4. How does a domain differ from a peer-to-peer network?

   In a domain, all domain controllers maintain a common directory database; therefore, a user can log on from any computer using a single user name and password. In a peer-to-peer network, each computer maintains its own directory database; therefore, a separate user account for each user must exist in each computer's directory database.

5. Name the logical link that combines domains into one administrative unit.

   A trust relationship, or trust.

Page 31

Review Answers

1. What is the primary difference between Windows NT Server and Windows NT Workstation?

   Windows NT Server is optimized for use as a file, print, and application server. Windows NT Workstation is optimized for use as a high-performance desktop operating system.

2. Which of the following describe a workgroup? (Circle all that apply.)

   Answers b, d, and e are correct.

3. Which of the following describe a domain? (Circle all that apply.)

   Answers a, c, and e are correct.

4. Which of the following accurately describe differences between a domain controller and a member server? (Circle all that apply.)

   All answers are correct.

5. What key sequence is used to log on to the computer or a domain and to access the **Window NT Security** dialog box?

   The correct key sequence is CTRL+ALT+DELETE.

CHAPTER 2

Setting Up User Accounts

About This Chapter

User accounts enable users to participate in a network and to access network resources. This chapter introduces you to the three types of user accounts and provides you with a planning strategy for implementing them. The hands-on procedures give you an opportunity to plan and create your own user accounts.

Before You Begin

To complete the lessons in this chapter, you must have:

- Viewed the *Overview of Directory Services* video referred to in Chapter 1, "Introduction to Administering Windows NT."
- Knowledge about the difference between a workgroup and a domain.
- Knowledge about the difference between a domain controller and a member server.
- Experience logging on and off Windows NT.

Lesson 1: Introduction to User Accounts

Windows NT security is based on the concept of user accounts. A user account is the user's unique credential that allows the user to access resources. This lesson provides an overview of user accounts.

After this lesson, you will be able to:

- Describe the types of user accounts.
- Describe the difference between a domain user account and a local user account.

Estimated lesson time: 10 minutes

Each person who will regularly use the network and participate in a domain, or who will log on to a local computer to access local resources, must have a user account. With user accounts, you can control how a user gains access to the domain or a local computer. For example, you can limit the number of hours a user can log on to the domain.

Types of User Accounts

There are three types of user accounts; one is the type of accounts that you create, and two are built-in user accounts that are created automatically when Windows NT Server or Windows NT Workstation is installed. The two built-in accounts are the Guest account and the Administrator account.

The following table describes the three types of user accounts.

Account	Description
Accounts that you create	A user account enables the user to log on to the local computer or domain and, with the appropriate permissions, allows access to network resources. User accounts contain information about the user, including the user's name and password.
Guest	The built-in Guest account is used to give occasional users the ability to log on and gain access to resources on the local computer. For example, an employee who needs to access the computer for a short time can use the Guest account. The Guest account is disabled by default.
Administrator	The built-in Administrator account is used to manage the overall computer and domain configuration and resources. The Administrator account is used when performing administrative tasks, such as creating or modifying user and group accounts, managing security policies, creating printers, and assigning permissions and rights to user accounts to access resources.

Where Accounts Are Created

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

- On computers running Windows NT Workstation, the account management tool is User Manager. It is used to manage the accounts of that computer only. Accounts created with User Manager are local accounts.
- On computers running Windows NT Server, the account management tool is User Manager for Domains. It is used to manage accounts on the local domain or on any computer, member server, or other domains to which you have access. Accounts created with User Manager for Domains can be local accounts or domain accounts.

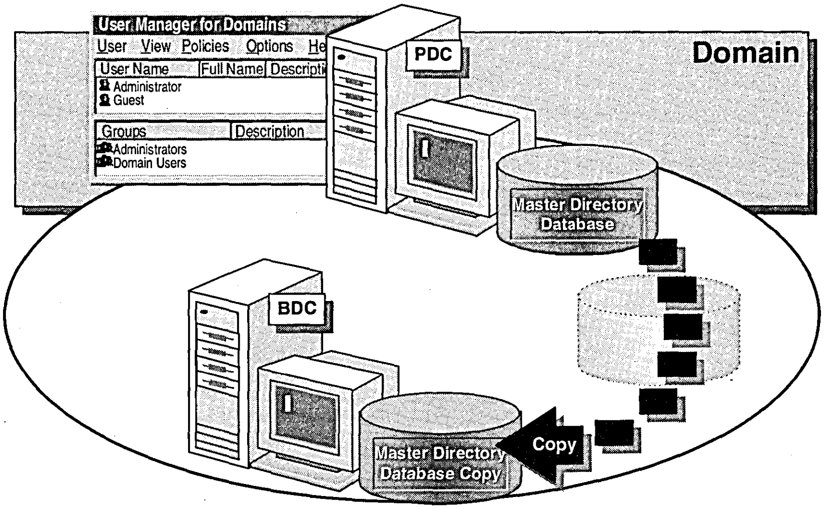
Domain User Account

A domain user account contains information that defines a user to the domain. With a domain user account, a user can log on to the domain and gain access to domain resources from any computer on the network using a single user account and password.

A domain user account is always created in User Manager for Domains. Although a domain user account can be created from any computer running User Manager for Domains, the account is always created in the master directory database on the primary domain controller (PDC).

A copy of the master directory database is stored on all backup domain controllers (BDCs). The copy is automatically synchronized every five minutes with the master directory database on the primary domain controller.

Create domain user accounts for all users.


User Manager for Domains
User View Policies Options He
User Name Full Name Descripti
Administrator
Guest
Groups Description
Administrators
Domain Users
PDC
Domain
Master Directory Database
BDC
Copy
Master Directory Database Copy

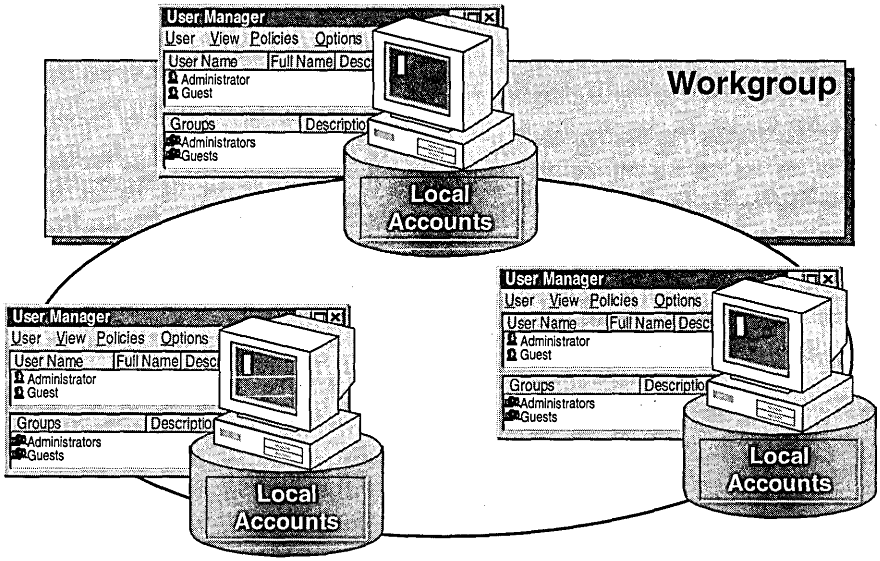
Note You can install User Manager for Domains on a computer running Windows NT Workstation or Windows® 95 by installing the Windows NT Server client-based administration tools.

Local User Account

A local user account contains information that defines a user to the local computer. With a local user account, a user can log on to and access local resources. To access resources on another computer, the user must have a separate user account on the other computer.

Although User Manager for Domains allows you to create accounts for the domain and for local computers, User Manager only allows you to create an account for the local computer.

Local user accounts should only be created within a workgroup, as shown in the following illustration.



Lesson Summary

The following information summarizes the key points in this lesson:

- Windows NT security is based on the concept of user accounts.
- The Administrator account is a built-in account on all computers running Windows NT. It is used for overall management of computer resources and configuration.
- The Guest account is a built-in account on all computers running Windows NT. It provides occasional users the ability to use local computer resources. It is disabled by default.
- A domain user account gives a user the ability to log on to and access domain resources from any computer on the network using a single user account and password.
- Create a domain user account for all users.
- A local user account gives a user the ability to log on to the local computer and access local resources. To access resources on another computer, the user must have a separate account on the other computer.
- Create local user accounts only in a workgroup environment.

For more information on	See
Creating user accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Installing client-based network administration tools	Chapter 11, "Managing Client Administration," in Microsoft Windows NT Server *Concepts and Planning*.

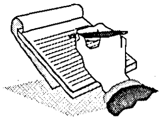
Lesson 2: Planning New User Accounts

Before you create user accounts, determine the requirements for each user based on the security level of your network. This lesson explores the strategies for creating new user accounts in networks with minimum, medium, and high levels of security.

After this lesson, you will be able to:

- Describe five elements of good user account planning.
- Plan a strategy for creating new user accounts.
- Explain how password requirements affect security levels.
- Describe the function and possible locations of a home folder.

Estimated lesson time: 30 minutes



Elements to Consider in Planning New User Accounts

To streamline the administration process, and to implement the most appropriate security measures for your organization, consider these elements in determining your planning strategy:

- *Naming convention.* Use a convention that ensures unique but consistent user account names.
- *Password requirements.* Select your password enforcement options, including whether a user can, or must, change his or her own password.
- *Logon hours.* Determine the hours that each user is allowed to log on.
- *Workstation restrictions.* Determine the computer names of the Windows NT computers that the user is permitted to work from. You can limit the choices. By default, the user can use any workstation.
- *Home folder location.* Determine location of home folders on the local computer or on a server for centralized backup and administration.

Naming Convention

A naming convention establishes how users will be identified on the network. A consistent naming convention makes it easy for you and your users to remember user names and locate them in lists.

To decide your naming convention, consider the following points:

- User names must be unique. Domain user accounts must be unique to the domain. Local user accounts must be unique to the local computer.
- User names can contain up to 20 uppercase or lowercase characters except for the following: " / \ [ ] : ; | = , + * ? < >. You can use a combination of special and alphanumeric characters.
- If you have a large number of users, establish a naming convention that accommodates employees with duplicate names. Two suggestions for handling duplicate names are:
  - Use the first name and the last initial, and then add additional letters from the last name to accommodate duplicate names. For example, if you have two users named Eric Lang, use EricL as one user name, and use EricLa for the other.
  - Add numbers to the user name. For example, EricL1 and EricL2.
- In large organizations, it is useful to identify temporary employees by their user account. For example, to identify temporary employees, use a "T" and a dash in front of the user name, as in, for example, T-EricL.

Password Requirements

The next element in planning new user accounts is identifying the password requirements. To protect access to the domain or a computer, every user account requires a password. This is especially important in networks with a medium to high level of security or in networks that are part of the Internet.

Consider the following guidelines for passwords:

- Always assign the Administrator account a password to prevent unauthorized users from using the account.
- Determine who will control the password. You may want to:
  - Assign users unique passwords and then prevent users from changing them. This gives control to administrators.
  - Assign users an initial password and then require users to change them the first time they log on. This way, the account is always protected and only individual users will know their passwords. This gives control to users.

- Determine whether an account needs to expire. For temporary employees, set their user accounts to expire when their contract or work assignment ends.
- Educate users on ways to protect their passwords by selecting passwords that deter computer hackers. Follow these guidelines:
  - Avoid using an obvious association, such as the name of a family member or pet.
  - Avoid using the user account name in any part of the password.
  - Use long passwords. Passwords can be up to 14 characters in length.
  - Use a combination of uppercase and lowercase characters. Passwords are case-sensitive. For example, the password *SeCret* is different from *secret.*
  - Include numbers in the password.

Logon Hours

By default, users can connect to a server 24 hours a day, 7 days a week. In a high-security network, restrict the hours when a user can log on to the network. For example, you may want to restrict hours in the following types of environments:

- Where logon hours are a condition for security certification, such as in a government network.
- Where there are multiple shifts; in this case, allow night shift workers to log on only during their working hours.

Workstation Restrictions

By default, any user with a valid account can log on to the network from any computer running Windows NT. In a high-security network where sensitive data is stored on the local computer, restrict which users can log on from that computer. For example, User1 can only log on from a computer named Computer1.

Home Folder Location

A home folder is a user's folder for storing files and programs. A home folder is useful because it provides a central location for a user's files, making it easy to locate files to back up or delete to clean up the hard disk. Each user should be assigned his or her own home folder.

If you create a home folder for a user, the home folder becomes the default folder whenever the user performs any of the following tasks within Windows NT or a program:

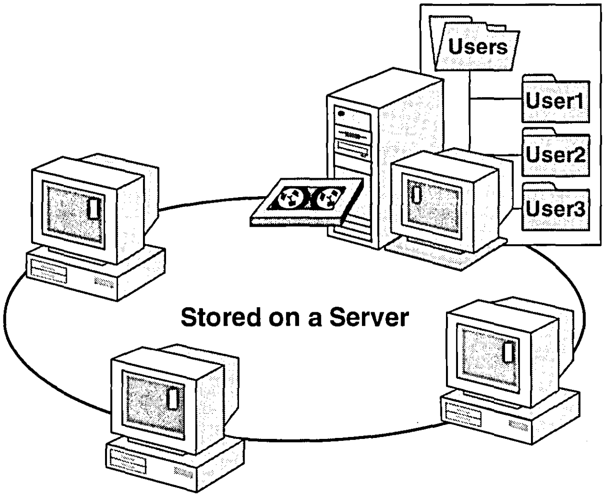
- Opens a file by clicking **Open** on the **File** menu.
- Saves a file by clicking **Save As** on the **File** menu.
- Starts a command prompt.

If you do not assign a home folder to a user, the default folder is Users\Default on the local computer.

A home folder can be stored on a network server or on a user's local computer.

Storing Home Folders on a Server

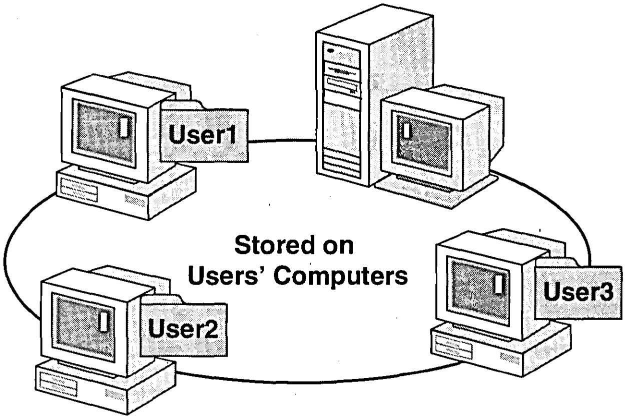
The following are considerations for storing home folders on a server.



- *Backup and restore.* Preventing the loss of data is your primary responsibility. It is much easier to ensure files are backed up when they are located in a central location on a server. If users' home folders are located on their local computers, you would need to perform regular backups on each computer.
- *Space on the server.* Is there enough hard disk space on the server to store users' data? Windows NT does not provide the ability to limit the amount of hard disk space used by each user.
- *Security.* In any network with sensitive data, it is easier to maintain security on data if it is in a central location.
- *Use RAS or share computers.* If users connect to the network using Remote Access Service (RAS), or if they share their computers, having a home folder on a server makes the users' data available from any location or computer.

Storing Home Folders on Users' Computers

If it is not important to you to have a central location for maintaining data, you can create a home folder for each user on his or her local computer. Having a home folder gives the user a familiar and central place for storing data. The following are considerations for storing home folders on a user's computer.



- *Space on the users' computers.* If users have space on their computers and it is not important to have centralized backup, locate home folders on users' computers.
- *Performance.* There is less network traffic if each user's home folder is located on the user's local computer.

▸ **To plan new user accounts**

Scenario: World Wide Importers hires approximately 300 new employees a year. Approximately 20 of those employees are temporary contract employees hired on a one-year contract; the others are permanent staff. Each employee requires his or her own user account.

As the administrator for World Wide Importers, you would set up the user accounts for their Quebec office. In this exercise, however, you will work with only 9 user accounts that are representative of the accounts that you would create for World Wide Importers.

You will record your planning strategies on the "User Accounts Planning Worksheet" located at the end of this lesson. Notice that the Description column in the "User Accounts Planning Worksheet" identifies the job title for each of the nine employees. After completing the exercise, turn to Appendix A, "Planning Worksheets," and compare your worksheet to the sample provided. (The sample presents only one set of possible answers. You may have planned your accounts differently.)

To complete the "User Accounts Planning Worksheet," you need to:

1. Specify a full name of your choice for each user, except where already noted. Record it under Full Name.
2. Define your naming convention. Then determine each user name based on your naming convention. Record it under User Account.
3. Under Description, the job title for each employee is already noted.
4. Determine each user's password requirements (for example, Change at next logon). Record it under Password Requirements.
5. Under Home Folder Location, record either "local computer" or "server."
6. Under Logon Hours, record the access hours for each user (for example, 24/7 for 24 hour access, 7 days per week).
7. Under Workstation Restrictions, record "Yes" if the user will be restricted, and "No," if not (Y/N).

Use the following criteria to make your decisions:

- Two employees have the same name. The vice president's name is Linda Mitchell; the customer service representative who works the night shift is also named Linda Mitchell.
- For permanent employees, allow each password to be controlled by the employee.
- For temporary employees, allow each password to be controlled by the administrator for tighter security.
- Each employee requires a home folder. All home folders need to be backed up each night.
- Permanent employees who work the night shift need access to the network from 6 P.M. to 6 A.M.
- Permanent employees who work the day shift require access to the network 24 hours a day, 7 days a week.
- Temporary employees should be able to log on to *only* their assigned computers and only from 8 A.M. to 5 P.M.

Lesson Summary

The following information summarizes the key points in this lesson:

- There are five key planning elements you need to consider before implementing user accounts: naming convention, password requirements, home folder location, logon hours, and workstation restrictions.
- Require passwords for all users.
- In medium-security and high-security networks, or if your network is on the Internet, require long passwords that use a combination of uppercase and lowercase characters, and numbers. Educate users to avoid obvious associations when they select a password.
- In high-security networks, restrict the hours that a user can log on to the network.
- If sensitive data is stored on a local computer, restrict who can log on to the network from that computer.
- Assign users their own home folders so that they have a familiar and central place to store data.
- Store home folders on a network server to simplify backing up user data and to maintain sensitive data centrally.

User Accounts Planning Worksheet

Naming Convention:____

Full Name	User Account	Description	Password Requirements	Home Folder Location	Logon Hours	Workstation Restrictions
Linda Mitchell		Vice president				
		Director of human resources				
		Sales manager				
		Sales representative				
Linda Mitchell		Customer service representative (night)				
		Customer service representative (day)				
		Accounting manager				
		Accountant				
		Temporary employee				

Lesson 3: Creating User Accounts

User accounts are created using User Manager or User Manager for Domains. To use either tool, you must have administrator privileges. This lesson explains the differences between User Manager and User Manager for Domains and takes you step-by-step through creating, deleting, and renaming user accounts.

After this lesson, you will be able to:

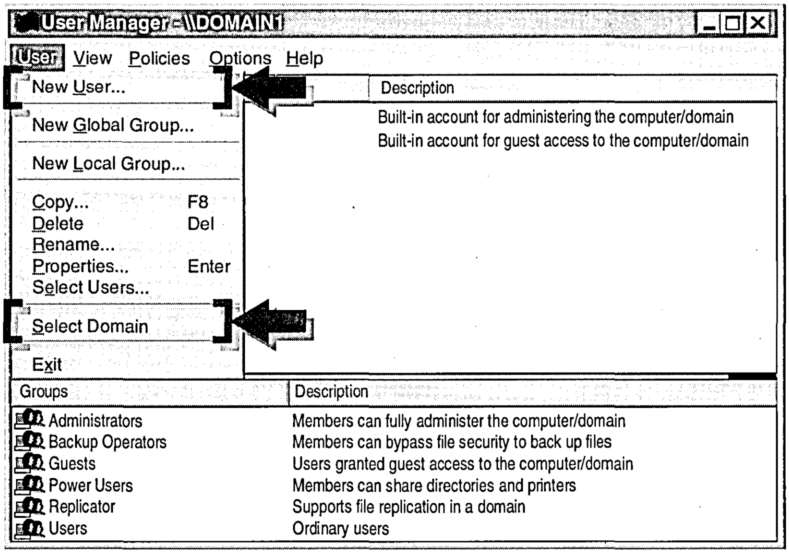
- Explain the difference between User Manager and User Manager for Domains.
- Create user accounts.
- Set password options.
- Create home folders.
- Set logon hours.
- Set workstation restrictions.
- Set account options.
- Grant dial-in permissions.
- Delete and rename user accounts.

Estimated lesson time: 40 minutes

User Manager vs. User Manager for Domains

User Manager and User Manager for Domains are very similar. In User Manager, you create, delete, or disable local user accounts on the local computer in a workgroup. In User Manager for Domains, you create, delete, or disable domain user accounts on the primary domain controller (PDC) or local user accounts on any computer in the domain.

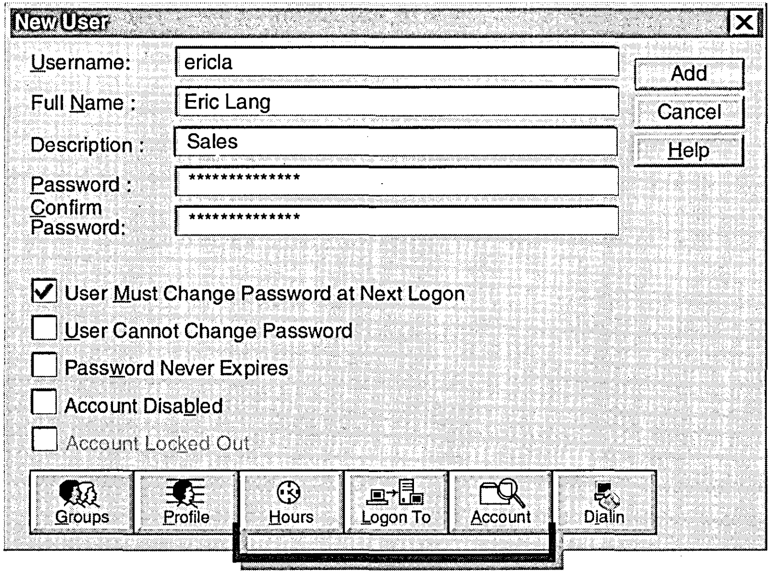
The following illustration shows User Manager for Domains. All user account options appear in User Manager, except for **Select Domain**. The **Select Domain** option allows an administrator to select a different domain or computer in which to create or manage user accounts.



	Description
	Built-in account for administering the computer/domain
	Built-in account for guest access to the computer/domain

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

The following **New User** dialog box is from User Manager for Domains. You can gain access to this dialog box by clicking **New User** on the **User** menu.



Username: ericla

Full Name : Eric Lang

Description : Sales

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

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

☑ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

□ Account Locked Out

User Manager for Domains only

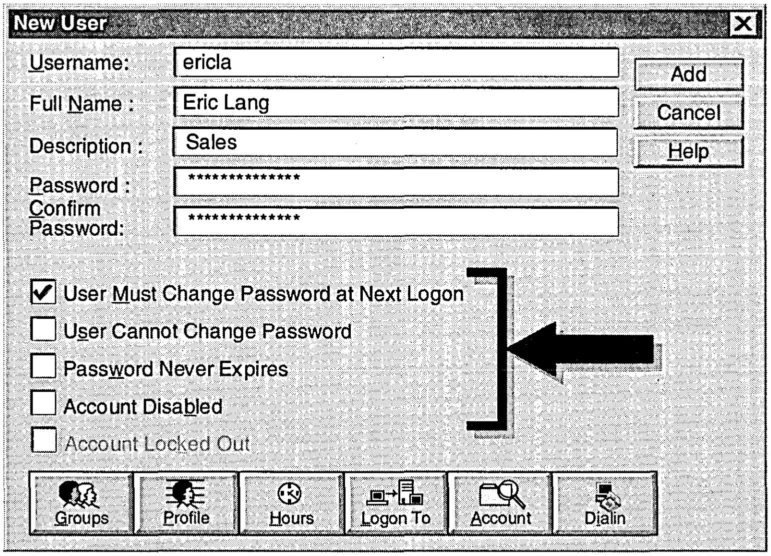
All options in the **New User** dialog box appear in User Manager except for the **Hours**, **Logon To**, and **Account** buttons. On domain user accounts, these buttons are used to set logon hours, restrict workstation access, and set an expiration on an account.

The following table describes the user name and password options in User Manager and User Manager for Domains.

In this box	Type
Username	A unique name based on your naming convention. This is the only required option.
Full Name	The complete name of the user, to determine which person belongs to an account. This is optional.
Description	A description that is useful for identifying users. It can be a job classification, a department, or an office location. This is optional.
Password	An initial password for the account. In medium-security to high-security networks, you should always assign an initial password to keep the account secure. By default, when the user logs on for the first time, he or she must change the password. Notice that the password is not displayed. Instead, once you enter the password, it is represented on the screen by a series of 14 asterisks, regardless of the length of the password.
Confirm Password	The password a second time to make sure that you typed the password correctly. This is required if you assign the password.

Setting Password Options

Whether or not you assign a password to a new user account, by default, the user will be required to assign a new password to the account the first time the user logs on. Password options are set in the **New User** dialog box.



New User

Username: ericla

Full Name : Eric Lang

Description : Sales

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

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

☑ User Must Change Password at Next Logon

☐ User Cannot Change Password

☐ Password Never Expires

☐ Account Disabled

☐ Account Locked Out

The following table describes the situations when you would select each password option.

Select this check box	If you
User Must Change Password at Next Logon (selected by default)	Want users to change their password the first time that they log on. This ensures that the user is the only person who knows his or her password. Even if you do not assign an initial password, you should require that users do this.
User Cannot Change Password	Have more than one person using the same user account (such as Guest) or want to maintain control over user passwords.
Password Never Expires	Have a user account for which you never want the password to change. For example, user accounts that will be used by Windows NT services (such as the Replicator service). This option overrides the selection of **User Must Change Password at Next Logon.**
Account Disabled	Want to temporarily prevent use of this account. For example, use when an employee takes a leave of absence.

Creating a Home Folder

To create home folders for users, you specify the name of the computer where the home folders will be located and names for the home folders.

The following checklist provides an overview of the tasks that you will need to do if you centralize home folders on a server. To create centralized home folders, do the following:

- ☐ On a server, create a folder named Users. This folder will be used to organize individual home folders. This task only needs to be done once.
- ☐ Share the folder and assign the Full Control permission to all users so that they can connect to it. This task only needs to be done once.

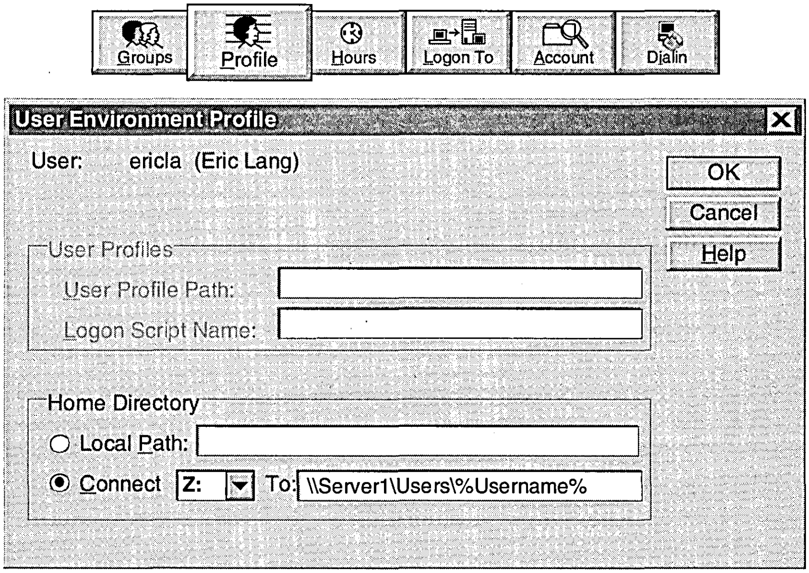
Note The Users folder was created and shared for you in the Setup procedures described in "About This Book." Sharing folders and assigning permissions is covered in more detail in Chapter 5, "Securing Network Resources with Share Permissions" and Chapter 6, "Securing Network Resources with NTFS Permissions."

- ☐ Specify a home folder name and location for a user account in the **User Environment Profile** dialog box.

  If you use %Username% in place of the home folder name, Windows NT will substitute %Username% with the user account name.

- ☐ Specify a network drive letter that will be used to connect to the user's home folder automatically when the user logs on.

The following **User Environment Profile** dialog box shows an example of how you specify a home folder location for a domain user account.



User: ericla (Eric Lang)

○ Local Path:

● Connect Z: To: \\Server1\Users\%Username%

Note In a workgroup, you must specify the home folder for a local user account while sitting at the local computer. In the **Local Path** box, enter the local path; for example, type **c:***folder_name* and Windows NT creates the folder that you specify.

▶ To create user accounts

In User Manager for Domains, you create the accounts that you planned in the hands-on procedure in the previous lesson, "Planning New User Accounts." If you did not complete the "User Accounts Planning Worksheet" from the lesson, use the sample plan provided in Appendix A, "Planning Worksheets."

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **User Manager for Domains**.
3. On the **User** menu, click **New User**.

   The **New User** dialog box appears.
4. Configure the following options based on the information from the "User Accounts Planning Worksheet" that you completed in the previous lesson or from the sample plan provided. For each user account on the worksheet, fill in the following options:
   - **Username**
   - **Full Name**
   - **Description**
   - **Password** (leave blank)
   - **Confirm Password**
5. Select the appropriate password options, and then click **Add**.

   The **New User** dialog box reappears and is cleared so that you can add another user.
6. Create the remaining user accounts.
7. When you have created all of the accounts on the "User Accounts Planning Worksheet," click **Close** to return to the User Manager window.

▶ To create a home folder

In this procedure, you create a home folder for a user account on the "User Accounts Planning Worksheet."

1. In the User Manager window, double-click a user account that you just created.

   The **User Properties** dialog box appears. Notice that this dialog box looks the same as the **New User** dialog box. The **User Properties** dialog box appears whenever you modify an existing user account (one that appears in the User Manager window).
2. Click **Profile.**

   The **User Environment Profile** dialog box appears.

3. Under **Home Directory**, click **Connect**.

   Notice that **Z:** appears in the **Connect** box. This is the drive letter that you will use to connect the user to the home folder upon logon.

4. In the **To** box, type \\computer_name\users\\%username% (where *computer_name* is the name of your computer).

   Remember, Users is the folder that was created and shared for you during the setup process.

5. Click **OK** to return to the **User Properties** dialog box.
6. Click **OK** to return to the User Manager window.

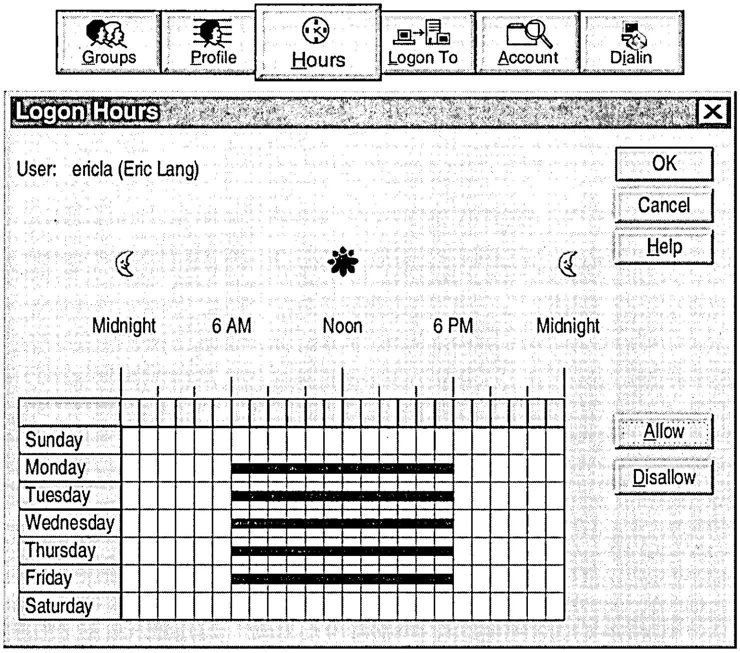
▸ **To assign home folders to multiple accounts at one time**

In this procedure, you create a home folder for the remaining user accounts on the "User Accounts Planning Worksheet."

1. In the User Manager window, select all of the remaining accounts that you created by holding down the CTRL key while you click each account.
2. On the **User** menu, click **Properties**.
3. In the **User Properties** dialog box, click **Profile**.
4. In the **Connect box**, click **Z:** so that drive Z will be used to connect to the user's home folder.
5. In the **To** box, type \\computer_name\users\\%username% (where *computer_name* is the name of your computer).
6. Click **OK** to return to the **User Properties** dialog box.
7. Click **OK** to return to the User Manager window.

Setting Logon Hours

When you set logon hours for a user account, you select the days of the week and the range of time for each day that you want to allow or disallow the user to have access the network.



User: ericla (Eric Lang)

Setting logon hours lets you control when a user can log on to the domain. Restricting logon hours limits the hours that users can explore the network, or the times that someone can try to break into the network.

Note A user who is connected to a network resource on the domain is not disconnected when the user's logon hours run out. However, the user will be unable to make any new connections.

▸ To specify logon hours

1. In the User Manager window, double-click a user account that requires logon hour restrictions (refer to the "User Accounts Planning Worksheet").
2. In the **User Properties** dialog box, click **Hours**.

   By default, all hours on all days are allowed. This is represented by a filled box for every hour of every day. A *filled* box indicates that the user is allowed to log on during that hour. An *empty* box indicates that the user cannot log on.
3. Position the mouse pointer on the rectangle on the day and hour that you want to disallow access. Press the mouse button, and drag the pointer through the last hour that you want to disallow. The area that you want to disallow should now be shaded.
4. Click **Disallow**. The area will still be shaded, but the line indicating hours of access should be gone.

   For more information about using the **Logon Hours** dialog box, click **Help**.
5. Repeat steps 3 and 4 for all of the times that you want the user to be disallowed.
6. Click **OK** to return to the **User Properties** dialog box.
7. Click **OK** to return to the User Manager window.
8. Restrict logon hours for any other users who only need to log on during specified times.

▸ To test logon hours

1. Log off and then attempt to log on as the user account that you created for the sales representative.
2. If prompted, change the password to **student**.

   Remember, passwords are case-sensitive.

   Were you able to successfully log on? Why or why not?

   ____

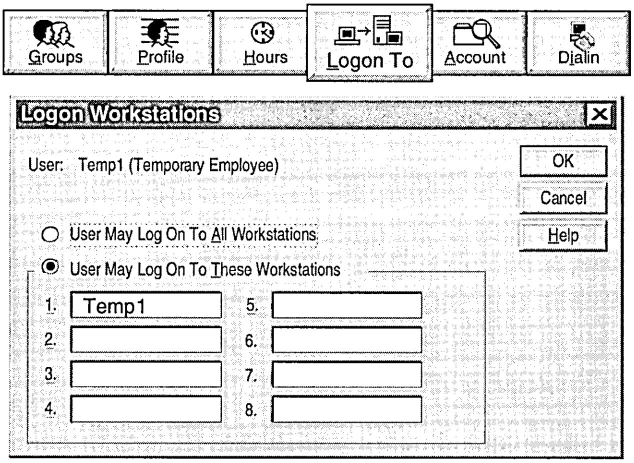
3. Log off and then attempt to log on as the user who is restricted to logging on during night time hours.
4. If prompted, change the password to **student**.

   Were you able to successfully log on? Why or why not?

   ____

Setting Workstation Restrictions

To set workstation restrictions, you can specify up to eight computer names from which a user can log on. Setting workstation access allows you to control which computers a user can use to log on to the domain. This prevents users from accessing another user's local data and can be used to require users to log on to workstations that are in an observed location. Set workstation restrictions in high-security networks.



User: Temp1 (Temporary Employee)

○ User May Log On To All Workstations

● User May Log On To These Workstations

1. Temp1

▸ To specify the workstation from which a user can log on

1. In the User Manager window, double-click the user account that you created for the temporary employee.
2. In the **User Properties** dialog box, click **Logon To**.

   The **Logon Workstations** dialog box appears. By default, each user account can log on from all computers.
3. Click **User May Log On To These Workstations**.
4. In the first box, type **Temp1** (the name of the computer from which the user is allowed to log on).
5. Click **OK** to return to the **User Properties** dialog box.
6. Click **OK** to return to the User Manager window.

▸ **To test workstation restrictions**

1. Log on to your computer as the user account that you created for the temporary employee.
2. If prompted, change the password to **student**.

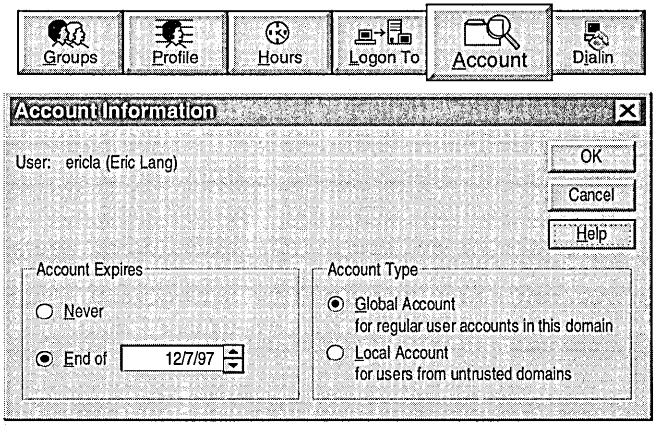
   You were restricted from logging on to the computer, because the temporary employee can only log on to a computer named Temp1.

Setting Account Options

The following two options can be set in the **Account Information** dialog box:

- *Account Expires.* Use this to set a date when the account will be automatically disabled. To specify when a user account expires, type the date of expiration. This is useful for temporary accounts for contractors or part-time employees.
- *Account Type.* Use this to create a local account for a user from an untrusted domain who needs access to a network resource in your domain. A local account can be used to connect to a resource over the network. It cannot be used to log on from a computer in the domain where it was created.

  You only use the **Local Account for users from untrusted domains** option under **Account Type** if you want to assign permission to a user who has an account in a domain that does not have the appropriate trust relationship to your domain.



Account Information

User: ericla (Eric Lang)

Account Expires
○ Never
● End of 12/7/97

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

▸ To set the account restriction

In this procedure, you configure the Temporary Employee user account to expire in 30 days.

1. In the User Manager window, double-click the user account that you created for the temporary employee (refer to the "User Accounts Planning Worksheet").
2. In the **User Properties** dialog box, click **Account.**

   The **Account Information** dialog box appears.

   Notice that the default option for **Account Expires** is **Never.**
3. Click **End of**, and then type the date that is 30 days from today.
4. Click **OK** to return to the **User Properties** dialog box.
5. Click **OK** to return to the User Manager window.

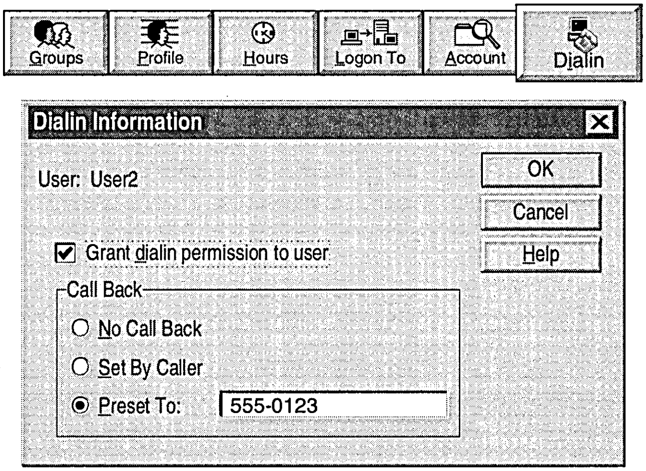
Granting Dial-in Permission

Windows NT dial-up networking client software gives a user access to server-based dial-in packages, such as Windows NT Server Remote Access Service (RAS). Once the connection is made from the RAS client to the RAS server, users at remote sites can use the network as if their computers were directly connected to the network.

Before a user can log on to the network using RAS, the user must have dial-in permission assigned to his or her user account.

Note Additionally, the Remote Access Service must already be installed and configured on the server, and the client must already be configured for dial-up networking.

You can specify an option for the RAS server to call the dial-in user back. The RAS server can dial the number specified by the user so that the company is billed for the call. Or, the RAS server can dial a number that you specify, which restricts the user to a specific dial-in location.



User: User2

☑ Grant dialin permission to user

Call Back

○ No Call Back

○ Set By Caller

● Preset To: 555-0123

The following table describes the **Dialin Information** dialog box options.

Option	Description
No Call Back	When selected, the RAS server will not call back the user, and the user will incur the telephone charges for the session. This is the default.
Set By Caller	When selected, lets the user specify a telephone number so that the RAS server can call the user back. This means that the organization that owns the RAS server will incur the telephone charges for the session.
Preset To	When selected, lets you specify a telephone number that the RAS server will use to call back the user. This reduces the risk of an unauthorized person using the user's account, because the user must be at the specified phone number in order to connect to the RAS server. In high-security networks, use this option and restrict users to dialing in from only one telephone number.

▶ **To grant dial-in permission**

In this procedure, you grant dial-in permission for the Accounting Manager who requires dial-in privileges from home.

1. In the User Manager window, double-click the user account that you created for the accounting manager (refer to the "User Accounts Planning Worksheet").
2. In the **User Properties** dialog box, click **Dialin.**

   The **Dialin Permission** dialog box appears.
3. Select the **Grant dialin permission to user** check box.
4. Click **OK** to return to the **User Properties** dialog box.
5. Click **OK** to return to the User Manager window.

Deleting and Renaming User Accounts

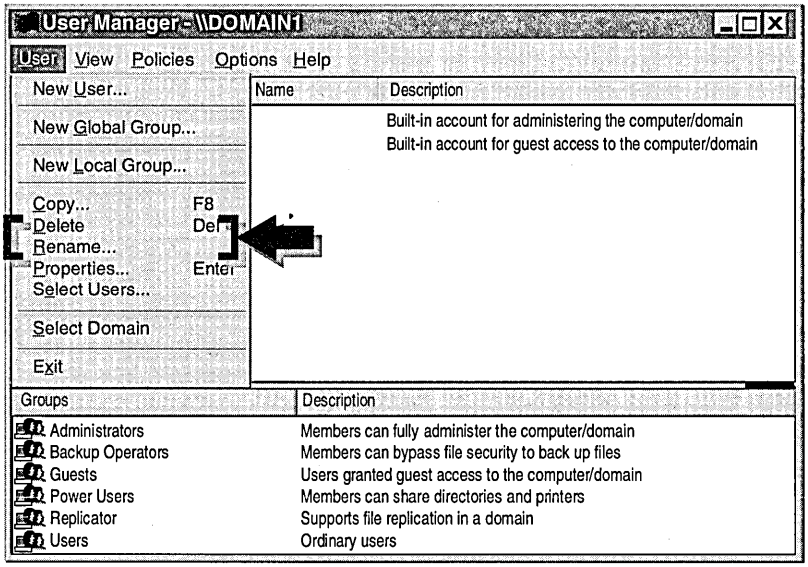
In Windows NT, every account is assigned a unique security identifier (SID) when the account is first created. A SID is a unique number that identifies the account. Internal processes in Windows NT refer to an account's SID rather than the account's user or group name.

Deleting an account permanently removes the account and the permissions and rights associated with it. For example, if you create an account, delete it, and then create an account with the same user name, the new account will not have the rights or permissions previously granted to the old account because the accounts have different SID numbers.

Renaming an account retains the permissions and rights associated with it because the SID was not deleted.

The following table describes the situations in which you should delete or rename an account.

Do this	When
Rename an account	You want to retain all rights, permissions, and group memberships for the account for a different user. For example, when a new employee replaces another employee, rename the user account and have the new employee change his or her password when he or she first logs on.
Delete an account	The account is no longer needed. When an account is deleted, all of the account information is lost. This information includes account properties, rights, permissions, and group memberships. The Administrator and Guest accounts cannot be deleted.



Name	Description
	Built-in account for administering the computer/domain
	Built-in account for guest access to the computer/domain

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

▸ To rename a user account

In this procedure, you create a user account and then rename it.

1. Create a new user account named Temp2.
2. In the User Manager window, select Temp2.
3. On the **User** menu, click **Rename**.
4. In the **Change To** box, type **temp3** and then click **OK**.

   The User Manager window is updated immediately.

▸ To delete a user account

1. In the User Manager window, select Temp3.
2. Press the DELETE key or, on the **User** menu, click **Delete**.

   A message appears warning you that once the account is deleted, even recreating it will not make the resources available to the newly created account that were available to the account that you deleted.
3. Click **OK** to acknowledge the warning.

   A message appears asking if you want to delete the user.
4. Click **Yes** and the user account is deleted.

Lesson Summary

The following information summarizes the key points in this lesson:

- In User Manager, you create, delete, or disable local accounts on a local computer in a workgroup.
- In User Manager for Domains, you create, delete, or disable domain and local accounts on the primary domain controller.
- Assign an initial password to an account and then require the user to change the password the first time that they log on. This ensures that the account is protected and only the user knows the password.
- When you create home folders for users, you specify the drive to which the user will connect, the server name, and the share name. In place of the user name, use %Username% to automatically name the home folder after the user name.
- When you set logon hours for a user account, you specify the days of the week and the time range for each day that you want to allow or disallow a user to log on.
- When you set workstation restrictions for a user account, you can specify up to eight names of the computers from which a user can log on.
- When you set account options, you specify the expiration date of a user account or you specify that the account is a local account for users from untrusted domains.

For more information on	See
Creating user accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning.*
Trusted relationships between domains	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning.* Chapter 2, "Network Security and Domain Planning," in the *Networking Guide* of the *Microsoft Windows NT Server Resource Kit.*
Dial-up networking and Remote Access Service (RAS)	Chapter 7, "RAS Security," in the Microsoft Windows NT Server *Networking Supplement.*

Lesson 4: Creating User Profiles

User profiles are useful for configuring or managing a user's desktop environment. This lesson introduces user profiles and explains the differences between personal user profiles, which are profiles users can change, and mandatory user profiles, which are profiles that users cannot change.

After this lesson, you will be able to:

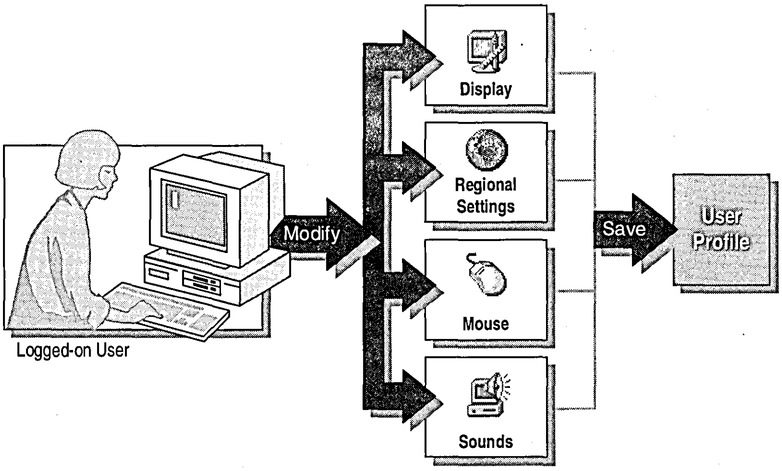
- Explain the difference between a roaming personal user profile and a mandatory user profile.
- Configure a local user profile.
- Create a roaming personal user profile.
- Create a roaming mandatory user profile.

Estimated lesson time: 30 minutes

User Profiles

In Windows NT, a user's computing environment is determined primarily by the user profile. Windows NT security requires a user profile for each account that has access to the system.

The user profile contains all user-definable settings for the work environment of a computer running Windows NT, including display, regional, mouse, and sounds settings, and network and printer connections.



When a user logs on for the first time from a Windows NT–based client, a default user profile is created for that user. All user-specific settings are automatically saved into the Profiles folder within the system root folder (typically C:\Winnt\Profiles\user_name).

A user profile can also be customized to restrict what users see in their interface and what tools they have available to use when they log on. For example, an administrator can remove the Administrative Tools folder to prevent a user from changing a configuration.

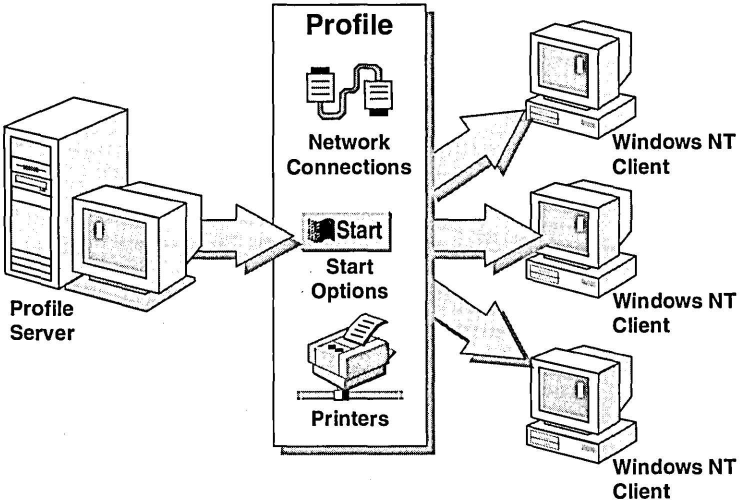
The following table describes the settings that are automatically saved in a user profile.

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

Note User profiles cannot be set for users who log on from LAN Manager, MS-DOS, Windows for Workgroups, or Windows 3.*x* clients. For these clients, you can write a logon script to configure the user's network and printer connections. For information on creating logon scripts, see Microsoft Windows NT Server *Concepts and Planning*.

Roaming User Profiles

Unlike a default user profile, roaming user profiles provide users with the same working environment, no matter which Windows NT–based computer a user logs on to. Roaming user profiles are stored centrally on a network server rather than on the user's local computer.



You can specify one of the following two roaming profiles for a user account:

- *Roaming personal user profile.* This is a user profile that a user can change. It is updated to include any changes made by the user when the user logs off. When the same user logs on again, the profile is loaded as it was last saved. If you use roaming personal user profiles, each user should be assigned his or her own profile.

  Roaming personal user profiles are named Ntuser.dat.

- *Roaming mandatory user profile.* This is a preconfigured user profile that users cannot change. One mandatory profile can be assigned to many users. This means that by changing one profile, you can change several desktop environments. You use this type of profile to assign common settings for all users who require identical desktop configurations—for example, bank tellers.

  Mandatory user profiles require an .man extension. You can make a personal profile mandatory by renaming it—for example, Ntuser.man.

Note Windows NT user profiles are not compatible with Windows 95 user profiles. Windows 95–based client profiles must be created on a computer running Windows 95.

Creating Roaming User Profiles

The following checklist provides an overview of the tasks required to implement roaming user profiles:

□ Create a template user profile with the appropriate configuration. You do this by creating a user account, and then configuring the appropriate desktop settings.

□ Create and share a folder named Profiles. (For this lesson, this step was done for you during the Setup process.) This will allow users to access the profiles from a remote computer.

□ Copy the template user profile to a network server and specify the users who are permitted to use the profile.

□ Specify the path to the profile for the user account in the **User Environment Profile** dialog box.

▸ To create a template user profile

In this procedure, you create a user account named Template Profile. This user account will be the model for a profile. Then, you configure the settings for the template profile.

1. In the **New User** dialog box, create a user account named **Template Profile** with no password. Clear the **User Must Change Password at Next Logon** check box.
2. Log on as **Template Profile**.

   A local user profile is automatically created for the Template Profile user on the local computer in the *drive:\systemroot*\Profiles folder.
3. Right-click anywhere on the desktop, and then on the shortcut menu, click **Properties**.

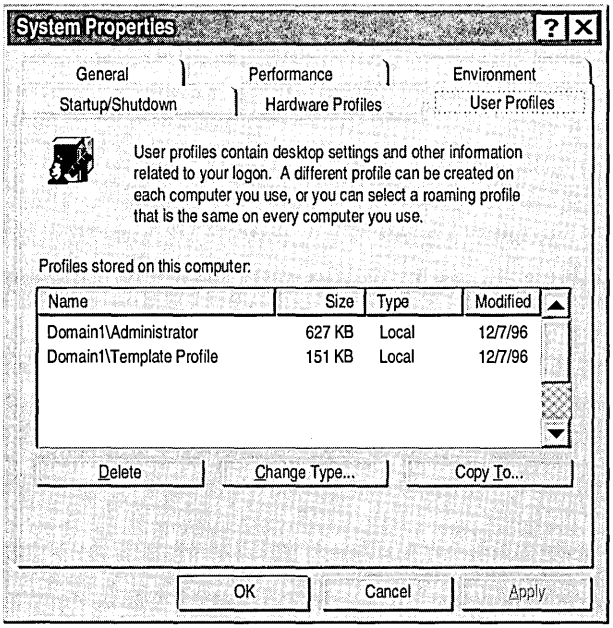
   The **Display Properties** dialog box appears.
4. Click **Appearance.**

   Notice the current color scheme.
5. In the **Color Schemes** box, select a different color scheme, and then click **OK**. The change will take effect immediately.
6. Log off and log on as the same user.

   Notice that the screen colors were those saved in the user's profile.

Copying the Profile to a Network Server

You copy a user profile using the System program in Control Panel. When you click the **User Profiles** tab of the **System Properties** dialog box, the default profiles appear for all users who have previously logged on to the computer.



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

Profiles stored on this computer:

Name	Size	Type	Modified
Domain1\Administrator	627 KB	Local	12/7/96
Domain1\Template Profile	151 KB	Local	12/7/96

▸ To copy the template user profile to a network server

In this procedure, you copy the Template Profile user profile to the server for User2. (This folder was created and shared if you completed the Setup procedures described in "About This Book.")

1. Log off and log on as Administrator.
2. In User Manager for Domains, create a user account named User2 with no password requirements.
3. Click the **Start** button, point to **Settings**, and then click **Control Panel**.
4. In Control Panel, double-click System.

   The **System Properties** dialog box appears.
5. Click the **User Profiles** tab.

   Notice that a user profile has been created for all users who have previously logged on to the computer, including a user profile named Template Profile.

6. Under **Profiles stored on this computer**, click **Template Profile**, and then click **Copy To**.

   The **Copy To** dialog box appears.

7. In the **Copy profile to** box, type \\computer_name\profiles\user2 (where *computer_name* is the name of your computer).

Important If you were to make the Template Profile mandatory, in the **Copy profile to** box, you would type \\computer_name\profiles (do not specify a user name).

▸ **To specify the users who are permitted to use the profile**

1. In the **Copy To** dialog box, under **Permitted to use**, click **Change**.

   The **Choose User** dialog box appears.

2. In the **List Names From** box, make sure the domain where your accounts reside appears, and then click **Show Users**.

3. In the **Names** box, click **User2**, and then click **Add**.

   Domain\User2 appears in the **Add Name** box.

4. Click **OK**.

   Domain\User2 appears as the user permitted to use this profile.

5. Click **OK**.

   A folder named after the user name you specified is created in the Profiles folder with all the desktop settings configured for the Template Profile user account.

6. In Windows NT Explorer, view Profiles\User2. Notice the folders for the desktop settings that are stored in the Template Profile folder and the file Ntuser.dat.

Important If you were to make the Template Profile mandatory, you would rename the Ntuser.dat file to Ntuser.man. If you did not specify a user name, this file would be located in the Profiles folder.

▸ **To delete the Template Profile user profile**

In this procedure, you delete the Template Profile user profile because it is no longer required. Only the profile on the server will be used.

1. On the **User Profiles** tab, under **Profiles stored on this computer**, click the profile that was created for the template, and then click **Delete**.

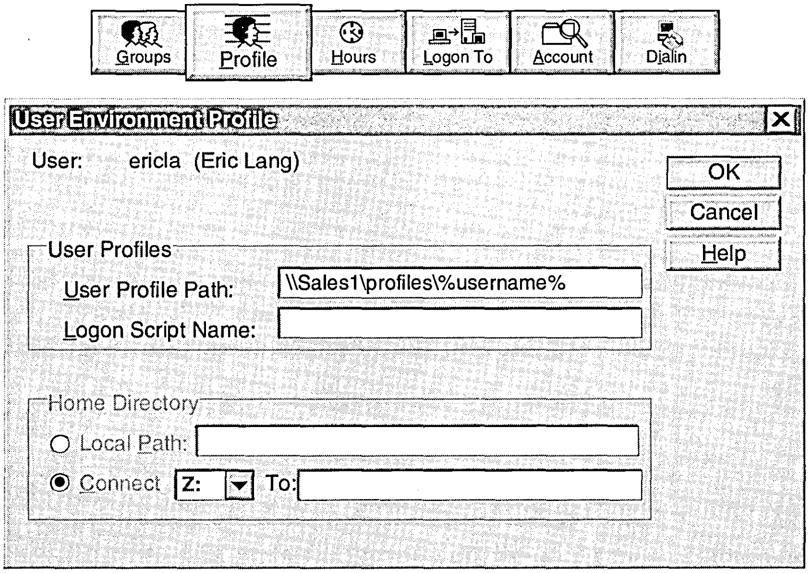
   A **Confirm Delete** message appears.

2. Click **Yes** to delete the local profile.

   The Template Profile user profile is deleted from the local computer.

Specifying the Path to the Roaming Profile

After you copy the roaming profile to a network server, specify the path to the profile for a user account in the **User Environment Profile** dialog box in User Manager for Domains.



User: ericla (Eric Lang)

User Profile Path: \\Sales1\profiles\%username%

Logon Script Name:

○ Local Path:

● Connect Z: To:

In the **User Profile Path** box, specify the server location of the user profile.

- If the profile is a roaming personal profile, enter the name of the server, the share name to the Profiles folder (in this lesson, the Profiles folder is shared as "Profiles"), and %Username%. If you use %Username%, Windows NT will substitute %Username% with the user account name.
- If the profile is a roaming mandatory profile, enter the name of the server, the share name to the Profiles folder, and the actual profile name. For example: \\Server1\Profiles\Ntuser.man.

Note If you have many users that require roaming profiles, you can specify the path to the profile for multiple user accounts at one time by doing the following: 1) In the User Manager window, select multiple accounts. 2) On the **User** menu, click **Properties**. 3) In the **User Properties** dialog box, click **Profile**.

▸ **To specify a path to the roaming profile**

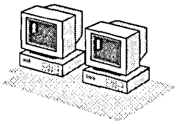
1. In the User Manager window, double-click User2.

   The **User Properties** dialog box appears.
2. In the **User Properties** dialog box, click **Profile**.
3. In the **User Profile Path** box, type \\*computer_name***profiles\%username%** (where *computer_name* is the name of your computer).
4. Click **OK** twice to apply your changes.
5. Exit User Manager for Domains and log off Windows NT.

▸ **To test the roaming profile**

- Log off and log on as User2.

  Notice that the screen colors are the same as the screen colors set for Template Profile.



▸ **To test the roaming profile from another computer**

If you have access to two computers on the same network, complete this procedure from the second computer.

1. Log on to the second computer as User2.
2. If a dialog box appears which provides profile options, click **Download.**

   Notice that the screen colors are the same as those set on the first computer because the roaming profile for the template user account is downloaded from the server and applied to the computer that the template user logs on to.
3. Log off.

▸ **To determine the type of profile assigned to a user**

1. Log on as an Administrator, and start Control Panel.
2. Double-click System, and then click **User Profiles**.

   Notice that the profile type for User2 is a roaming profile.
3. Exit all programs and log off Windows NT.

Lesson Summary

The following information summarizes the key points in this lesson:

- User profiles define a user's desktop environment and are created by default when a user logs on for the first time.
- A local user profile contains all user-definable settings controlling a user's desktop environment on the local computer.
- Roaming user profiles provide users with the same desktop environment from any Windows NT–based computer on a network.
- A roaming personal user profile is updated whenever a user makes a change to his or her desktop configuration. Each user has his or her own personal profile.
- A roaming mandatory user profile cannot be changed by users. One profile is assigned to many users.

For more information on	See
Logon scripts	Chapter 3, "Managing User Work Environments," in Microsoft Windows NT Server *Concepts and Planning*.
User profiles	Chapter 3, "Managing User Work Environments," in Microsoft Windows NT Server *Concepts and Planning*.
Creating Windows 95 user profiles	Chapter 15, "User Profiles and System Policies," in the *Microsoft Windows 95 Resource Kit.*

Best Practices

Review this checklist before you begin to create user accounts.

The following checklist provides best practices for setting up user accounts:

- □ To provide a greater degree of security, create a user account that you can use to perform non-administrative tasks; only log on as Administrator to perform administrative tasks.
- □ Only enable the Guest account in low-security networks and always assign it a password. This account is disabled by default.
- □ Always assign a password to an account.
- □ Always require new users to change their passwords the first time that they log on (this is the default setting). This will force users to protect their user account.
- □ In medium-security and high-security networks, create random initial passwords for all user accounts.
- □ Use roaming profiles if users frequently log on from different computers. This ensures that the user's familiar desktop configuration will always appears.
- □ Use the %Username% variable whenever you create a home folder or personal user profile. This variable will automatically be replaced with the user account name.
- □ If your server is on an Internet, rename the Administrator account. This will help to deter hackers.

Review

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

1. What is the difference between a domain user account and a local user account?

2. User Manager for Domains is (circle all that apply):

   a. Used to create and manage accounts on the local domain or on any computer, member server, or other domains to which you have access.

   b. Used to create and manage accounts on the local domain only.

   c. The account management tool on computers running Windows NT Server.

   d. Can be installed on a computer running Windows NT Workstation or Windows 95 using the client-based administration tools.

3. User Manager is (circle all that apply):

   a. Used to create and manage user accounts on the local computer only.

   b. The account management tool on computers running Windows NT Workstation and Windows NT Server.

   c. The account management tool on computers running Windows NT Workstation only.

4. In a high-security network, what can you do to make the Administrator and Guest accounts more secure?

5. What is the difference between a local and a roaming profile?

Answer Key

Procedure Answers

Page 44

▸ **To plan new user accounts**

Sample Answer:

User Account: One common naming convention uses first name, plus the first initial of the last name. When a duplicate first name exists, use additional characters from the last name. For example, use Lindam for the vice president, and Lindami for the night shift customer service representative.

Password Requirements: For all permanent employees, the administrator will select the User Must Change Password at Next Logon check box in User Manager for Domains. For all temporary contract employees, the administrator will select the User Cannot Change Password check box and will provide the password.

Home Folder Location: Home folders will be stored on the server.

Logon Hours: The night shift customer service representative's logon hours will be restricted to 6 P.M. through 6 A.M., 7 days a week. The temporary contract employee will be restricted to 8 A.M. to 5 P.M. All other employees will have 24-hour access, 7 days per week.

Workstation Restrictions: The temporary contract employee will only be able to log on at his or her own computer.

Page 56

▸ **To test logon hours**

2. Were you able to successfully log on? Why or why not?

   Yes, because the sales representative has access to the network 24 hours a day, 7 days a week.

4. Were you able to successfully log on?

   No, because night shift personnel are only allowed to log on between 6 P.M. and 6 A.M.

   -or-

   Yes, if the current time is between 6 P.M. and 6 A.M.

Page 75

Review Answers

1. What is the difference between a domain user account and a local user account?

   A domain user account defines a user to the domain. A user can log on to the domain and access domain resources from any computer on the network using a single user account and password.

   A local user account defines a user to the local computer only. To access resources on another computer, the user must have a separate user account on the other computer.

2. User Manager for Domains is (circle all that apply):

   Answers a, c, and d are correct.

3. User Manager is (circle all that apply):

   Answers a and c correct.

4. In a high-security network, what can you do to make the Administrator and Guest accounts more secure?

   Assign the Administrator account a password. Rename the Administrator account. The Guest account should remain disabled.

5. What is the difference between a local and a roaming profile?

   A local profile is created and stored on the computer where the user logs on and is only applied at that computer for the user. A roaming profile is stored in a shared folder on a network server and is applied at whichever computer the user logs on from.

CHAPTER 3

Setting Up Group Accounts

About This Chapter

Groups simplify administration by organizing user accounts into units. This chapter provides you with a groups planning strategy and procedures for creating groups. The hands-on procedures give you an opportunity to plan and implement local and global groups for a network.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- The knowledge and skills covered in Chapter 2, "Setting Up User Accounts."
- Knowledge about the difference between a workgroup and a domain, and between a domain controller and a member server.
- Nine user accounts created, named VicePresident3, Director3, SalesMgr3, SalesRep3, CustomerService3-A, CustomerService3-B, AccountingMgr3, Accountant3, and Temp3.

  Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter3.cmd to create these accounts.

Lesson 1: Introduction to Groups

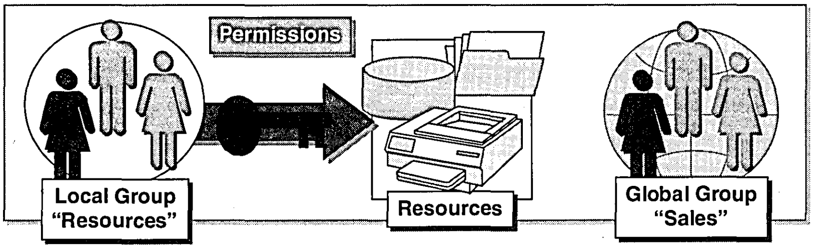
Group accounts are collections of user accounts that share similar needs. By organizing accounts into groups, you can greatly simplify administration tasks. This lesson introduces you to the basics about groups.

After this lesson, you will be able to:

- Explain the purpose of local and global groups.
- Compare and contrast local and global groups.
- Explain where local and global groups are created.

Estimated lesson time: 30 minutes

Group memberships govern much of what one can do on the network and on a particular computer. Adding a user account to a group makes the user a member and gives the user all the rights and permissions granted to the group. Group membership provides an easy way to assign permissions and user rights to sets of users at one time. For example, if several users need to read a file, the user accounts are added to a group. Permission to read the file is assigned just once, to the group, rather than to each user.



Permission and User Rights

Permissions are rules that regulate which users can use a resource, such as a folder, file, or printer. Because maintaining permissions for a group is easier than maintaining permissions for many user accounts, you generally want to use groups to manage access to resources.

User rights are rules that regulate which users can perform certain tasks on the system, such as creating a user account, logging on to the local computer, or shutting down a server.

A user can be a member of one or more groups. A user who is a member of more than one group possesses all user rights and permissions of all groups of which he or she is a member.

Local and Global Groups

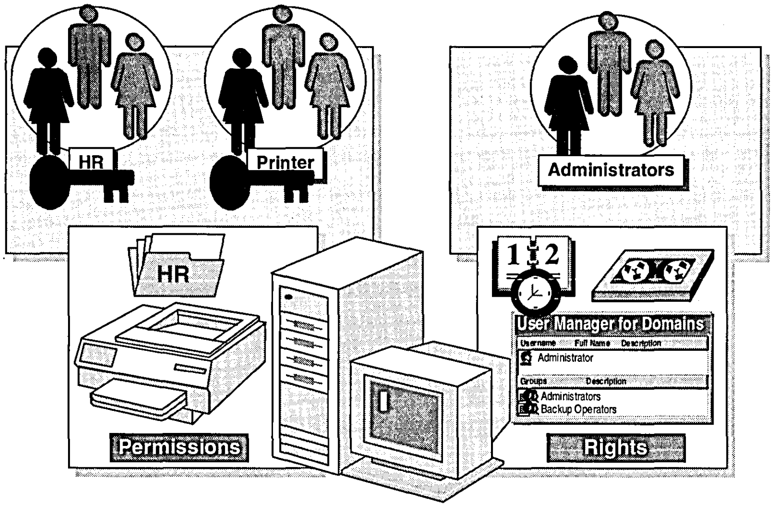
There are two types of groups, local and global.

Local Groups

Local groups are used to provide users with permission to access a network resource on the local computer. You assign resource permissions to a local group, and then add user accounts or global groups to the local group from one or more domains.

Local groups are also used to provide users with rights to perform system tasks, such as changing the system time on a computer, or backing up and restoring files. Windows NT includes several built-in local groups with pre-assigned user rights. For example, the built-in Administrators group gives members the rights to perform tasks such as creating user and group accounts, backing up data, and making changes to a Windows NT configuration.

The following illustration shows two local groups with permissions for network resources and the built-in local Administrators group with user rights to perform administrative tasks.

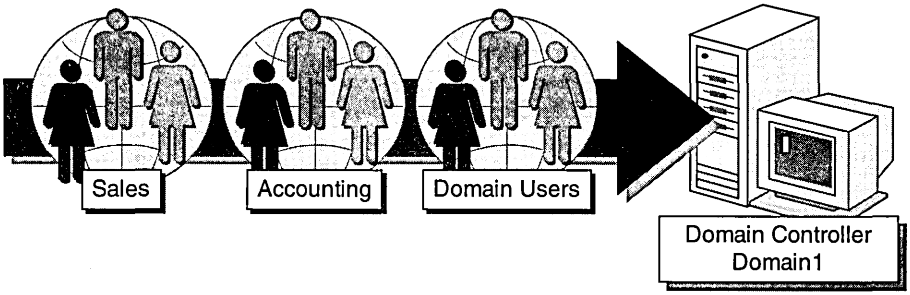


Local groups can contain user accounts and global groups from any domain (with the appropriate trust relationship). However, local groups cannot contain other local groups.

Global Groups

Global groups are used to organize domain user accounts, typically by function or geographical location. Global groups can contain only user accounts from the domain where the global group is created. They cannot contain local groups or other global groups.

The following illustration shows three global groups in Domain1.



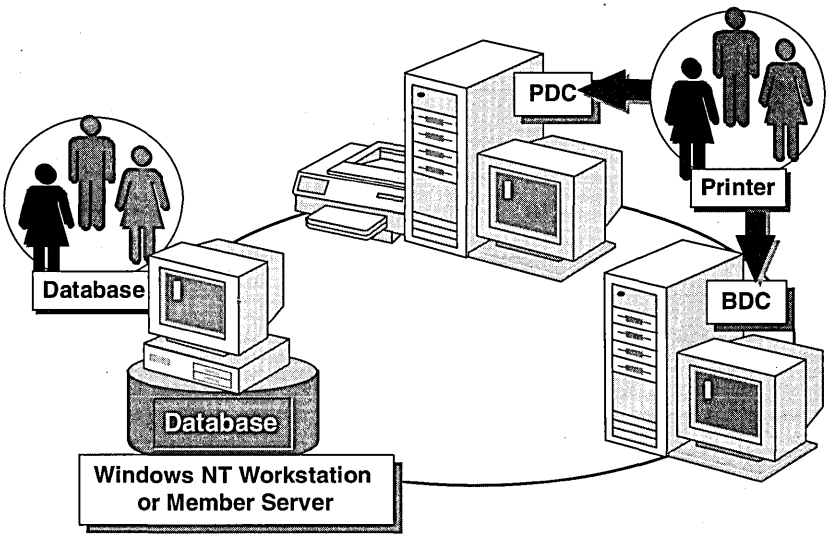
Although global groups can be assigned permissions to resources, use global groups only for grouping domain user accounts. Members of global groups obtain resource permissions when the global group is added to a local group.

Windows NT includes several built-in global groups—for example, the Domain Users group. By default, all domain user accounts are added to the Domain Users group. Unlike built-in local groups, built-in global groups do not have any inherent user rights.

Where Local Groups Are Created

If a resource resides on a member server or computer running Windows NT Workstation, the local group for the resource must be created on that computer. If the resource resides on any domain controller, the local group is created on the primary domain controller (PDC). The PDC will then provide its user account and security information to all other domain controllers in the domain.

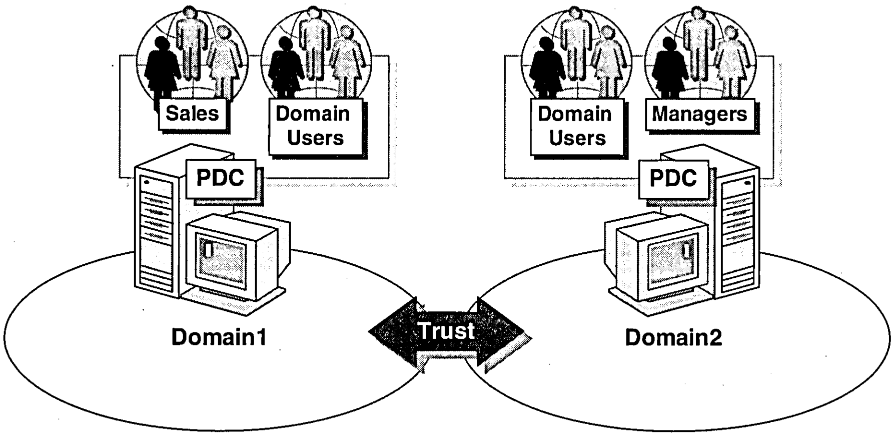
The following illustration shows the local group Database on the computer where the database resides, and the local group Printer on either the primary domain controller (PDC) or the backup domain controller (BDC), which allows access to the network printer located on the PDC.



For resources on computers running Windows NT Workstation and on member servers, you use User Manager or User Manager for Domains to create local groups. For resources on any domain controller, you create local groups on the PDC from any computer running User Manager for Domains.

Where Global Groups Are Created

Global groups are always created on the primary domain controller (PDC) in the domain where the user accounts reside. For example, global groups in Domain1 are created on the PDC in Domain1. Global groups in Domain2 are created on the PDC in Domain2.



Global groups can be created on the PDC from any computer running User Manager for Domains.

Video: Local and Global Groups

This six minute video defines local and global groups and explains how they are used in single-domain and multiple-domain networks. The complete video script is available under "Course Materials" on the accompanying Supplemental Material compact disc.

▸ **To start the video from the Start menu**

1. Insert the Supplemental Material compact disc into the CD-ROM drive.
2. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Local and Global Groups Video**.

▸ **To start the video from the compact disc**

1. Start Windows NT Explorer.
2. In the root of the Supplemental Material compact disc, double-click Open.htm.
3. Click the center of the screen to continue to the home page.
4. Click **Course Materials**.

5. Under **Contents**, click **Local and Global Groups Video**.
6. Follow the instructions in the text box to install the required DLL files and to start the video.

Note If you completed the Setup procedures located in "About This Book," or if you have run a video on this computer before, you do *not* need to install the DLL files.

▸ To review the video

The following study guide highlights the main points of the video. Complete the guide as you view the video, or use the guide as a follow-up test (recommended).

1. What is the purpose of a local group?

____

____

2. What is the purpose of a global group?

____

____

3. Where are local groups created?

____

____

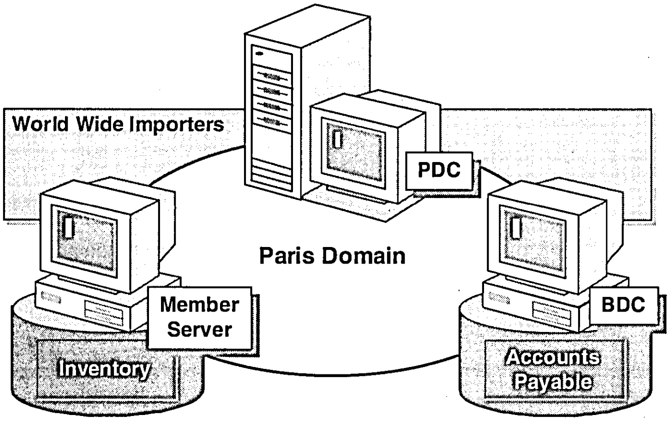
4. Where are global groups created?

____

____

Example: Using Groups in a Single-Domain Network

Scenario: The Paris office of World Wide Importers has a single-domain network with a PDC, a BDC, and a member server (non-domain controller). The BDC has an accounts payable database, and the member server has an inventory database. All users need access to both databases.



1. On which computer would you create a global group for organizing the user accounts? Why?

   ____

   ____

2. On which computer would you create a local group to provide users with access to the Accounts Payable database? Why?

   ____

   ____

3. On which computer would you create a local group to provide users with access to the Inventory database? Why?

   ____

   ____

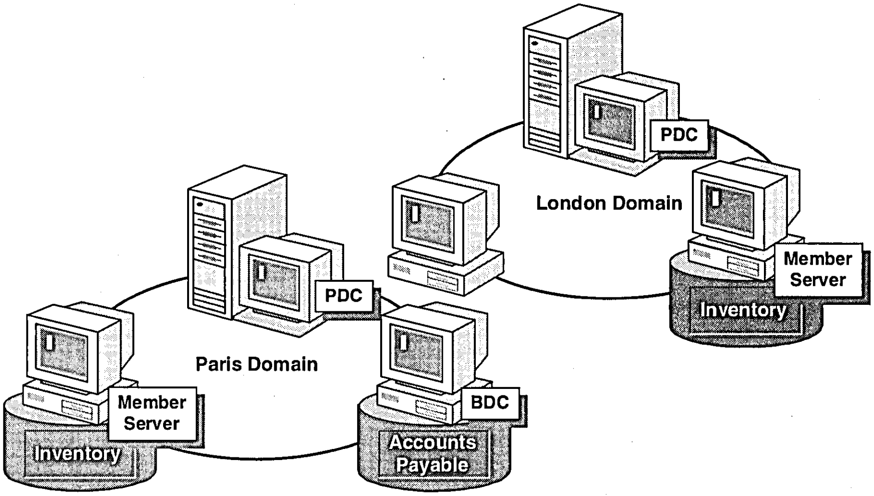
4. How would you give members of the global group access to both databases?

   ____

   ____

Example: Using Groups in a Multiple-Domain Network

Scenario: The Paris office of World Wide Importers has expanded its network to include a second domain for its London office. Both London and Paris maintain an Inventory database. All users in the London office need access to the Inventory database in the Paris domain, and all users in the Paris office need access to Inventory database in the London domain. The appropriate trust relationship exists between the two domains.



1. On which computers would you create a global group for organizing the user accounts? Why?

____

____

2. On which computers would you create a local group to provide users with access to the Inventory databases? Why?

____

____

3. How would you give members of the global groups that you just created in London and in Paris access to the Inventory databases in each other's domain?

____

____

Lesson Summary

The following information summarizes the key points in this lesson:

- Groups simplify administration by providing an easy way to assign permissions and grant user rights to sets of users.
- Local groups are used to provide users with permission to access a network resource on the local computer. You assign resource permissions to a local group, and then add user accounts or global groups to the local group from one or more domains.
- On computers running Windows NT Workstation or on member servers, local groups are created where the resource resides. On domain controllers, local groups are created on the PDC.
- Global groups are used to organize domain user accounts, typically by function or geographical location. Global groups can contain only user accounts from the domain where the global group is created.
- Global groups are created on the PDC.

For more information on	See
Group accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Assigning permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 5, "Securing Network Resources with Share Permissions," in this book.
	Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.
User rights	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 2: Planning a Group Strategy

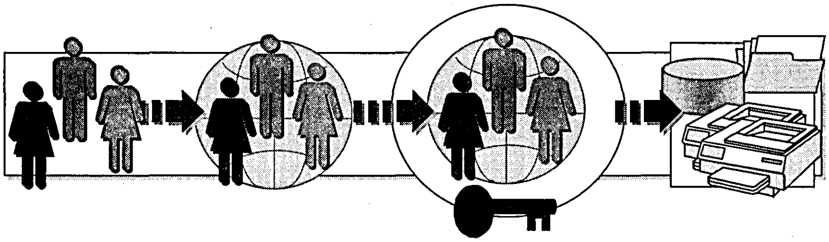
Having a strategy for implementing groups will simplify administration. This lesson presents the guidelines for implementing local and global groups.

After this lesson, you will be able to:

- Describe the steps of a sound implementation strategy.
- Plan a strategy for creating local and global groups in a multiple-domain network.

Estimated lesson time: 30 minutes

For better control over user and resource management, first organize users into global groups, and then add global groups to local groups.



To create groups, follow these general guidelines:

1. Logically organize domain users based on the common needs of your users. For example, if all sales personnel need access to a color printer and all managers need access to an employee records file, organize users by sales personnel and managers.
2. In each domain where user accounts reside, create a global group for each logical group of users. Then add the appropriate user accounts to the appropriate global groups.
3. Create local groups based on resource access needs. For example, if managers need full control of files in the EmployeeHandbook folder and sales personnel only need to read the files, create one local group for the managers and another local group for the sales personnel.
   - If the resource is on a member server or a computer running Windows NT Workstation, create the local group where the resource is located.
   - If the resource is on a primary domain controller (PDC) or backup domain controller (BDC), create the local group on the PDC.

4. Assign the appropriate permissions to the local groups.
5. Add the global groups to the local groups.

Note To add global groups from one domain to local groups in another domain, the appropriate trust relationship must have been established.

▶ To plan group accounts

Scenario: Users from the Istanbul domain and the Quebec domain of World Wide Importers need to access resources in each other's domain.

As the administrator, you need to determine:

- The global groups and global group memberships for each domain.
- The local groups for each resource, and the computer and domain where they need to be created.
- Which global groups to add to each local group to give members access to a resource.

You will record your planning strategies on the "Group Accounts Planning Worksheet" located at the end of this lesson. After completing the exercise, turn to Appendix A, "Planning Worksheets" and compare your worksheet to the sample provided. (The sample presents only one set of possible answers. You may have planned your accounts differently.)

To complete the "Group Accounts Planning Worksheet," do the following:

1. On the worksheet, provide a name for each group. Record each name in the Group Account column.
2. Specify whether the account is to be a local or global group. Record it in the Local or Global column.
3. List the user accounts that will be added as members to the global groups. Record these in the Members column for each global group that you specify. The following table lists the user accounts for the Istanbul and Quebec domains (both domains have the same set of user accounts).

User account	Description
VicePresident3	Vice President
Director3	Director of Human Resources
SalesMgr3	Sales Manager
SalesRep3	Sales Representative

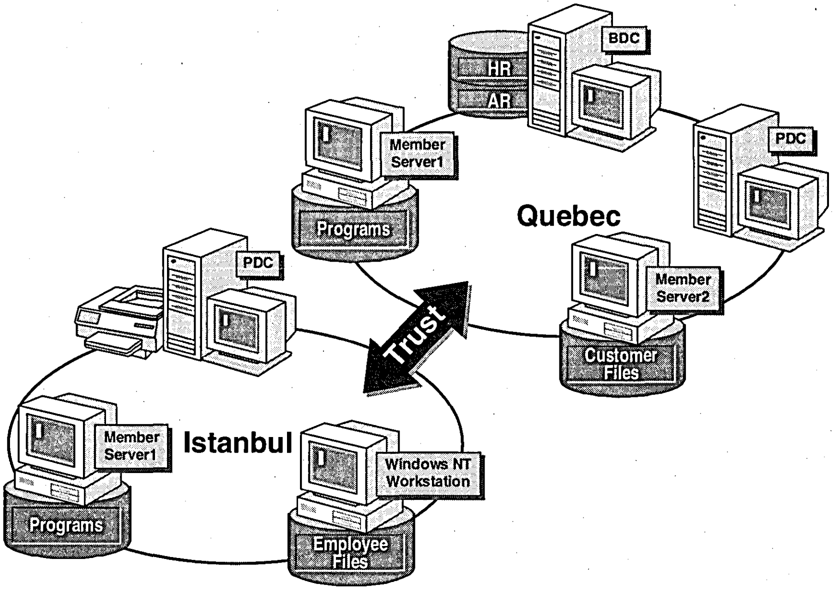
(continued)

User account	Description
CustomerService3-A	Customer Service Representative (night shift)
CustomerService3-B	Customer Service Representative (day shift)
AccountingMgr3	Accounting Manager
Accountant3	Accountant
Temp3	Temporary employee

Note To distinguish between the same user name in each domain, include the domain name when you record it. For example: Istanbul\VicePresident3 and Quebec\VicePresident3.

4. List the global groups that will be added as members to the local groups. Record them in the Members column for each local group that you specify.
5. Provide the server location—either the PDC, BDC, or member server. Record it in the Location column.

Base your implementation plan on the following illustration and criteria.



Use the following criteria to make your decisions:

- All employees need access to the programs in their own domain.
- All employees need access to the printer in the Istanbul domain.
- The executives and managers from both domains need access to the Human Resources (HR) information in the Quebec domain.
- The executives, managers, and customer service and sales representatives from both domains need access to the Customer Files in the Quebec domain.
- The accountants from both domains need access to Accounts Receivable (AR) information in the Quebec domain.
- The managers from both domains need access to Employee Files in the Istanbul domain.

Lesson Summary

The following information summarizes the key points in this lesson:

- As an effective planning strategy, use groups for organizing user accounts and for assigning permissions.
- Logically organize domain users into global groups, typically by geographic location or organizational structure.
- Create local groups based on resource access needs and assign the appropriate permissions to the local groups.
- Add global groups as members of the local groups.

For more information on	See
Group strategies	Chapter 2, "Working With Users and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Assigning permissions	Chapter 5, "Securing Network Resources with Share Permissions," in this book.
	Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.
	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.

Group Accounts Planning Worksheet

Group Account	Local or Global	Members	Location

Lesson 3: Creating Local and Global Groups

You create local groups to give sets of users permissions to access a resource. You create global groups to logically organize domain user accounts. This lesson shows you how to create and use local and global groups.

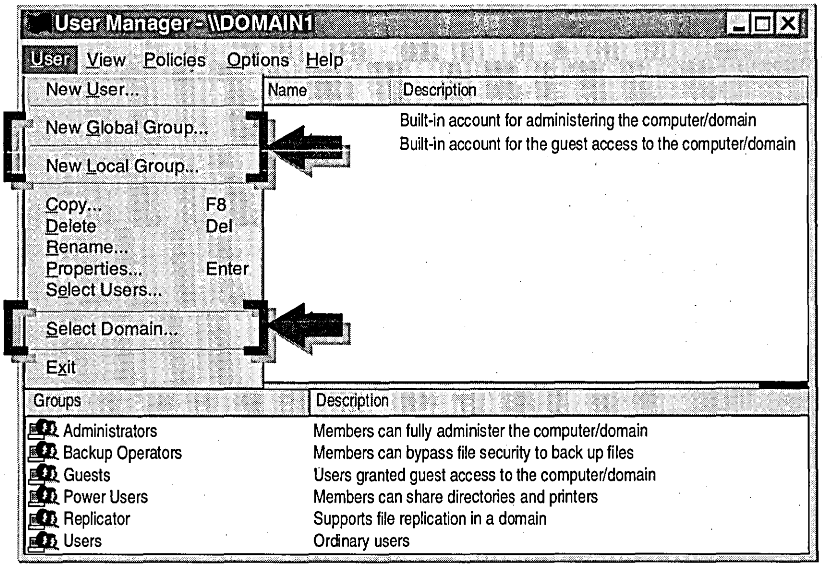
After this lesson, you will be able to:

- Create local groups and add members from local or trusted domains.
- Create global groups and add members.
- Delete local and global groups.

Estimated lesson time: 30 minutes

In a domain, local and global groups are created using User Manager for Domains. In a workgroup, local groups are created using User Manager. Global groups cannot be created in a workgroup.

The following illustration shows User Manager for Domains. All group account menu commands appear on the **User** menu in User Manager, except for **New Global Group** and **Select Domain**. The **Select Domain** menu command allows an administrator to select a different domain or computer in which to create or manage local or global groups.



Name	Description
	Built-in account for administering the computer/domain
	Built-in account for the guest access to the computer/domain

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

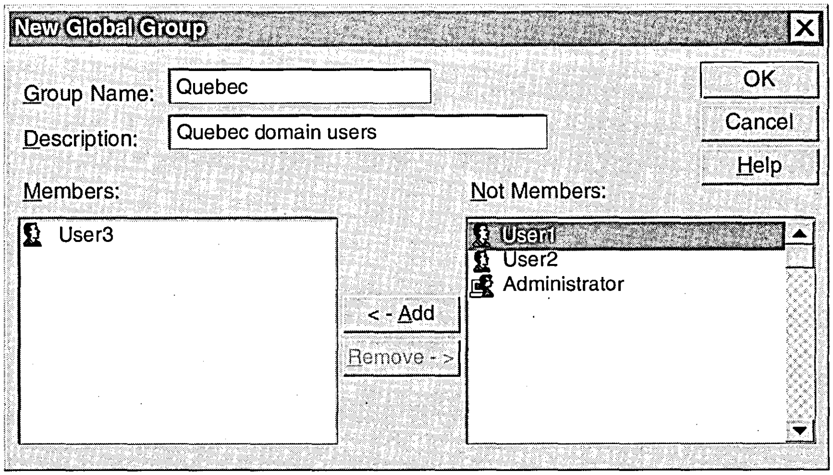
Rules for Creating Groups

When you create local and global groups, the following rules apply:

- You must be a member of the built-in Administrators or built-in Account Operators group on the computer where the group is being created.
- A local group can be created on any computer running Windows NT.
- A global group must be created on a primary domain controller (PDC), but can be created from any computer running User Manager for Domains. This includes:
    - A backup domain controller (BDC).
    - A member server that is part of the domain.
    - A computer running Windows NT Workstation or Microsoft Windows 95 with the client-based administration tools installed.
- Group names must be unique to the domain. They cannot be identical to other user names or group names.

Creating Global Groups

Your implementation strategy begins with organization. Your users must be logically organized in order to create global group accounts for them.



Group Name: Quebec

Description: Quebec domain users

Members:

- User3

Not Members:

- User1
- User2
- Administrator

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

▸ To create a global group

In User Manager for Domains, you create the groups that you planned in the hands-on procedures from the previous lesson, “Planning a Group Strategy.” If you did not complete the “Groups Planning Worksheet” from the lesson, use the sample plan provided in Appendix A, “Planning Worksheets.”

To simplify the exercise, assume that all groups that you create are for the Quebec domain only.

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **User Manager for Domains**.
3. On the **User** menu, click **New Global Group**.

   The **New Global Group** dialog box appears.
4. In the **Group Name** box, type a name for your global group (from the “Group Accounts Planning Worksheet” planned for the Quebec domain only). The global group name:
   - Can contain any uppercase or lowercase characters except for the following: “ / \ [ ] : ; | = , + ? < >
   - Is especially useful if it describes the function of the group.
   - Is limited to 20 characters.
5. In the **Description** box, type a description for the global group, such as the type of users that the group contains. Although the description is optional, it can be helpful in identifying the function of a group.

   Do not close the **New Global Group** dialog box.

▸ To add members to a global group

The user accounts that you will add as members to global groups were created in "Before You Begin" by running the Chapter3.cmd batch file located in the LabFiles folder. To distinguish these user accounts from user accounts that you may have created in other chapters, the number 3 has been appended to each user name.

1. In the **New Global Group** dialog box, in the **Not Members** box, select one user account (from those accounts in the "Group Accounts Planning Worksheet" planned for the Quebec domain only) or select multiple user accounts by holding down the CTRL key while clicking each user.
2. Click **Add.**

   Notice that each new member appears in the **Members** box.
3. Add the remaining user accounts (if any) to the same group, and then click **OK** to create the global group containing all of the users you added as members.

   Notice that the global group appears under **Groups** with a globe as part of the icon.

▸ To complete the exercise

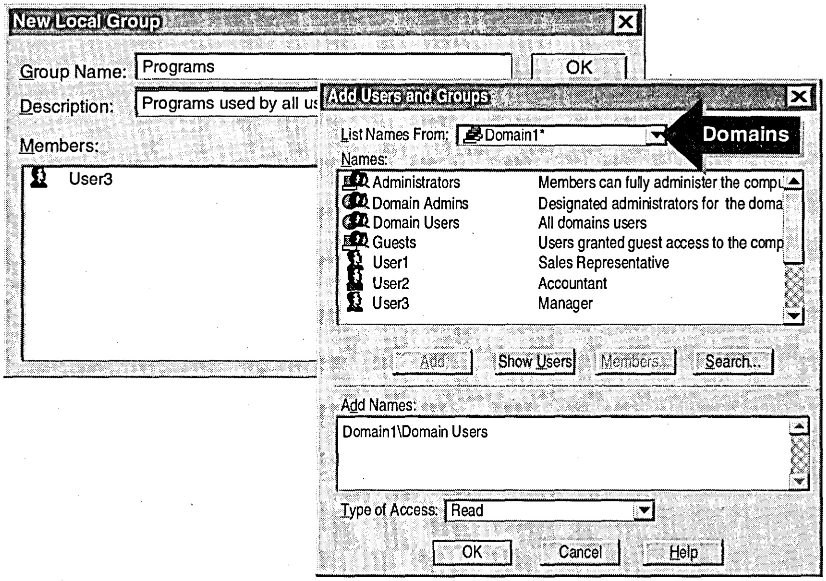
- Create the remaining global groups and add members from the "Group Accounts Planning Worksheet" (of those planned for the Quebec domain only).

Tip As a shortcut to adding users to a global group, in User Manager for Domains hold down the CTRL key, select each user that you want to add to the group, and then on the **User** menu, click **New Global Group**. The **New Global Group** dialog box will appear with the selected members in the **Members** box.

Creating Local Groups

Once you have organized your domain user accounts into global groups, the next step is to create your local groups.

To create a new local group, give the group a name and add members (user accounts and global groups from the local domain or a trusted domain) to it. Even though user accounts and global groups can be added to local groups, it is easier to administer group accounts than individual user accounts.



Group Name: Programs

Description: Programs used by all us

Members:

User3

List Names From: Domain1*

Domains

Names:

Administrators	Members can fully administer the compu
Domain Admins	Designated administrators for the doma
Domain Users	All domains users
Guests	Users granted guest access to the comp
User1	Sales Representative
User2	Accountant
User3	Manager

Add Names:

Domain1\Domain Users

Type of Access: Read

To create a local group

1. In the User Manager window, on the **User** menu, click **New Local Group**.

   The **New Local Group** dialog box appears.

   Note In real-world situations, if you want to create the local group on a computer that is not a domain controller, select the computer on which to create the local group first. To do this, click **Select Domain** on the **User** menu, and then in the **Domain** box, type the name of the computer. For example, you may type **\\computer1**

2. In the **Group Name** box, type a unique, descriptive name for a local group (from the "Group Accounts Planning Worksheet"). Type a name that meets the following criteria:
   - Describes the function of the group.
   - Contains any uppercase or lowercase characters except for the backslash (\).
   - Is up to 256 characters in length; however, remember that only the first 22 characters display in most of the windows.
3. In the **Description** box, type a description of the local group, such as the name of the resource that the local group will be used for.

▸ To add members to a local group

1. In the **New Local Group** dialog box, click **Add**.

   The **Add Users and Groups** dialog box appears.
2. Make sure that your domain name appears in the **List Names From** box. If it does not appear, in the **List Names From** box, click your domain name.
3. Under **Names**, click one or more global groups (of those planned for the Quebec domain only), and then click **Add**.

   Notice that the selected names appear in the **Add Names** box.

   Note In a real-world situation where you need to add global groups from other domains, select the domain where the global group resides in the **List Names From** box. If other domains do not appear in the **List Names From** box, either you do not have other domains in your network or the appropriate trust relationship is not set up.

4. Click **Add**, and then click **OK**.

   The selected global groups appear in the **Members** box of the **New Local Group** dialog box.
5. Click **OK** to create the local group.
6. Click **OK**.

   Notice that the new local group appears under **Groups** with a computer as part of the icon.

▸ To complete the exercise

- Create the remaining local groups and add members, as planned for the Quebec domain only, from the "Group Accounts Planning Worksheet."

Tip As a shortcut to adding users and global groups from the local domain to a new local group, in User Manager for Domains hold down the CTRL key, select each user that you want to add to the group, and then on the **User** menu, click **New Local Group**.

▸ To determine the possible group combinations

In this procedure, you test four different group combinations to determine whether one group can be added as a member to another group.

- Using User Manager for Domains, try the following:

  a. Add a global group to a global group.

  b. Add a global group to a local group.

  c. Add a local group to a local group.

  d. Add a local group to a global group.

  Which group combination or combinations are possible?

  ____

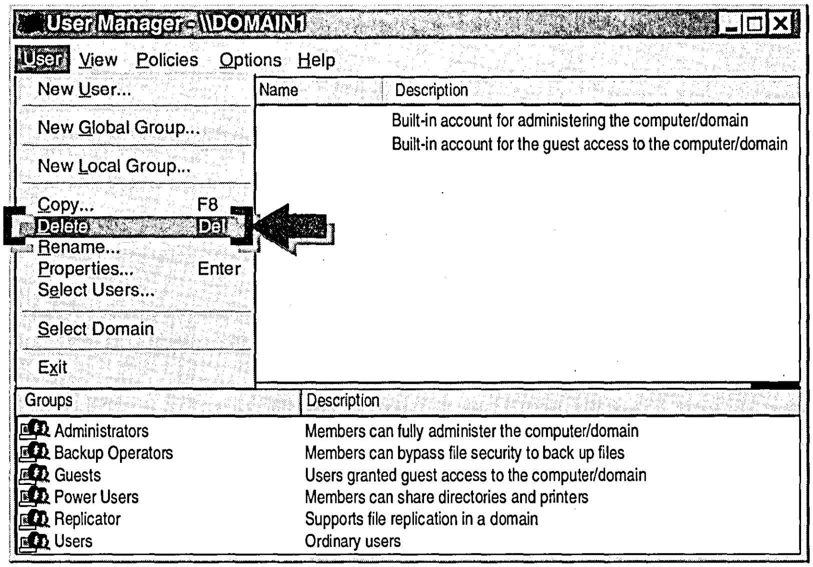
  ____

Note In real-world situations, you would assign permissions to local groups before you add accounts to them. Assigning permissions is covered in detail in Chapter 5, "Securing Network Resources with Share Permissions," and Chapter 6, "Securing Network Resources with NTFS Permissions."

Deleting Groups

Deleting a group deletes the name of the group, its description, and the rights or permissions associated with it. It does not delete the user accounts that it contains.

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



Name	Description
	Built-in account for administering the computer/domain
	Built-in account for the guest access to the computer/domain

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

▸ To delete a group account

1. In User Manager for Domains, double-click the global group that you created for the Accountants.

   Notice the members of the group that appears in the **Global Group Properties** dialog box.

2. Click **Cancel** to return to the User Manager window.

3. Make sure that the same group is selected, and then on the **User** menu, click **Delete.**

   The following message appears:

   Each group is represented by a unique identifier that is independent of the group name. Once this group is deleted, even creating an identically named group in the future will not restore access to resources that currently name this group in the access control list.

4. Click **OK**, and the group is deleted.

   Notice that the members of that group have not been deleted. They still appear in the User Manager window because deleting a group account does not delete its members.

5. Quit User Manager for Domains.

Lesson Summary

The following information summarizes the key points in this lesson:

- In a domain, local and global groups are created using User Manager for Domains.
- In a workgroup, local groups are created using User Manager.
- Creating groups requires that you be a member of the Administrators or Account Operators group.
- A local group can be created on any computer running Windows NT. A global group can only be created on the PDC.
- A global group can only be a member of a local group. A local group cannot be a member of any other groups.

For more information on	See
Creating groups	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Trusted domains	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.
Assigning permissions to groups	Chapter 5, "Securing Network Resources with Share Permissions," in this book. Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.

Lesson 4: Implementing Built-in Groups

Built-in groups are predefined groups that have a predetermined set of user rights. User rights determine the system tasks that a user or member of a built-in group can perform. This lesson explains how built-in groups are used.

After this lesson, you will be able to:

- Determine the user rights associated with a built-in group.
- Determine the default membership of a built-in group.

Estimated lesson time: 30 minutes

Even though individual user rights can be assigned directly to a user, in most cases, it is not recommended.

Computers running Windows NT have three types of built-in groups:

- *Built-in local groups.* These groups give users rights to perform system tasks, such as backing up and restoring files, changing the system time, and administering system resources.

  Built-in local groups are on all computers running Windows NT.
- *Built-in global groups.* These groups give administrators an easy way of controlling all users in a domain.

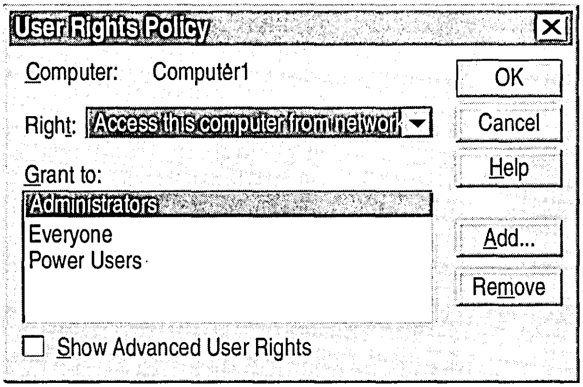
  Built-in global groups are on domain controllers only.
- *System groups.* These groups automatically organize users for system use. Administrators do not assign users to them. Rather, users are either members by default or become members during network activity.

  System groups are on all computers running Windows NT.

Note Built-in groups cannot be deleted or renamed.

Determining the Rights of Built-in Groups

You can determine the inherent rights of the built-in local groups in the **User Rights Policy** dialog box.



User Rights Policy

Computer: Computer1

Right: Access this computer from networ

Grant to:

Administrators
Everyone
Power Users

□ Show Advanced User Rights

▸ **To determine which groups have access to the computer**

- Start User Manager for Domains, and then on the **Policies** menu, click **User Rights.**

  The **User Rights Policy** dialog box appears. The listed right is **Access this computer from network.**

  Which built-in groups have been granted this right?

  ____

▸ **To determine which groups can log on locally**

- In the **Right** box, click **Log on locally**.

  Which built-in groups have been granted this right?

  ____

Note The group Everyone does not have the Log on locally right by default on Windows NT Server domain controllers. This user right was assigned to the Everyone group when you completed the Setup procedures located in "About This Book."

▶ **To determine which groups can change the system time**

- In the **Right** box, click **Change the system time.**

  Which built-in groups have been granted this right?

  ____

▶ **To determine which groups can shut down the system**

- In the **Right** box, click **Shut down the system.**

  Which built-in groups have been granted this right?

  ____

▶ **To determine which groups can back up files and directories**

- In the **Right** box, click **Back up files and directories.**

  Which built-in groups have been granted this right?

  ____

▶ **To determine which groups can restore files and directories**

- In the **Right** box, click **Restore files and directories.**

  Which built-in groups have been granted this right?

  ____

▶ **To determine the inherent rights that are *only* assigned to the Administrators group**

- Select each right to determine which ones are automatically assigned to *only* the Administrators group, and then mark all the check boxes in the following list that apply:

  □ **Access this computer from network**

  □ **Back up files and directories**

  □ **Change the system time**

  □ **Force shutdown from a remote system**

  □ **Load and unload device drivers**

  □ **Log on locally**

  □ **Manage auditing and security log**

  □ **Restore files and directories**

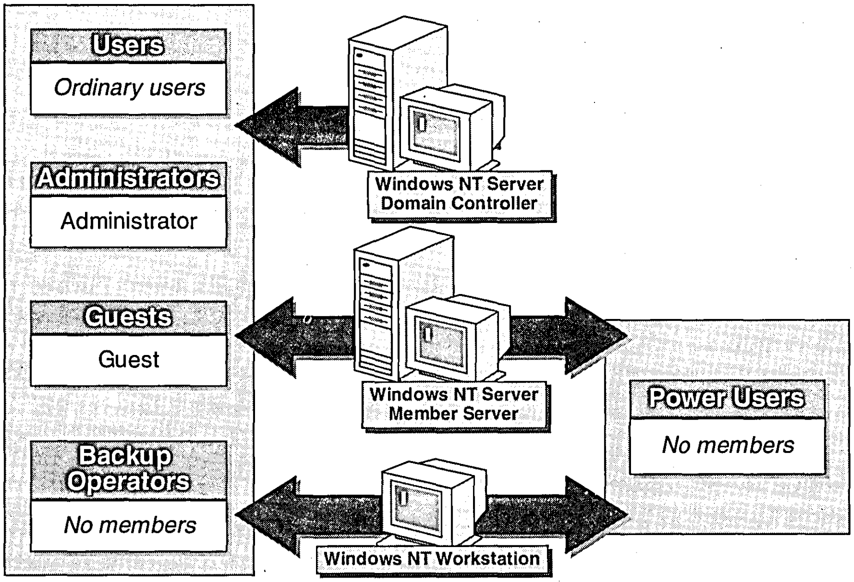
  □ **Shut down the system**

  □ **Take ownership of files or other objects**

Built-in Groups on All Windows NT Computers

All computers running Windows NT have built-in Users, Guests, Administrators, and Backup Operators groups. Member servers and computers running Windows NT Workstation also have a Power Users group.

A built-in group on a domain controller determines what its members can do in the domain. A built-in group on non-domain controllers determines what its members can do on the local computer.



The following table describes the built-in local groups that reside on all computers running Windows NT.

Local group	Members can
Users	Perform tasks for which they have been granted rights, and access resources to which they have been assigned permissions. By default, all user accounts in the local directory database are members of the Users group.
Administrators	Can perform all administrative tasks on the local computer. If the computer is a domain controller, members can fully administer the domain. By default, the local Administrator user account is a member of the Administrators group.
Guests	Perform tasks for which they have been given rights, and access resources to which they have been assigned permissions. Members of Guests cannot make permanent changes to their local environment. By default, the local Guest user account is a member of the Guests group.

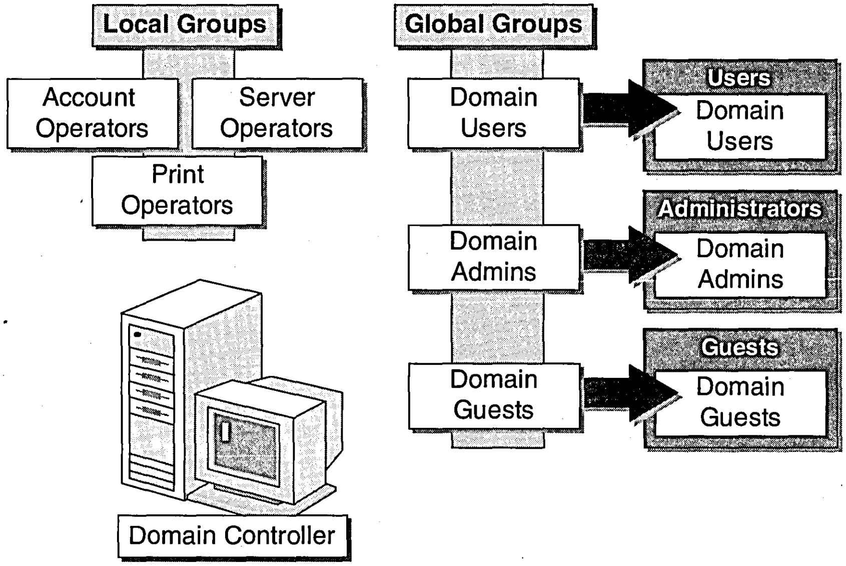
(continued)

Local group	Members can
Backup Operators	Back up and restore files on the local computer using the Windows NT Backup program. There are no default members.
Power Users	Create and modify accounts, and share resources on the local computer. This group is only on member servers and computers running Windows NT Workstation. There are no default members.

Note The built-in Replicator group is used by the Directory Replicator Service. This group is not used for administration and therefore, it is not covered in the book.

Built-in Groups on Domain Controllers Only

Domain controllers have three additional built-in local groups—Account Operators, Server Operators, and Print Operators; Domain controllers also have three additional built-in global groups—Domain Users, Domain Admins, and Domain Guests.



Local Groups

The following table describes the built-in local groups on domain controllers only. There are no initial members of these groups.

Local group	Capabilities
Account Operators	Create, delete, and modify users, global groups, and local groups. Cannot modify the Administrators or Server Operators groups.
Server Operators	Share disk resources, and back up and restore server.
Printer Operators	Set up and manage network printers.

Global Groups

When Windows NT Server is installed as a domain controller, three global groups are created in the domain's directory database—Domain Admins, Domain Users, and Domain Guests. By default, built-in global groups do not have any inherent rights. They get rights when they are added to local groups or when they are assigned user rights or permissions.

The following table describes what happens to built-in global groups when a Windows NT computer is added to the domain.

This group	Is automatically added to this group
Domain Admins	Local Administrators group. Members of the Domain Admins group can then perform administrative tasks on the local computer. The Administrator account is a member by default.
Domain Users	Local Users group. When a domain user account is created, it is automatically made a member of this group. The Administrator account is a member by default.
Domain Guests	Local Guests group. The Guest account is a member by default.

▸ To determine the default membership of the global group Domain Admins

1. Log on as Administrator.
2. Start User Manager for Domains.
3. Under **Groups**, double-click the global group **Domain Admins**.

   By *default*, what built-in user accounts or groups are members of Domain Admins?

4. Click **Cancel** to return to the User Manager window.

▸ To determine membership of the local group Administrators

- Under **Groups**, double-click the local group **Administrators**.

  By default, what built-in user accounts or global groups are members of the Administrators group?

▸ To determine the default membership of other built-in global groups

- Under **Groups**, double-click each of the following global groups.
  - Domain Users contains the following user accounts:
  - Domain Guests contains the following user accounts:

▸ **To determine the default membership of the built-in local group Guests**

- Under **Groups**, double-click **Guests**.

  What user accounts or groups are members of the Guests group?

  ____

▸ **To determine the default membership of the built-in local group Users**

- Under **Groups**, double-click **Users**.

  What user accounts or groups are members of the Users group?

  ____

Built-in System Groups

System groups are installed on all computers running Windows NT. Unlike other built-in groups, users become members of system groups during network activity. Membership cannot be altered.

Built-in system groups reside on all computers running Windows NT. Users become members by default during network activity. Membership cannot be modified.

The following table describes the key system groups used for network administration.

System group	Description
Everyone	Includes all local and remote users who have connected to the computer, including those who connect as Guest. You cannot control who becomes a member of the Everyone group. However, you can assign permissions and rights to the Everyone group. The Everyone group is useful when you do not need to restrict resource access to specific users and groups.
Creator Owner	Includes the user that created or took ownership of a resource. If a member of the Administrators group takes ownership of a resource, the new owner is the Administrators group. This group can be used to manage access to files and folders on NTFS volumes.

The following table describes the system groups that are not used for network administration.

System group	Description
Network	Includes any user who is currently connected from another computer on the network to a shared resource on your computer.
Interactive	Automatically includes a user who logs on to the computer locally. Interactive members access resources on the computer at which they are physically sitting. They log on and access resources by "interacting" with the computer.

Note The Everyone and Creator Owner groups are covered in more detail later in this book.

System groups can only be viewed on an NTFS volume. They do not appear in User Manager.

▶ To view system groups

1. Start Windows NT Explorer.
2. Right-click any NTFS volume.
3. On the shortcut menu, click **Properties.**

   The *drive_name*: **Properties** dialog box appears.
4. Click the **Security** tab.
5. Click **Permissions.**

   The **Directory Permissions** dialog box appears.
6. Click **Add.**

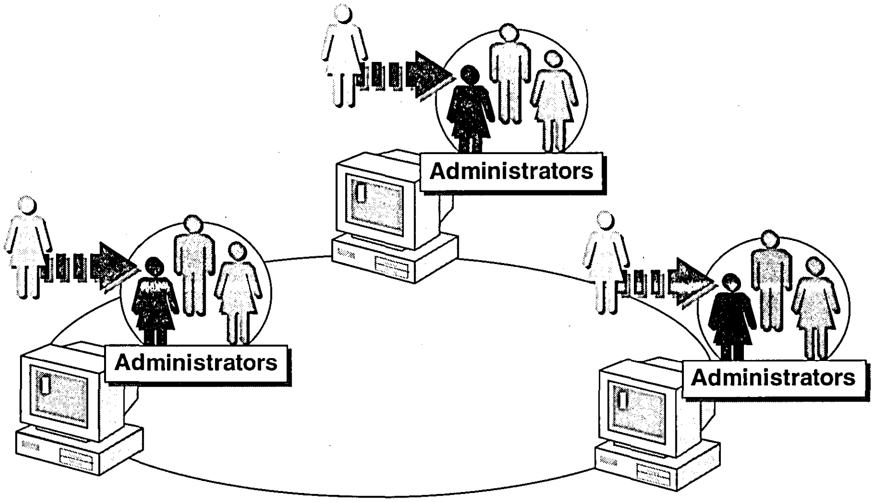
   The **Add Users and Groups** dialog box appears.

   The following system groups appear under Names. If there are many accounts, you may need to scroll through the **Names** list to see the four system groups:

   - Creator Owner
   - Interactive
   - Network
   - System
7. Close all dialog boxes and Windows NT Explorer.

Implementing Built-in Groups for Local Administration

You can give administrative privileges to a user by adding the user's account to the built-in local Administrators groups. This will give the user administrative privileges on the local computer. This is useful when you want to give a user administrative privileges for his or her own computer.



Note If you add a user account to the Administrators group on a PDC, the user will have administrative privileges on all domain controllers in the domain.

▸ **To add a user to the local Administrators group**

In this procedure, you give the administrative privileges to the Vice President of World Wide Importers.

1. Log on as Administrator.
2. In User Manager for Domains, add the user account VicePresident3 to the Administrators group.
3. Log off Windows NT.

▸ **To test the administrative privileges for a user**

1. Log on as VicePresident3.
2. Start User Manager for Domains, and try to create a user account.

   Were you successful? Why or why not?

   ____

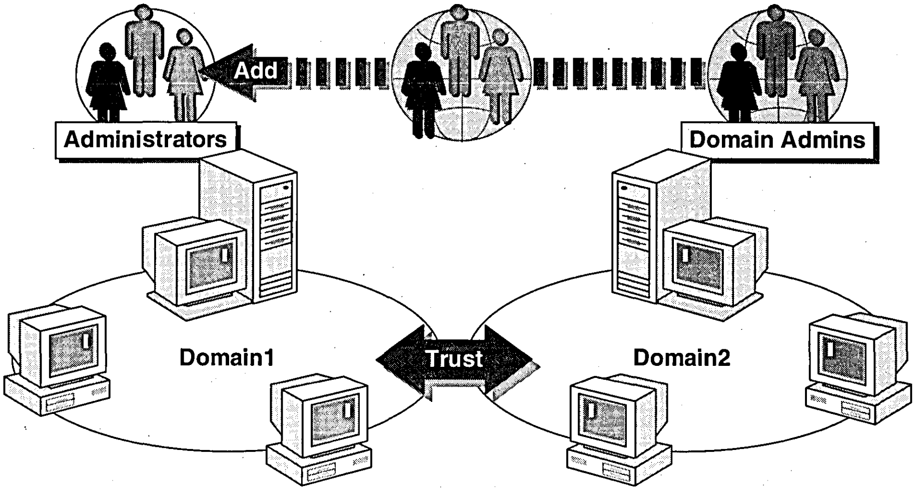
3. Log off Windows NT.

Implementing Built-in Groups for Centralized Administration

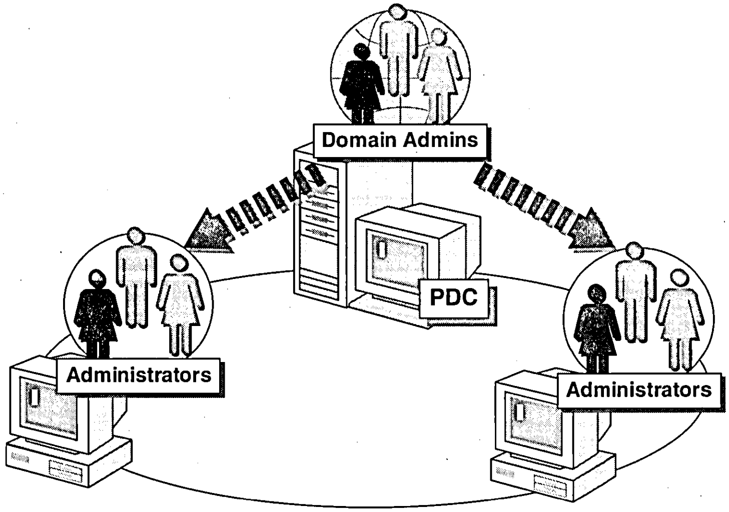
You can give members of an Administrators group in one domain the ability to administer resources in another domain. You can do this by using the built-in global group Domain Admins.

On the PDC of a domain, add the Domain Admins group from another domain to the local Administrators group. This will give members of the Domain Admins group from the other domain the ability to administer domain user accounts and security for resources on any domain controller.

The following illustration shows the addition of the Domain Admins group from Domain2 to the Administrators group on the PDC in Domain1; as a result, Domain Admins in Domain2 have administrative privileges in Domain1.



In a domain with computers running Windows NT Workstation or running Windows NT Server configured as a member server, the Domain Admins group for the local domain is automatically added to the local Administrators group. If you want Domain Admins from a different domain to administer computers running Windows NT Workstation or running Windows NT Server configured as a member server, you need to add Domain Admins to each computer's Administrators group.



- **To add a user to the global group Domain Admins**

1. Log on as Administrator.
2. Start User Manager for Domains, and remove VicePresident3 from the local Administrators group.
3. Add VicePresident3 to the global Domain Admins group.

- **To test the user account as a member of the Domain Admins group**

1. Log off and log on as VicePresident3.
2. Start User Manager for Domains, and try to create another user account.

   Were you successful? Why or why not?

   ____

3. Exit User Manager for Domains and log off Windows NT.

Lesson Summary

The following information summarizes the key points in this lesson:

- A built-in group on a domain controller determines what its members can do in the domain.
- A built-in group on all Windows NT non-domain controllers determines what its members can do on the local computer.
- Built-in local groups are on all computers running Windows NT and give user rights to perform system tasks. Built-in local groups have inherent user rights.
- Built-in global groups are on domain controllers only and provide administrators with control of all users in a given domain. Built-in global groups do not have any inherent user rights.
- System groups are on all computers running Windows NT and automatically organize users for system use. Membership of system groups cannot be changed.

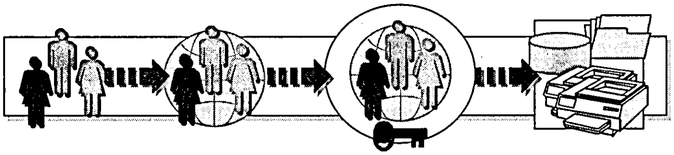
For more information on	See
Built-in groups	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
NTFS volumes	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.

Best Practices

The following checklist provides the best practices for implementing local and global groups. Review this checklist before you begin assigning users to groups or creating group accounts:

□ Apply the following strategy when using local and global groups:

- Organize user accounts into global groups
- Assign permissions to local groups
- Add global groups to local groups



□ For increased security, use the global group Domain Users instead of the Everyone group. The Domain Users group contains only accounts in the domain, and not the Guest account or other accounts that have connected to the network.

□ To enable administrators to perform administration tasks in other domains, add the global group Domain Admins to the local Administrators group on the computer in the domain that you want to administer.

□ If the rights of a built-in group meet your needs, add a user account to the group. Otherwise, create a local group and assign the appropriate user rights.

For example, if for security reasons you want a user to have the right to back up files but *not* the right to restore files, create a local group named *Backup Only* and assign it the *Back up files and directories* right.

□ Always add users to built-in groups that are the most restrictive, yet still allow them to accomplish all necessary tasks.

Note If you want to remove the accounts that were created by running the Chapter3.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter3.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. Which of the following describe a local group? (Circle all that apply.)
   a. Are used to provide users with permission to access a network resource and with rights to perform system tasks.
   b. Are used to organize domain user accounts.
   c. Are assigned resource permissions.
   d. Can contain user accounts and global groups.
   e. Are created on the computer where the resource resides, unless the resource resides on a domain controller. If the resource resides on a domain controller, the local group is created on the PDC.
   f. Are always created on the PDC.
   g. Can be created using User Manager or User Manager for Domains.
   h. Can only be created using User Manager for Domains.

2. Which of the following describe a global group? (Circle all that apply.)
   a. Are used to provide users with permission to gain access to a network resource and with rights to perform system tasks.
   b. Are used to organize domain user accounts.
   c. Are assigned resource permissions.
   d. Can contain user accounts and global groups.
   e. Are created on the computer where the resource resides, unless the resource resides on a domain controller. If the resources resides on a domain controller, the local group is created on the PDC.
   f. Are always created on the PDC.
   g. Can be created using User Manager or User Manager for Domains.
   h. Can only be created using User Manager for Domains.

3. What is the difference between a built-in local group and a built-in global group?

   ____

   ____

4. Which of the following tasks will work? (Circle all that apply.)
   a. To give a user administrative privileges on his or her computer running Windows NT Workstation, add the user account to the built-in Administrators group.
   b. To give administrators from Domain2 the ability to administer all domain controllers in Domain2, add the Domain Admins group from Domain1 to the Administrators group on the PDC of Domain2.
   c. To give administrators from Domain2 the ability to administer all computers in Domain2, add the Domain Admins group from Domain1 to the Administrators group on the PDC of Domain2.
   d. To give administrators from Domain2 the ability to administer computers running Windows NT Workstation and member servers, add the Domain Admins group from Domain1 to the Administrators group on those computers in Domain2.

5. What is the recommended strategy for implementing local and global groups?

   ____

   ____

6. What is the difference between the Domain Users group and the Everyone group?

   ____

   ____

Answer Key

Procedure Answers

Page 86

▸ **To review the video**

1. What is the purpose of a local group?

   The purpose is to provide users with permission to access a resource, such as a printer or file. Local groups are also used to provide users with rights to perform system tasks, such as changing the system time on a computer or logging on to the local computer.

2. What is the purpose of a global group?

   The purpose is to organize domain user accounts, typically by function or geographical location.

3. Where are local groups created?

   Local groups are created on the computer where the resource is located.

4. Where are global groups created?

   Global groups are always created on the PDC in the domain where the accounts reside.

Page 87

Example: Using Groups in a Single-Domain Network

1. On which computer would you create a global group for organizing the user accounts? Why?

   You would create a global group from any computer running User Manager for Domains. User Manager for Domains creates the global group on the PDC because global groups always reside in the domain's directory database.

2. On which computer would you create a local group to provide users with access to the Accounts Payable database? Why?

   You would create a local group from any computer running User Manager for Domains. User Manager for Domains creates the local group on the PDC even though the Accounts Payable database is on the BDC. This is because all domain controllers share account information with each other and maintain a common directory database.

3. On which computer would you create a local group to provide users with access to the Inventory database? Why?

   You would create a local group on the member server because that is where the Inventory database resides. The local group is then stored in the local directory database.

4. How would you give members of the global group access to both databases?

   Add the global group to both local groups, the one created for the Inventory database and the other created for the Accounts Payable database. Members of the local groups now have access to both databases, assuming that the appropriate permissions are assigned to the local groups.

Page 88

Example: Using Groups in a Multiple-Domain Network

1. On which computers would you create a global group for organizing the user accounts? Why?

   You would create two global groups, one from any computer running User Manager for Domains in the London domain and the other on the from any computer running User Manager for Domains in the Paris domain. User Manager for Domains creates the global group on the PDC in each domain because global groups always reside in the domain's directory database where the user accounts reside.

2. On which computers would you create a local group to provide users with access to the Inventory databases? Why?

   In each domain, you would create a local group on the member server because each member server has its own directory database.

3. How would you give members of the global groups that you just created in London and in Paris access to the Inventory databases in each other's domain?

   Add the global group created for London users to the local group created for the Paris Inventory database. Add the global group created for Paris users to the local group created for the London Inventory database. Members of the local groups now have access to the Inventory databases, assuming that the appropriate permissions are assigned to the local groups.

Page 102

▶ **To determine the possible group combinations**

- Which group combination or combinations are possible?

  Only b is correct. A global group can be added to a local group.

Page 107

▸ **To determine which groups have access to the computer**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators, Everyone, and Power Users.

  On domain controllers: Administrators and Everyone.

Page 107

▸ **To determine which groups can log on locally**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators, Backup Operators, Everyone, Guests, IUSR_*computer_name* (if Internet Information Server or Peer Web Server is installed), Power Users, and Users.

  On domain controllers: Account Operators, Administrators, Backup Operators, Everyone, IUSR_*computer_name* (if Internet Information Server is installed), Print Operators, and Server Operators.

Page 108

▸ **To determine which groups can change the system time**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators and Power Users.

  On domain controllers: Administrators and Server Operators.

Page 108

▸ **To determine which groups can shut down the system**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators, Backup Operators, Everyone, Power Users, and Users.

  On domain controllers: Account Operators, Administrators, Backup Operators, Print Operators, and Server Operators.

Page 108

▸ **To determine which groups can back up files and directories**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators and Backup Operators.

  On domain controllers: Administrators, Backup Operators, and Server Operators.

Page 108

▸ **To determine which groups can restore files and directories**

- Which built-in groups have been granted this right?

  On Windows NT Workstation and member servers: Administrators and Backup Operators.

  On domain controllers: Administrators, Backup Operators, and Server Operators.

Page 108

▸ **To determine the inherent rights that are *only* assigned to the Administrators group**

- Select each user right to determine which ones are automatically assigned to *only* the Administrators group, and then mark all the check boxes in the following list that apply:

  Load and unload device drivers, Manage auditing and security log, and Take ownership of files or other objects.

Page 112

▸ **To determine the default membership of the global group Domain Admins**

- By *default*, what built-in user accounts or groups are members of Domain Admins?

  Administrator is the only user account. There are no groups. Domain Admins only exists on domain controllers.

Page 112

▸ **To determine membership of the local group Administrators**

- By default, what built-in user accounts or global groups are members of the Administrators group?

  On computers running Windows NT Workstation and on member servers that are in a domain, Administrator is the only user account.

  On domain controllers, Administrator is the only user account and Domain Admins is the only global group.

Page 112

▸ **To determine the default membership of other built-in global groups**

- Domain Users contains the following user accounts:

  The Administrator and all domain user accounts except for the Guest account.

- Domain Guests contains the following user account:

  Guest.

Page 113

▸ **To determine the default membership of the built-in local group Guests**

- What user accounts or groups are members of the Guests group?

  On Windows NT Workstation and member servers, the Guest user account is a member. If Internet Information Server or Peer Web Server is installed, a user account IUSR_*computer_name* (where *computer_name* is the name of your computer) is also a member.

  On domain controllers, the global group Domain Guests. If Internet Information Server is installed, a user account IUSR_*computer_name* (where *computer_name* is the name of your computer) is also a member.

Page 113

▸ **To determine the default membership of the built-in local group Users**

- What user accounts or groups are members of the Users group?

  On all Windows NT–based computers that have been added to the domain, the global group Domain Users.

Page 115

▸ **To test the administrative privileges for a user**

2. Start User Manager for Domains, and try to create a user account.

   Were you successful? Why or why not?

   Yes, because VicePresident3 is a member of the Administrators group and has all of the user rights inherent in the Administrators group.

Page 117

▸ **To test the user account as a member of the Domain Admins group**

2. Start User Manager for Domains, and try to create another user account.

   Were you successful? Why or why not?

   Yes, because the Domain Admins group is a member of the Administrators group.

Page 120

Review Answers

1. Which of the following describe a local group? (Circle all that apply.)

   Answers a, c, d, e, and g are correct.

2. Which of the following describe a global group? (Circle all that apply.)

   Answers b, f, and h are correct.

3. What is the difference between a built-in local group and a built-in global group?

   Built-in local groups have a predetermined set of user rights. Built-in global groups get their rights from other local groups.

4. Which of the following tasks will work? (Circle all that apply.)

   Answers a, b, and d are correct.

5. What is the recommended strategy for implementing local and global groups?

   Organize users into global groups, assign permissions to local groups, and add global groups to local groups.

6. What is the difference between the Domain Users group and the Everyone group?

   The Domain Users group is a built-in global group on domain controllers that only contains domain accounts. The Everyone group is a system group on all computers that contains all local and remote users that have connected to the computer, including guest users.

CHAPTER 4

Administering User and Group Accounts

About This Chapter

This chapter presents tasks related to maintaining existing accounts and streamlining administrative tasks, including creating template accounts, modifying multiple accounts at one time, planning and implementing an account policy, maintaining domain controllers, and troubleshooting user logon problems. The hands-on procedures give you an opportunity to implement and practice each task.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- The knowledge and skills covered in Chapter 2, "Setting Up User Accounts."
- Knowledge and skills covered in Chapter 3, "Setting Up Group Accounts."
- A user account named User4 and two global groups—Managers4 and CustomerService4. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter4.cmd to create these accounts.

Lesson 1: Introduction to Administering Accounts

In this lesson, you are introduced to procedures and tools used by network administrators. Starting with an overview of the key elements that will be examined throughout this chapter, the lesson then steps you through several tasks.

After this lesson, you will be able to:

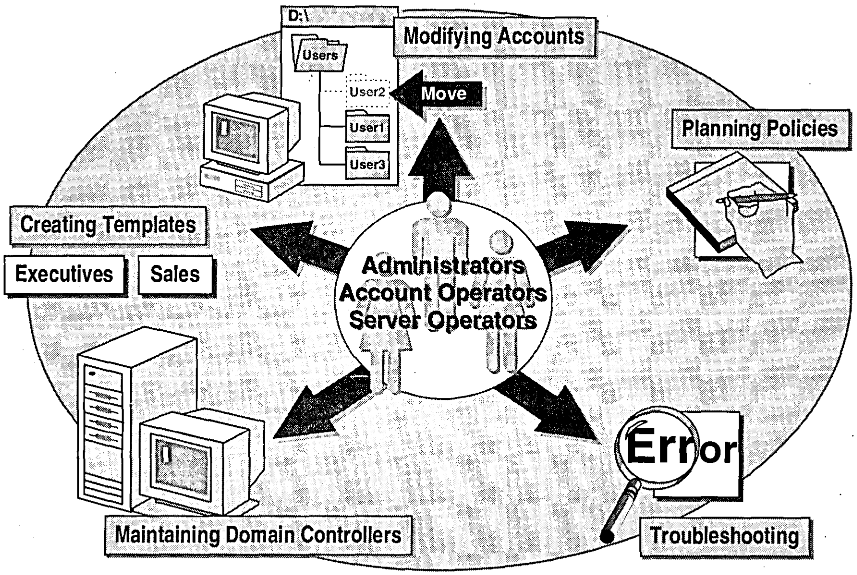
- Assign Account Operator privileges.
- Create and use account templates.

Estimated lesson time: 20 minutes

Administrative Tasks

There are several procedures that an administrator can use to efficiently administer accounts and keep the network running smoothly. Some of the most useful are:

- *Creating Templates*. Creating templates for adding new user accounts streamlines the work.
- *Modifying Accounts*. Making changes to multiple user accounts at one time, (for example, moving home folders) lightens the work load.
- *Planning Policies*. Planning and implementing an account policy helps to keep the network secure.
- *Maintaining Domain Controllers*. Maintaining domain controllers means that user accounts can always be successfully validated.
- *Troubleshooting*. Solving problems associated with user accounts ensures that users can log on.



Distributing Administrative Tasks

To distribute some of your administrative tasks, you can grant administrative privileges to a user account by adding the user to one of the following groups:

- *Administrators*. Members of the Administrators group have full administrative capabilities. They are responsible for planning and maintaining network security.
- *Account Operators*. Members of the Account Operators group can create, delete, and modify user accounts, global groups, and local groups, and they can set account policies.

▸ To give Account Operator privileges to a user account

In this procedure, you add a user account to the Account Operators group.

1. Log on as Administrator and start User Manager for Domains.
2. In the **Username** list, double-click User4.
3. In the **User Properties** dialog box, click **Groups**.

   The **Group Memberships** dialog box appears.
4. In the **Not member of** list, click **Account Operators**, and then click **Add**.

   Notice that **Account Operators** appears in the **Member of** list.
5. Click **OK** to close the **Group Memberships** dialog box.
6. Click **OK** to close the **User Properties** dialog box, but do not exit User Manager for Domains.

▸ **To determine the inherent rights that are assigned to Account Operators**

1. In the User Manager window, on the **Policies** menu, click **User Rights**.
2. In the **Right** box, select each user right one at a time to determine which of the following rights are automatically assigned to the Account Operators group, and then mark the check boxes that apply in the following list:

   ❑ **Access this computer from network**

   ❑ **Add workstations to domain**

   ❑ **Back up files and directories**

   ❑ **Change the system time**

   ❑ **Force shutdown from a remote system**

   ❑ **Load and unload device drivers**

   ❑ **Log on locally**

   ❑ **Manage auditing and security log**

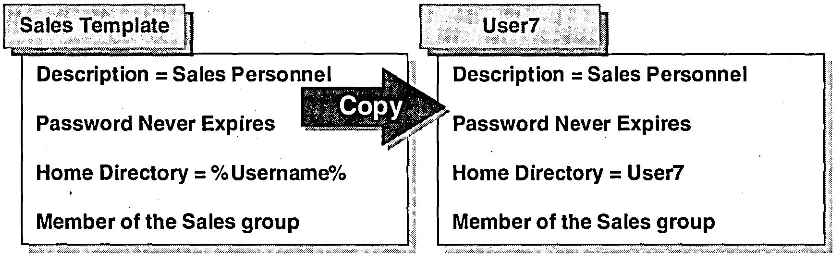
   ❑ **Restore files and directories**

   ❑ **Shut down the system**

   ❑ **Take ownership of files or other objects**
3. Click **Cancel**.

Using Templates

A user account template is a standard user account that you create with the properties that apply to users who have common needs. User account templates are useful administrative tools for creating new user accounts. For example, if all sales personnel require membership in the Sales group, you can create a template that includes membership to that group.


Sales Template
Description = Sales Personnel
Password Never Expires
Home Directory = %Username%
Member of the Sales group
Copy
User7
Description = Sales Personnel
Password Never Expires
Home Directory = User7
Member of the Sales group

To use a template to create a new user account, copy the template account and assign a user name and password for the new user. The following options become properties of the new user account:

Description	Profile
User Must Change Password at Next Logon	**Hours** (domain controllers only)
User Cannot Change Password	**Logon to** (domain controllers only)
Password Never Expires	**Account** (domain controllers only)
Groups	**Dialin**

Note Rights and permissions granted to an individual user account are not copied.

Suggestions for creating templates include the following:

- Make a template for each classification of employee, such as sales, accountants, managers, and so on.
- If you commonly have short-term or temporary network users, create a template with limited logon hours, workstation specifications, and other necessary restrictions.

▶ To define the user account template for new managers

In this procedure, you create a user account template that will be used to create accounts for new managers.

1. Log on as User4 (the user that you added to the Account Operators group) and start User Manager for Domains.
2. In the **User** menu, click **New User**.
3. Provide the following information:
   - **Username:** *name* **Manager_Template**
   - **Description**: the description that you want to appear for each user account that is created using the template

Tip Add any valid non-alphabetic character, such as the underscore (_), as the first character of all template account names to make them appear at the top of the **Username** list. For example, "_Manager_Template."

▶ To define the password requirements for new managers

1. In the **New User** dialog box, make sure that the **User Must Change Password At Next Logon** check box is selected.
2. Select the **Account Disabled** check box.

▸ To define the template home folder path

1. In the **New User** dialog box, click **Profile.**
2. Under **Home Folder**, click **Connect**, and then click **Z.**
3. In the **To** box, type \\computer_name\users\\%**username**% (where *computer_name* is the name of your computer), and then click **OK.**

▸ To define the group accounts for new managers

1. In the **New User** dialog box, click **Groups.**
2. Add the managers template to the following groups:
   - Managers4
   - Domain Users

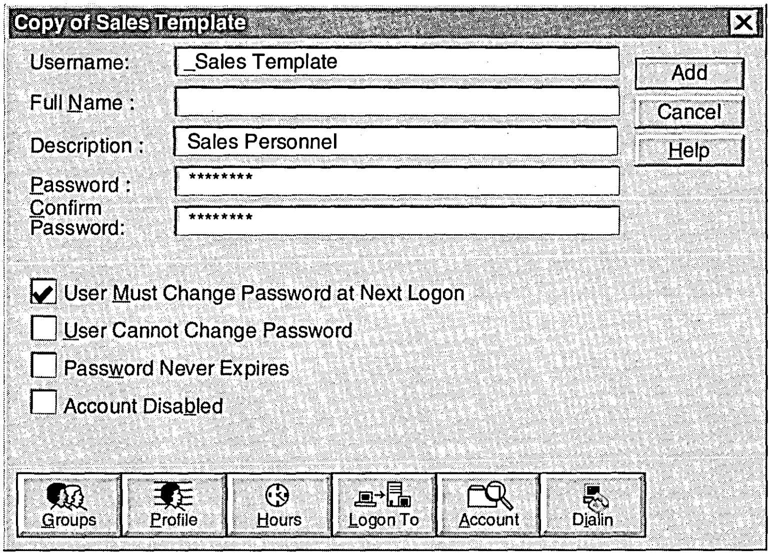
▸ To define the template for new night shift employees

In this procedure, you define a template account for employees who work the night shift.

1. Create a template for the new night shift employees, using the same properties as the managers template (except for groups).
2. Add the night shift employees template to the following groups:
   - CustomerService4
   - Domain Users
3. Restrict the logon hours for night shift employees to 6:00 P.M. through 6:00 A.M., Monday through Friday.

Using Templates to Create User Accounts

To create a new user account using a template, copy the template.



Copy of Sales Template

Username: _Sales Template

Full Name :

Description : Sales Personnel

Password : ********

Confirm Password: ********

☑ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

▸ To create a user account using a template

1. In the User Manager window, under **Username**, select one of your templates.
2. On the **User** menu, click **Copy**.
3. Type a **Username**, **Full Name**, and **Password** for the user, and then click **Add**.
4. Repeat this procedure using the other template that you created.

▸ To determine which account options were copied

- In the User Manager window, double-click the user account that you created using the night shift employees template. Compare the following account options with those in the template account. In the following list, mark the check boxes next to those options that were copied:

  □ **Username**

  □ **Full Name**

  □ **Description**

  □ **Password** and **Confirm Password**

  □ **User Must Change Password at Next Logon**

  □ **User Cannot Change Password**

  □ **Password Never Expires**

  □ **Account Disabled**

  □ **Profile button options**

  □ **Groups button options**

  □ **Hours button options**

Lesson Summary

The following information summarizes the key points in this lesson:

- Administrative tasks can be distributed by granting administrative privileges to a user account by adding the user to the Administrators or Account Operators groups.
- Create template accounts with the properties that apply to users who have common needs.

Lesson 2: Implementing an Account Policy

The account policy determines how passwords must be used by all user accounts for a computer or domain and also determines the account lockout policy. This lesson provides conceptual and procedural information on setting up and using an account policy.

This lesson requires that you have completed Lesson 1.

After this lesson, you will be able to:

- Implement an account policy for all accounts in a domain.
- Reset user account passwords.
- Unlock a user account.

Estimated lesson time: 20 minutes

Setting an Account Policy

The account policy sets the requirements for:

- Password minimum and maximum ages
- Password minimum length
- Password uniqueness
- Account lockout options

Changes that you make to the account policy go into effect for users at one of the following two times:

- The next time the user logs on.
- The next time the user makes a change covered by the policy. For example, the minimum password length does not apply to existing passwords, but it will apply the next time a user changes his or her password.

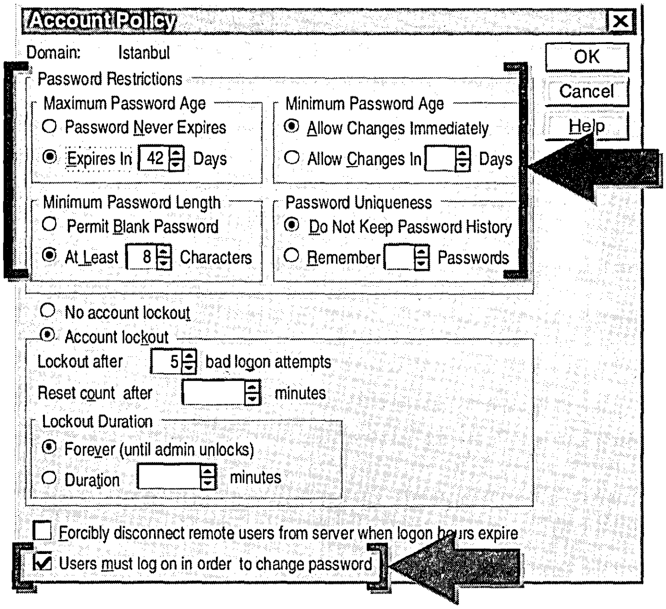
Planning an Account Policy

By default, the only password requirement for user accounts is that users change their passwords the first time that they log on. To use an account policy to provide additional security for user accounts, consider the following:

- Never allow blank passwords. Blank passwords mean *no* security. Do not allow the use of blank passwords on any system connected to the Internet or any system that has dial-in capabilities.
- Require a minimum length for all passwords. The longer the password, the more difficult it is to guess.
  - In a medium-security network, require 6–8 characters.
  - In a high-security network, require 8–14 characters.
- Require users to change their passwords frequently. This helps to prevent unauthorized users from guessing them.
  - In a medium-security network, change passwords every 45–90 days.
  - In a high-security network, change passwords every 14–45 days.
- Require users to use a different password each time they change it. Make sure that once it is changed, it cannot be changed back to a previous password.
  - In a medium-security network, require 8–12 different passwords.
  - In a high-security network, require 12–24 different passwords.
- Lock out accounts after multiple failed logon attempts. This reduces the chance of an unauthorized person gaining access to the network.
  - In a medium-security network, lock out a user after five failed logon attempts.
  - In a high-security network, lock out a user account after three failed logon attempts.
- Require that all locked accounts be unlocked by an administrator. This guarantees that you will be aware of unauthorized users attempting to guess passwords for an account until it becomes locked out.
- Require that users with restricted logon hours are disconnected from the network during off hours. This will prevent users from dialing in to the network.

Setting Password Options

The password options set the requirements for user account passwords. Account policies allow control over password implementation.



Account Policy

Domain: Istanbul

Password Restrictions

Maximum Password Age
○ Password Never Expires
● Expires In 42 Days

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

Minimum Password Length
○ Permit Blank Password
● At Least 8 Characters

Password Uniqueness
● Do Not Keep Password History
○ Remember Passwords

○ No account lockout
● Account lockout
Lockout after 5 bad logon attempts
Reset count after minutes
Lockout Duration
● Forever (until admin unlocks)
○ Duration minutes

□ Forcibly disconnect remote users from server when logon hours expire
☑ Users must log on in order to change password

The following table describes the password options.

Option	Description
Maximum Password Age	The period of time that a password can be used before the user is required to change it. Range of values: 1–999 days.
Minimum Password Age	The period of time that a password must be kept before the user can change it. Do not allow immediate changes if a password uniqueness value will be entered. The value of the **Minimum Password Age** must be less than the value of the **Maximum Password Age**. Range of values: 1–999 days.
Minimum Password Length	The minimum number of characters required in a password. Range of values: 1–14 characters.

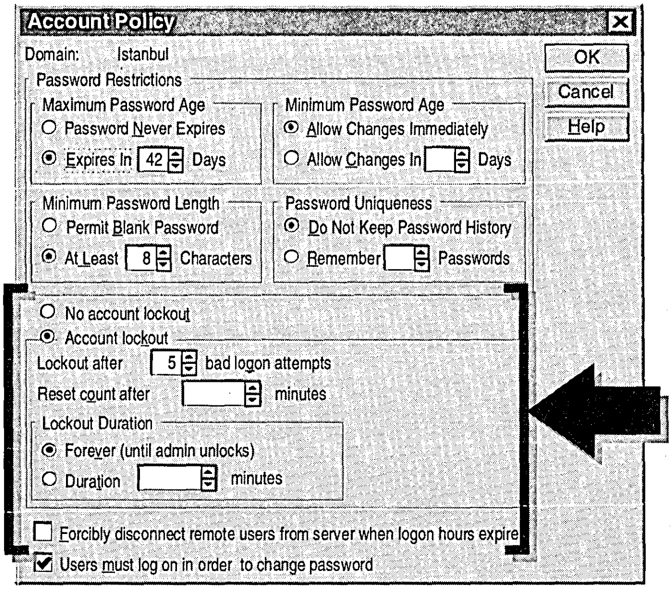
(continued)

Option	Description
Password Uniqueness	The number of new passwords that must be used by a user before an old password can be reused. For uniqueness to be effective, immediate changes should not be allowed by the **Minimum Password Age** parameter. Range of values: 1–24 passwords.
Users must log on in order to change password	If selected, users cannot change their own expired passwords. If cleared, users can change their own expired passwords.

Important If the **Password Never Expires** check box is selected in the **New User** or **User Properties** dialog boxes for an individual user account, that setting overrides the **Maximum Password Age** setting.

Setting Account Lockout Options

The account lockout feature enables you to make Windows NT more secure from intruders who try to log on by guessing the passwords of existing user accounts. The account lockout options set the requirements for locking out a user account after failed logon attempts.



Account Policy

Domain: Istanbul

Password Restrictions

Maximum Password Age
○ Password Never Expires
● Expires In 42 Days

Minimum Password Age
● Allow Changes Immediately
○ Allow Changes In ___ Days

Minimum Password Length
○ Permit Blank Password
● At Least 8 Characters

Password Uniqueness
● Do Not Keep Password History
○ Remember ___ Passwords

○ No account lockout
● Account lockout
Lockout after 5 bad logon attempts
Reset count after ___ minutes

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

□ Forcibly disconnect remote users from server when logon hours expire
☑ Users must log on in order to change password

The following table describes the account lockout options.

Option	Description
Account Lockout	If you click **Account Lockout,** the next three options are available.
Lockout After	The number of incorrect logon attempts that will cause the account to be locked. Range of values: 1–999.
Reset Count After	The maximum number of minutes that can elapse between any two bad logon attempts before lockout occurs. Range of values: 1–99999 minutes.
Lockout Duration	**Forever** option: Causes locked accounts to remain locked until an administrator unlocks them. (The Administrator account set up during installation cannot be locked out.) **Duration** option: Causes accounts to remain locked for the specified number of minutes. If a lockout duration expires, a locked out account will become unlocked automatically. Range of values: 1–99,999 minutes.
Forcibly disconnect remote users from server when logon hours expire	If selected, the user account is disconnected from any server in the domain when the account exceeds logon hours. If cleared, the user account is not automatically disconnected, but no new connections are allowed. Available only on Microsoft Windows NT Server.

▸ To plan an account policy

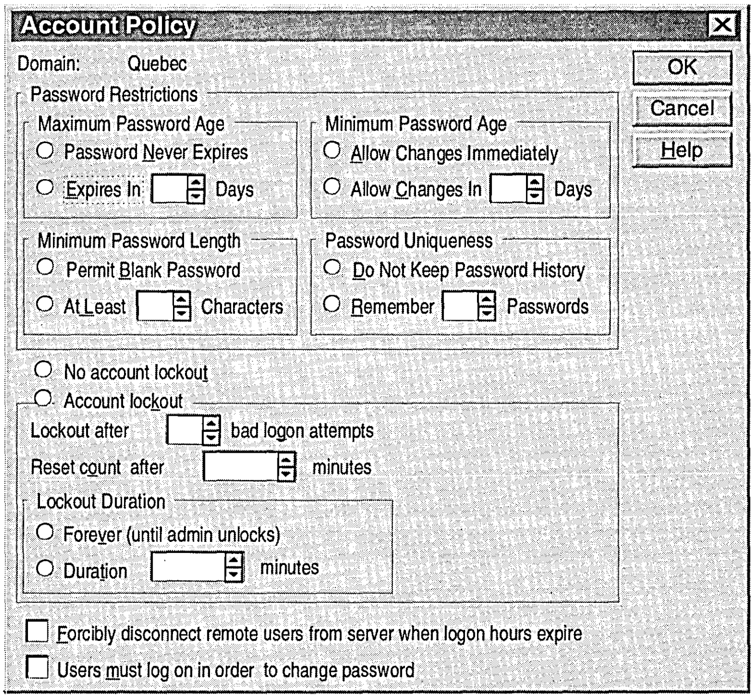
In this exercise, you plan an account policy for the Quebec domain. You need to determine the following:

- Password restrictions
- Account lockout requirements

To make your decisions, use the following criteria:

- Require users to change their passwords once a month.
- Do not allow users to reuse a password for at least six months.
- Make every effort to prevent unauthorized users from breaking into the system.
- Disconnect employees with restricted logon hours from the network during off hours.

Record your decisions by marking the appropriate options on the following reproduction of the **Account Policy** dialog box.



Account Policy

Domain: Quebec

Password Restrictions

Maximum Password Age
○ Password Never Expires
○ Expires In ☐ Days

Minimum Password Age
○ Allow Changes Immediately
○ Allow Changes In ☐ Days

Minimum Password Length
○ Permit Blank Password
○ At Least ☐ Characters

Password Uniqueness
○ Do Not Keep Password History
○ Remember ☐ Passwords

○ No account lockout
○ Account lockout
Lockout after ☐ bad logon attempts
Reset count after ☐ minutes

Lockout Duration
○ Forever (until admin unlocks)
○ Duration ☐ minutes

☐ Forcibly disconnect remote users from server when logon hours expire
☐ Users must log on in order to change password

To set the account policy

In this procedure, you set an account policy for all domain user accounts in a medium-security network.

1. Log on as Administrator.
2. In the User Manager window, on the **Policies** menu, click **Account**.

   The **Account Policy** dialog box appears.

3. Set the following account policy for password restrictions and account lockout based on a medium level of security.

Password or account lockout restrictions	Set this way for medium security
Maximum Password Age	Expires in 90 days
Minimum Password Age	Allow changes in 30 days
Minimum Password Length	8 characters
Password Uniqueness	Remember 8 passwords
Account Lockout	Yes
Lockout After	3 bad logon attempts
Reset Count After	30 minutes
Lockout Duration	Forever (until administrator unlocks)

4. Click **OK** to set the account policy.

▸ **To test the password restriction portion of the account policy**

In this procedure, you test how passwords are affected by the new account policy.

1. Try to create a user account with no password.

   An error message appears stating that the password you typed is invalid. This error occurred because your account policy requires passwords to be a minimum of eight characters. Blank passwords are not permitted.

2. Click **OK** to acknowledge the message.
3. In the **Password** and **Confirm Password** boxes, type a password that is at least eight characters, and then click **Add.**

   Make sure that the **User Must Change Password at Next Logon** check box is selected.

4. Log off and then log on using the new user account.

   A message box appears, indicating that you are required to change your password at first logon attempt. Even though this was not set in your account policy, it was set by default when you created the user account.

5. Click **OK** to acknowledge the message.
6. In the **New Password** and **Confirm New Password** boxes, type **watermelon** and then click **OK.**

   A message appears indicating that the password was changed.

7. Press CTRL+ALT+DELETE to access the **Windows NT Security** dialog box, and then click **Change Password.**
8. In the **Old Password** box, type **watermelon**

9. In the **New Password** and **Confirm New Password** boxes, type **cantaloupe** and then click **OK.**

   A message appears stating that the account cannot be changed at this time. This occurs because the account policy does not permit password changes more than once in 30 days. You were able to change your password the first time because it was required when the account was created.

10. Click **OK.**

▸ **To test the account lockout portion of the account policy**

In this procedure, you incorrectly type a password several times to see the effect of the account lockout policy.

1. Log off and try to log on again as the same user, without specifying a password.

   You receive an error message indicating that the system could not log you on.

2. Click **OK.**
3. Log off and log on two more times with no password.
4. Now log on with the correct password.

   Why were you unable to log on using the correct password?

   ____

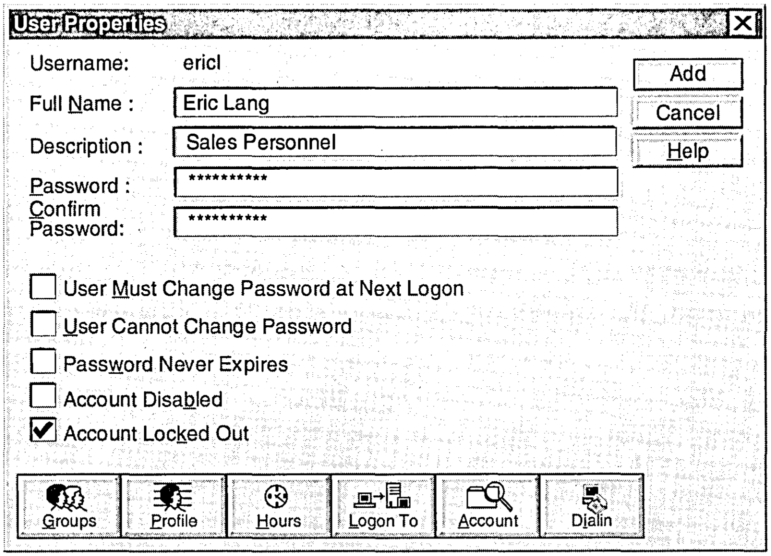
   How should the user solve the problem?

   ____

5. Click **OK.**

Unlocking User Accounts

If you have an account policy set up that locks out the user after several failed logon attempts, you may need to unlock the account.



User Properties

Username: ericl

Full Name : Eric Lang

Description : Sales Personnel

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

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

□ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

☑ Account Locked Out

▸ To unlock a locked account

1. Log on as Administrator, and start User Manager for Domains.
2. In the **Username** list, double-click the locked account (from the previous exercise).
3. Clear the **Account Locked Out** check box.
4. Click **OK.**
5. Exit User Manager for Domains.

▸ To verify that the account is unlocked

- Log on as the user whose account you unlocked.

Tip If the user has failed several times in trying to log on to the domain, the user may have forgotten his or her password. If that is the case, reset it while you are unlocking it.

Resetting User Account Passwords

If a user's password expires before the user has a chance to change it, or if a user forgets a password, you can reset the password by deleting it and typing a new one.

▶ **To reset a user account password**

1. Log on as Administrator.
2. Start User Manager for Domains.
3. Double-click the user that you used in the previous exercise.

   The **User Properties** dialog box appears.
4. In the **Password** box, double-click the entry, and then press DELETE.
5. In the **Password** box, type a new password.
6. In the **Confirm Password** box, retype the password, and then click **OK**.
7. Exit User Manager for Domains.

Note Before you continue, you may want to clear the account policy settings. Clearing the settings will allow you to experiment with other user accounts used throughout this book without the restrictions set in the account policy.

Lesson Summary

The following information summarizes the key points in this lesson:

- The account policy sets the requirements for passwords and lockout options for all domain user accounts.
- To protect accounts from unauthorized use, never allow blank passwords.
- To make passwords difficult to guess, require a minimum password length.
- Require that users change their passwords frequently and that they are unique each time. This will help deter unauthorized access.
- To catch computer hackers, lock out accounts after multiple failed attempts.

For more information on	**See**
Domain security policies	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 3: Modifying Multiple User Accounts

Windows NT provides a shortcut for making modifications to multiple user accounts at one time. This is especially useful for moving user home folders to a different server or volume.

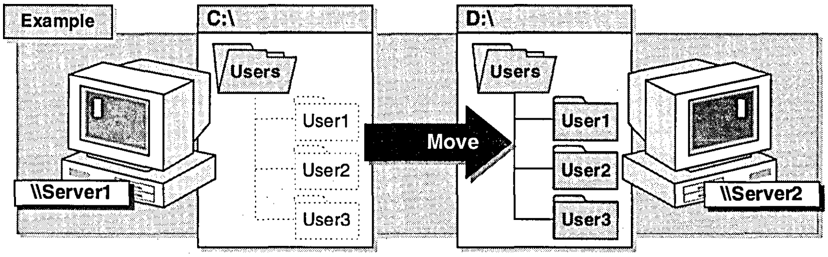
This lesson guides you through the steps to modify multiple user accounts at one time.

After this lesson, you will be able to:

- Modify multiple accounts at one time.

Estimated lesson time: 10 minutes

You can easily modify multiple user accounts at one time by selecting multiple user accounts and then modifying the properties. Use this procedure when you need to modify multiple user accounts in the same manner—for example, when you need to move home folders to another server or volume, or set the logon hours for 100 users.



▸ To modify multiple user accounts at one time

1. Start User Manager for Domains.
2. Select the user accounts that you created using the Manager and Night Shift employee templates (in Lesson 1). Use one of the following methods:

   To select accounts in random order, click the first account, hold down the CTRL key, and then click the remaining accounts.

   –or–

   To select accounts in consecutive order, click the first account, hold down the SHIFT key, and then click the last account.
3. On the **User** menu, click **Properties**.

   The **User Properties** dialog box appears with both of the user account names listed in the **Users** box.
4. Click **Dialin.**

   The **Dialin Information** dialog box appears.
5. Select the **Grant dialin permissions to user** check box and then click **OK** twice to apply your changes.
6. View the properties of each account to verify that the Dialin permission has been granted.

Lesson Summary

The following information summarizes the key points in this lesson:

- Modify multiple user accounts at one time by selecting multiple user accounts and then modifying the properties. This method is especially useful for moving user home folders to a different server or volume.

For more information on	See
User accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*. Chapter 2, "Setting Up User Accounts," in this book.

Lesson 4: Maintaining Domain Controllers

Maintaining domain controllers means making sure that a primary domain controller (PDC) is always online and that all copies of the directory database are current.

This lesson provides an overview of the procedures required to maintain domain controllers when a PDC needs to be taken offline, and when a PDC goes offline unexpectedly.

After this lesson, you will be able to:

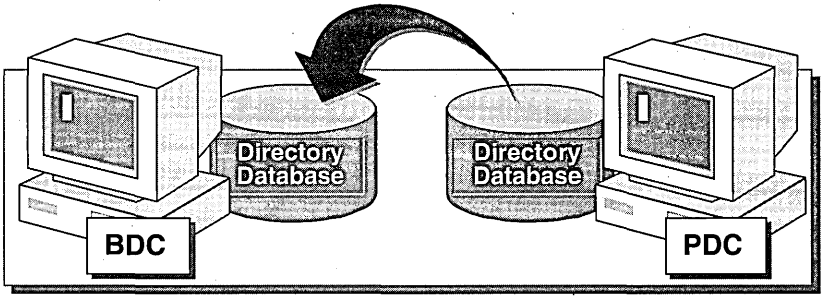
- Describe the function of Server Manager.
- Promote a backup domain controller to a primary domain controller.
- Restore a primary domain controller.
- Synchronize domain controllers.

Estimated lesson time: 20 minutes

If your PDC goes offline for any reason, you need to perform a series of tasks to be sure that your security account database is maintained. The PDC maintains the master copy of the domain's directory database.

If the PDC goes offline, users can still log on, but you can no longer administer accounts. Maintaining domain controllers means making sure that a primary domain controller (PDC) is always online and that all copies of the directory database are current.

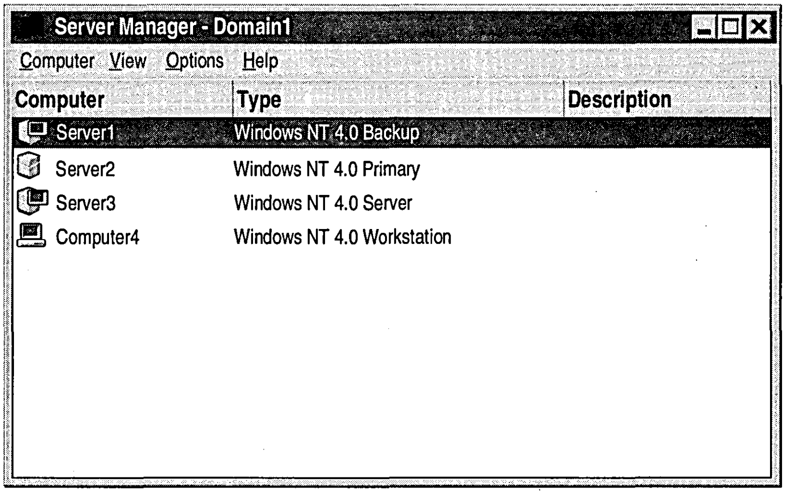
Every domain has only one PDC. The PDC maintains the master copy of the domain's directory database. The directory database is automatically replicated to all the backup domain controllers (BDCs) in the domain every five minutes.



If the PDC goes offline for any reason, users will still be able to log on and be validated by the BDC. But you will no longer be able to do any account administration.

Server Manager

Server Manager is a Windows NT Server tool that you can use to maintain domain controllers. Using Server Manager, you can promote a backup domain controller to become the primary domain controller, synchronize servers with the primary domain controller, and add computers to and remove computers from the domain. To start Server Manager, click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Server Manager**.



Computer	Type	Description
Server1	Windows NT 4.0 Backup	
Server2	Windows NT 4.0 Primary	
Server3	Windows NT 4.0 Server	
Computer4	Windows NT 4.0 Workstation	

The following information appears in the Server Manager window for the current domain:

- The computer name and the operating system and version it is running.
- An icon indicating whether the computer is a primary domain controller, a backup domain controller or member server, or a computer running Windows NT Workstation or another client.

  In the previous illustration, the icon for Server1 and Server3 indicates a backup domain controller or a member server. The icon for Server2 indicates a primary domain controller. The icon for Computer4 indicates a computer running Windows NT Workstation or another client.
- If a computer is not running, the icon for the computer appears dimmed.
- A description (configured during installation).

When the PDC Needs to Be Taken Offline

When you need to take a PDC offline, perform the following tasks:

- ❑ Promote a BDC to take the place of the PDC while its offline. This will force the PDC to become a BDC. When you promote a BDC, an up-to-date copy of the domain directory database is replicated from the old PDC to the new one. The original PDC is automatically demoted to a BDC.
- ❑ When the original PDC is brought back online, promote it back to a PDC, which forces the temporary PDC to demote itself to a BDC.

Scenario

Your PDC needs to be taken offline for some routine maintenance. You will use Server Manager to promote a BDC to a PDC while demoting the original PDC to a BDC. When this is accomplished, you can then take the original PDC offline for maintenance.

Note For this lesson, you use the Server Manager Simulation. This is a program that simulates a BDC in a domain.

▸ **To promote a BDC to a PDC**

1. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Server Manager Simulation.**
2. In the **Server Manager Simulation** dialog box, click **Promoting a BDC When the PDC Needs to Be Taken Offline.**

   The Server Manager window appears.

   Notice that the current BDC is Server1 and the current PDC is Server2.
3. Select the BDC, and then on the **Computer** menu, click **Promote to Primary Domain Controller.**

   The following message appears:

   ```
   Promoting Server1 to Primary may take a few minutes.
   Promoting Server1 will also close client connections to Server1 and
   to the current domain controller (if any). Press 'Help' for details
   if either machine is a Remote Access server.
   Do you want to make the change?
   ```

4. When prompted for confirmation of the change, click **Yes**.

   The Server Manager status box appears. Notice the following actions as they occur during the promotion.

   ```
   Synchronizing Server1 with its primary domain controller
   Synchronizing Server1 with its primary
   Stopping Net Logon Service on Server1
   Stopping Net Logon Service on Server2
   Changing Server2's role to Backup
   Changing Server1's role to Primary
   Starting Net Logon service on Server2
   Starting Net Logon service on Server1
   ```

   When this procedure is finished, the original PDC (Server2) automatically becomes a BDC.

▸ To return the BDC to PDC status

1. In the Server Manager window, select Server2 (the original PDC).
2. Promote the BDC to a primary domain controller.

   The following message appears:

   ```
   Promoting Server2 to Primary may take a few minutes.
   Promoting Server2 will also close client connections to Server2 and
   to the current domain controller (if any). Press 'Help' for details
   if either machine is a Remote Access server.
   Do you want to make the change?
   ```

   The Server Manager status box appears. Notice the following actions as they occur during the promotion.

   ```
   Synchronizing Server2 with its primary
   Stopping Net Logon Service on Server2
   Stopping Net Logon Service on Server1
   Changing Server1's role to Backup
   Changing Server2's role to Primary
   Starting Net Logon service on Server1
   Starting Net Logon service on Server2
   ```

   Notice that the current PDC (Server1) was automatically demoted to a BDC.

When a PDC Goes Offline Unexpectedly

When a PDC goes offline unexpectedly, you need to perform the following steps:

□ Promote a BDC to take the place of the PDC.

□ Once the original PDC is fixed and brought back online, demote it to a BDC. This will force the temporary PDC to become a BDC.

□ Promote the original PDC again.

Scenario

Your primary domain controller goes offline unexpectedly. The computer failed, and when you ran diagnostics on it, you discovered that some of the memory was corrupted. It will take a week before you can get the replacement memory chips, and users need access to their files on the network.

▸ To promote a BDC to PDC when the PDC is already offline

1. In the **Server Manager Simulation** dialog box, click **Promote a BDC When the PDC Goes Offline Unexpectedly.**

   The Server Manager window appears.

   Notice that the current BDC is Server2 and the current PDC is Server1. The PDC icon appears dimmed because it is currently offline.

2. In **Server Manager**, select the BDC.
3. On the **Computer** menu, click **Promote to Primary Domain Controller.**

   The following message appears:

```
Promoting Server2 to Primary may take a few minutes.
Promoting Server2 will also close any client connections to Server2
and to the current domain controller (if any). Press 'Help' for
details if either machine is a Remote Access server.
Do you want to make the change?
```

4. Click **Yes.**

   The following message appears:

```
Cannot find the Primary for domain_name. Continuing with the
promotion may result in errors when domain_name's old Primary comes
back online. Do you want to continue with the promotion?
```

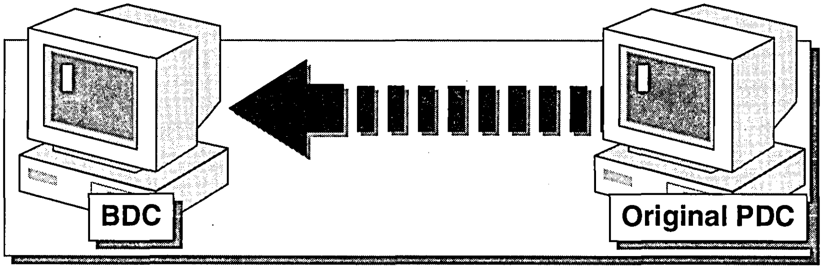
5. Click **OK.**

   The Server Manager status box appears. Notice the following actions as they occur during the promotion.

```
Stopping Net Logon Service on Server2
Changing Server2's role to Primary
Starting Net Logon service on Server2
```

Restoring the Original Domain Controller Roles

If your PDC goes offline and you promote a BDC to be the PDC, you may want to restore the original PDC. To do this, you will need to demote the current PDC.



You can also promote a BDC to a PDC after the PDC has gone offline, but the PDC will not automatically be demoted. Also, because the PDC is offline, no automatic replication of the accounts database can occur between the two PDCs.

When the original PDC is brought back online, there is already a PDC in the domain, so its Net Logon service will fail to start. You will need to restore the original PDC.

▸ **To restore the original PDC to the role of PDC**

1. In the **Server Manager Simulation** dialog box, click **Restoring the Original Domain Controller Roles.**

   The Server Manager window appears.

   Note If this were not a simulation, you would start Server Manager on the computer that was originally functioning as the PDC.

   Notice that both the original and the current PDC are listed as primary domain controllers, but the icon for the original PDC (Server2) is unavailable. The Net Logon service on the original PDC was not started at system boot when the original PDC detected that a PDC was already running on the network; with the Net Logon service stopped; the original PDC cannot validate logon requests.

2. Select the original PDC.
3. On the **Computer** menu, click **Demote to Backup Domain Controller**.

   The following message appears:

```
Demoting Server2 to Backup Domain Controller may take a few minutes.
Demoting Server2 will also close client connections to Server2. Press
'Help' for details if Server2 is a Remote Access server.
Do you want to make the change?
```

4. When prompted, click **Yes** to make the change.

   The Server Manager status box appears. Notice the following actions as they occur during the promotion.

5. Try to start the Net Logon service on Server2.

   The PDC is demoted to a BDC and the Net Logon service is started. Now Server2 is a functioning BDC in the domain as indicated by its icon.

6. Select the BDC that was the original PDC, and on the **Computer** menu, click **Promote to Primary Domain Controller**.

   The following message appears:

   ```
   Promoting Server2 to Primary may take a few minutes.
   Promoting Server2 will also close client connections to Server2 and
   to the current domain controller (if any). Press 'Help' for details
   if either machine is a Remote Access server.
   Do you want to make the change?
   ```

7. Click **Yes** to make the change. Notice the following actions.

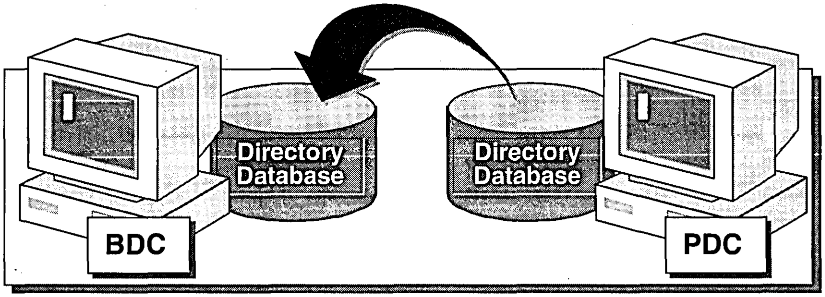
   ```
   Synchronizing Server2 with its primary
   Stopping Net Logon service on Server2
   Stopping Net Logon service on Server1
   Changing Server1's role to Backup
   Changing Server2's role to Primary
   Starting the Net Logon service on Server2
   Starting the Net Logon service on Server1
   ```

   Observe that the original BDC is demoted back to BDC. Also, notice that you receive messages indicating that the directory database on the current PDC was synchronized with the directory database on the current BDC before it is promoted to a PDC.

   If any administration, such as adding user accounts or changing passwords, was done while the original PDC was down, this automatic synchronization of the directory databases ensures that these changes are not lost.

Synchronizing Domain Controllers

Synchronizing domain controllers ensures that all directory databases in the domain are up-to-date. By default, Windows NT synchronizes domain controllers every few minutes. You may want to synchronize domain controllers manually after you make changes to an account database, to apply the changes immediately.



The greater the number of BDCs, the longer it takes to synchronize them.

You can manually synchronize domain controllers for the following reasons:

- To apply changes made to the domain's directory database immediately.
- To solve problems related to password mismatches. If users change their passwords, it takes time for new passwords to be distributed automatically to all the BDCs in a large domain.

▸ **To synchronize a BDC with the PDC**

1. In the **Server Manager Simulation** dialog box, click **Synchronizing Domain Controllers.**

   The Server Manager window appears.

   Notice that the current BDC is Serverl and the current PDC is Server2.

2. Select the BDC, and then on the **Computer** menu, click **Synchronize with Primary Domain Controller.**

   The following message appears:

   ```
   Resynching Serverl with its Primary may take a few minutes. Do you
   want to make the change?
   ```

Note If there are multiple BDCs in the domain, you can synchronize all of them by clicking **Synchronize Entire Domain.**

3. Click **Yes** to make the change.

   The following message appears:

   ```
   Backup Domain Controller Server1 will synchronize its account
   database with the Primary Domain Controller. Check the Event Log on
   Backup Domain Controller Server1 and on the Primary Domain Controller
   to determine whether synchronization was successful.
   ```

4. Click **OK**.
5. On the **Computer** menu, click **Exit**.
6. In the Server Manager Simulation window, click **Exit**.

Verifying the Synchronization

You can determine if a synchronization is successful by using Event Viewer to view the system log for Net Logon events.

Note The Server Manager Simulation does not generate any system log events, so you will not be able to view the Net Logon service events resulting from the previous procedures.

To view the system log, follow these steps:

1. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**.
2. On the **Log** menu, click **System**.

   The System event log appears.

3. Under **Source**, select the most recent NETLOGON event.
4. On the **View** menu, click **Detail**.
5. Read the event details by clicking **Next**, until you find confirmation of synchronization.
6. Exit Event Viewer.

About Windows NT Services

Most of the functionality of Windows NT is implemented as a service. For example, the Workstation service must be running before you can connect to resources on other computers; the Server service must be running before you can share resources. On domain controllers, the Net Logon service must be running before user logon attempts can be validated.

Some services are dependent on other services. For example, the Server service must be started before the Net Logon service can start.

You can determine which services are running by typing **net start** from a command prompt, by starting the Services program in Control Panel, or in Server Manager by clicking **Services** on the **Computer** menu.

Lesson Summary

The following information summarizes the key points in this lesson:

- Maintaining domain controllers means making sure that a primary domain controller (PDC) is always online and that all copies of the directory database are current.
- Administrators must be able to perform a series of tasks to ensure that the network security account database is maintained if the PDC goes offline for any reason.
- When a PDC needs to be taken offline, promote a backup domain controller (BDC) to take its place.
- When a PDC goes offline unexpectedly, temporarily promote a BDC to take its place. Once the original PDC is repaired and brought back online, demote it to a BDC and promote the original PDC again.

For more information on	See
Promoting and demoting domain controllers	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.
The Net Logon service	Chapter 2, "Network Security and Domain Planning," in the *Networking Guide* of the *Microsoft Windows NT Server Resource Kit.*

Lesson 5: Troubleshooting Logon Problems

One of the most common problems that users encounter is the inability to log on to the network successfully. This lesson describes the error messages and solutions to common user logon problems.

After this lesson, you will be able to:

- Identify and troubleshoot logon problems.

Estimated lesson time: 20 minutes

The following table describes common error messages and solutions to logon problems.

User error message	Solution
The system could not log you on. Make sure your user name and domain name are correct, and then type your password again. Letters in passwords must be typed using the correct case. Make sure that CAPS LOCK is not accidentally on.	Verify that the user name, domain name, and password are correct; check the CAPS LOCK key—passwords are case sensitive. (The domain name can be verified using the Network program in Control Panel.) If a user has forgotten the password, delete or reset the user's password. If the user account is new, it may not have been synchronized with BDCs. Synchronize domain controllers.
A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes made to your profile since you last logged on may not be available.	Check to see if this is the only computer having difficulty. Verify that domain controllers are online. If the PDC is still online, select a BDC and promote it to a PDC. If the PDC is offline, promote a BDC to a PDC. If it is the only computer having the problem, verify that a cable connects the computer to the network. Check the network adapter card. If the network adapter has a light on or is blinking. If the problem is not obvious, restart the computer.
Your account has time restrictions that prevent you from logging on at this time. Please try again later.	The logon hours for the user are not allowed for the current time. To allow a user to log on, modify the user's logon hours.
Your account is configured to prevent you from using this workstation. Please try another workstation.	The user has been restricted from using that workstation. To allow the user to use the workstation, modify the Logon To restrictions.

Troubleshooting User Logon Problems

In the following procedures, you troubleshoot two problems related to users logging on to the network. You produce each problem by running a batch file.

Scenario 1

You have just added a new user account, and you want to test it before allowing the user to use the account. The user account is *PDC1* and the password is *password.*

▶ **To produce the problem**

1. Log on as Administrator.
2. Start Windows NT Explorer, expand the LabFiles folder and double-click Scenario1.cmd.

   A Command Prompt window opens briefly and then closes automatically. The screen is blank to prevent you from guessing the answer to the scenario as it is being created.

▶ **To test the problem for Scenario 1**

- Log off and then log on as PDC1.

  What is the symptom of the problem?

  ____

  ____

▶ **To solve the problem for Scenario 1**

- Use User Manager for Domains to determine the problem and solve it.

  What is the problem?

  ____

  ____

  What is the solution to the problem?

  ____

  ____

Scenario 2

A user needs to change her password, but is having problems logging on. The user account is *PDC2* and the password is *password.*

▸ **To produce the problem**

1. Log on as Administrator.
2. In Windows NT Explorer, expand the LabFiles folder, and double-click Scenario2.cmd.

   A Command Prompt window opens briefly and then closes automatically. The screen is blank to prevent you from guessing the answer to the scenario as it is being created.

▸ **To test the problem for Scenario 2**

- Log off and then log on as PDC2 (the name specified in the scenario).

  What is the symptom of the problem?

▸ **To solve the problem for Scenario 2**

- Use User Manager for Domains to determine the problem and solve it.

  What is the problem?

  What are possible solutions to the problem?

Lesson Summary

The following information summarizes the key points in this lesson:

- Always verify that the user typed the user name, domain name, and password correctly, and that he or she used the correct case for the password. This is the most common problem.
- If the user name, domain name, and password are correct, check the restrictions set on the account.
- If other users have problems logging on, make sure that the domain controller is functioning properly.

For more information on	See
How the user logon process works	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.

Note If you want to remove the accounts that were created by running the Chapter4.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter4.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. When and why would you create a template for creating new user accounts?

   ____

   ____

2. What is included in the account policy and why is it important?

   ____

   ____

3. If your PDC goes offline unexpectedly, what do you need to do to maintain the directory database?

   ____

   ____

4. What are some possible reasons why a user cannot log on?

   ____

   ____

Answer Key

Procedure Answers

Page 133

▸ **To determine the inherent rights that are assigned to Account Operators**

2. In the **Right** box, select each user right one at a time to determine which of the following rights are automatically assigned to the Account Operators group, and then mark the check boxes that apply in the following list:

   Log on locally and Shut down the system are inherent rights of the Account Operators group.

Page 137

▸ **To determine which account options were copied**

- In the User Manager window, double-click the user account that you created using the night shift employees template. Compare the following options with the template account. In the following list, mark the check boxes next to those options that were copied:

  All options were copied except for Username, Full Name, Password, Confirm Password, and Account Disabled.

Page 168

▸ **To plan an account policy**

Suggested answers:

Maximum Password Age: 28–31 days.

Minimum Password Age: 7–14 days.

Minimum Password Length: 8–10 characters.

Password Uniqueness: Remember 6–24 passwords.

Lockout after 3–5 bad logon attempts. Reset count after 15–30 minutes.

Lockout Duration: Forever. The administrator should unlock accounts.

Select the Forcibly Disconnect Remote Users From Server When Logon Hours Expire check box.

Page 145

▸ **To test the account lockout portion of the account policy**

4. Now log on with the correct password.

   Why were you unable to log on using the correct password?

   Your account has been locked out based on the account policy.

   How should the user solve the problem?

   The user should contact the administrator.

Page 164

▸ **To test the problem for Scenario 1**

- Log off and then log on as PDC1.

  What is the symptom of the problem?

  For the first *x* logon attempts, an error message appeared indicating that the name or password was incorrect. At *x*+1 logon attempts, an error message appeared indicating that the account was locked out.

Page 164

▸ **To solve the problem for Scenario 1**

- Use User Manager for Domains to determine the problem and solve it.

  What is the problem?

  The password was incorrect. It was set up using all uppercase characters, and the user typed all lowercase characters. This is a typical logon problem, even though there is no way for the administrator to know if the user typed the password incorrectly.

  What is the solution to the problem?

  Log on as Administrator and clear or reset the password.

Page 165

▸ **To test the problem for Scenario 2**

- Log off and then log on as PDC2 (the name specified in the scenario).

  What is the symptom of the problem?

  A message appears indicating that the account has been disabled. Once the account is enabled, a new message indicates that the account has expired. Once the account has been made active again, a message appears indicating that the user does not have permission to change his or her password.

Page 165

▸ **To solve the problem for Scenario 2**

- Use User Manager for Domains to determine the problem and solve it.

  What is the problem?

  The account has been disabled. The account expired at the end of 1995. The user has been restricted from changing the password.

  What are possible solutions to the problem?

  Log on as Administrator, and then change the user properties to enable the account.

  Log on as Administrator, and then set the account to never expire.

  Log on as Administrator, and then change the password for the user, or enable the user to change the password.

Page 167

Review Answers

1. When and why would you create a template for creating new user accounts?

   Create templates when you need to create new user accounts that have similar requirements.

2. What is included in the account policy and why is it important?

   Account Policy settings include password and account lockout options. The account policy is important because the selections you make will determine how secure your network is.

3. If your PDC goes offline unexpectedly, what do you need to do to maintain the directory database?

   Initially, promote a BDC to a PDC. When the original PDC goes back online, you restore the original PDC, which automatically demotes the temporary PDC.

4. What are some possible reasons why a user cannot log on?

   Possible reasons include the following: password not entered correctly, workstation restrictions set for the user account, or the computer is not connected to a domain controller.

CHAPTER 5

Securing Network Resources with Share Permissions

About This Chapter

Shared folders give users centralized access to network files. This chapter explains how to share folders and how to assign permission for gaining access to the shared folders to user and group accounts.

The hands-on procedures give you an opportunity to plan and share folders and to secure them with permissions.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- The knowledge and skills covered in Chapter 3, "Setting Up Group Accounts."
- A user account named SalesRep5. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter5.cmd to create this account.

Lesson 1: Introduction to Shared Folders

Windows NT enables you to designate disk resources that you want to share with others. For example, when a folder is shared, authorized users can make connections to the folder (and access its files) from their own computers. This lesson introduces you to shared folders and how they are used.

After this lesson, you will be able to:

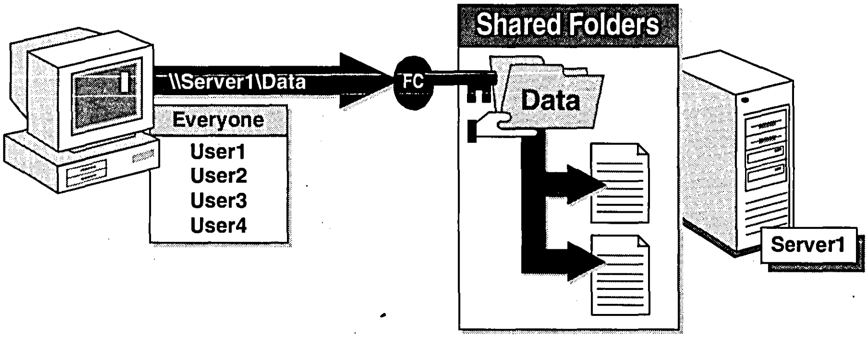
- Explain the situations in which shared folders are used.
- Describe the four levels of share permissions.
- Describe the result when share permissions are applied.

Estimated lesson time: 20 minutes

What Are Shared Folders?

Shared folders give network users centralized access to network files. When a folder is shared, all users by default can connect to the shared folder and gain access to the folder's content.

You can assign *share permissions* to user and group accounts to control what users can do with the content of a shared folder. For example, if you want a user to only view files, you can assign the user's account (or a group of which the user is a member) the Read permission; if you want a user to modify and add new files and folders, you can assign the Change permission.



A shared folder appears in Windows NT Explorer and My Computer as an icon of a hand holding the shared folder and is often referred to simply as a *share*.

Note By default, the built-in Everyone group is automatically assigned Full Control permission to all shared folders.

Why Share Folders?

Shared folders are used to give users access to network programs, data, and user home folders:

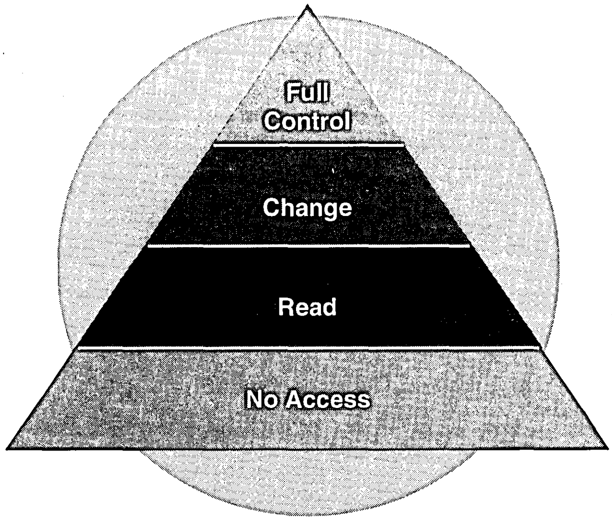
- Network program folders centralize administration by designating one location for configuring and upgrading software. In this way, you avoid maintaining programs on clients.
- Data folders provide a central location for users to store and access common files.
- User home folders provide a central location for users to store their own files. If home folders are stored on a network server, they provide a central location for maintaining and backing up users' data.

Note If the volume where the folder is located is formatted as FAT (file allocation table), share permissions are the only way to secure disk resources. If the volume is formatted with the Windows NT File System (NTFS), NTFS permissions can be assigned for additional security. NTFS permissions are covered in Chapter 6, "Securing Network Resources with NTFS Permissions."

Share Permissions

To control how users access a shared folder, you can assign share permissions to users, groups, or both.

The following illustration shows the hierarchy of share permissions, from most restrictive at the bottom to least restrictive at the top.



The following table describes the four share permissions.

This permission	Gives users the ability to
Full Control (default permission to Everyone group)	Modify file permissions. Take ownership of files on NTFS volumes. Perform all tasks permitted by the Change and Read permissions.
Change	Create folders and add files. Change data in files. Append data to files. Change file attributes. Delete folders and files. Perform all tasks permitted by the Read permission.
Read	Display folder names and file names. Display the data and attributes of files. Run program files. Access other folders within that folder.
No Access	Establish only a connection to the shared folder. Access to the folder is denied and the contents do not appear. This is the most restrictive permission, and is useful for high security. The No Access permission overrides other permissions.

Limitations of Share Permissions

Share permissions are effective only when a user connects to the folder over the network. They do not prevent users from gaining access to the folder while sitting at the computer where the folder resides.

On computers running Windows NT Server, where users do not have the Log on locally user right, this is not a problem. However, on computers running Windows NT Workstation, users are automatically assigned this user right and can bypass share permissions on their local computer.

If the volume where the folder resides is formatted with NTFS, you can secure local resources with NTFS permissions.

How Share Permissions Are Applied

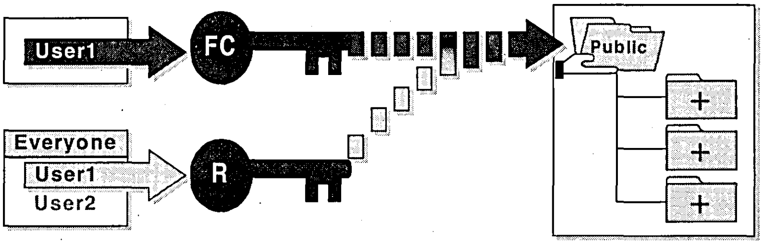
You can assign a user permission to access a shared folder directly or as a member of a group. If you assign different permissions to multiple groups of which the user is a member, the user gets all the permissions, unless one of the permissions is the No Access permission.

There are two rules for how share permissions are applied:

1. When you assign permissions to a user and also to a group of which the user is a member, the user's effective permissions are the least restrictive permissions that result from the combination of the user and group permissions.
2. When you assign the No Access permission, the No Access permission overrides all other permissions that are assigned to the user or to the groups of which the user is a member. No Access always becomes the effective permission.

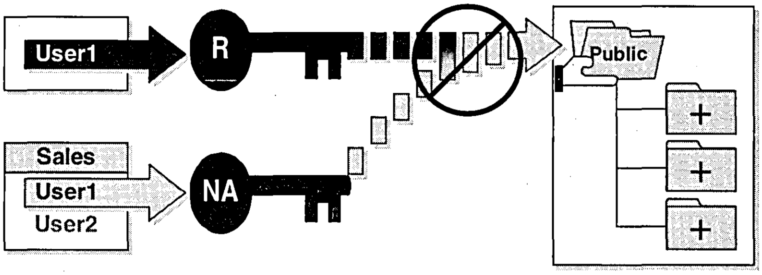
Multiple Permissions

In the following illustration, User1 is assigned the Full Control permission to the shared folder named *Public*. Full Control is the least restrictive permission. User1 is also a member of the Everyone group to which a different permission, Read, is assigned. User1's effective permissions are the combination of the user and group permissions, in this case, Full Control. (Full Control includes the permissions Read and Change.)



The No Access Permission

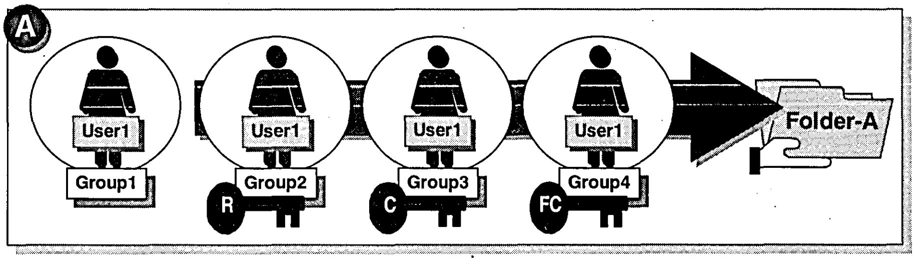
In the following illustration, User1 is assigned Read permission to the shared folder named *Public*. User1 is also a member of the Sales group to which a different permission, No Access, is assigned. Therefore, User1's effective permissions are none because the No Access permission overrides any other permissions assigned to a user or to groups to which the user belongs.



Example of Applied Permissions

The following two illustrations show two examples of applied share permissions. Examine each illustration and determine the effective permissions for User1.

Example A shows that User1 is a member of Group1, Group2, Group3, and Group4. Group1 does not have any permissions for Folder-A. Group2 has Read permission, Group3 has Change permission, and Group4 has Full Control permission for shared Folder-A.

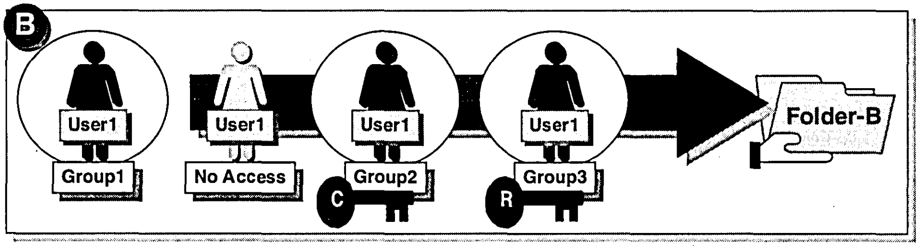


- In Example A, what are User1's effective permissions for Folder-A?

____

____

Example B shows that User1 is a member of Group1, Group2, and Group3. Group1 does not have any permissions for Folder-B. Group2 has Change permission and Group3 has Read permission. Additionally, User1 is assigned the No Access permission.



- In Example B, what are User1's effective permissions for Folder-B?

  ____

  ____

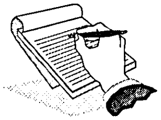
Lesson Summary

The following information summarizes the key points in this lesson:

- Shared folders give network users centralized access to network programs, data, and user home folders.
- Folder permissions are assigned to users, groups, or both, to control how users access a shared folder.
- There are four levels of share permissions: Full Control, Change, Read, and No Access.
- A user's effective permissions are the least restrictive permissions that result from the combination of the user and group permissions.
- The No Access permission overrides all other permissions assigned to a user or to a group to which the user is a member. It always becomes the effective permission.

For more information on	See
Procedures for setting share permissions	Windows NT Help.
Share permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
NTFS permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*. Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.
FAT and NTFS volumes	Chapter 17, "Disk and File System Basics," in the *Microsoft Windows NT Workstation Resource Kit*.
Group accounts	Chapter 2, "Working with User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*. Chapter 3, "Setting Up Group Accounts," in this book.

Lesson 2: Guidelines for Planning Shared Folders



Before you begin sharing folders, you need to determine what resources to share and to whom. For a network to be successful, network programs, public and working data, and user home folders must be easily accessible to authorized users. This lesson presents planning guidelines for shared folders.

After this lesson, you will be able to:

- Outline the tasks required to plan shared folders.
- Plan what permissions to assign to groups or users for network programs, data, and home folders.

Estimated lesson time: 20 minutes

When sharing folders, consider the following points:

- Determine which folders on your servers users are to use, and then organize them so that folders with the same security requirements are located within one folder hierarchy. For example, if users require Read permission to several program folders, store those folders within the same folder.
- Use intuitive share names so that users can easily recognize and locate resources. For example, for the folder *Application,* use the share name *Apps*.
- Use share names and folder names that are readable by all client operating systems. The following table describes share and folder naming conventions.

Client	Share name	Folder name
Windows NT and Windows 95	12 characters	255 characters
MS-DOS, Windows 3.*x*, and Windows for Workgroups	8.3 characters	8.3 characters

Note For client operating systems that can only read 8.3 characters, Windows NT provides 8.3 character equivalent names, but the resulting names are not always intuitive to users. For example, a folder named *Accountants Database*, would appear as *Accoun~1* to clients running MS-DOS, Windows 3.*x*, and Windows for Workgroups.

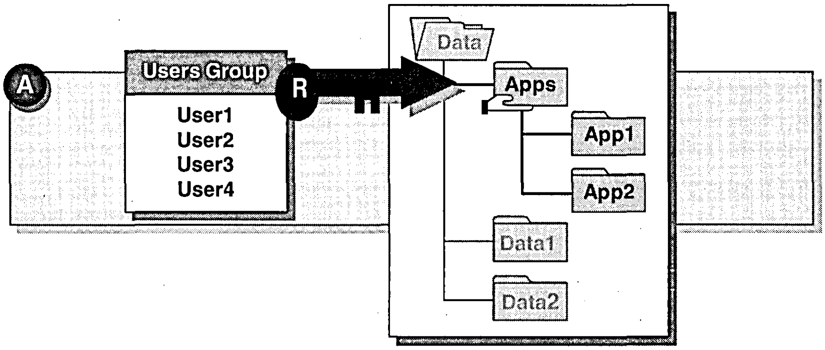
Examples of Shared Folders

How you organize folders may help you to secure data. For example, if you group folders with the same security requirements in one hierarchy, you only have to share the top-level folder. Users with the appropriate permissions have the same level of access to the contents of the shared folder, but cannot access folders that are at a higher level or at the same level as the shared folder.

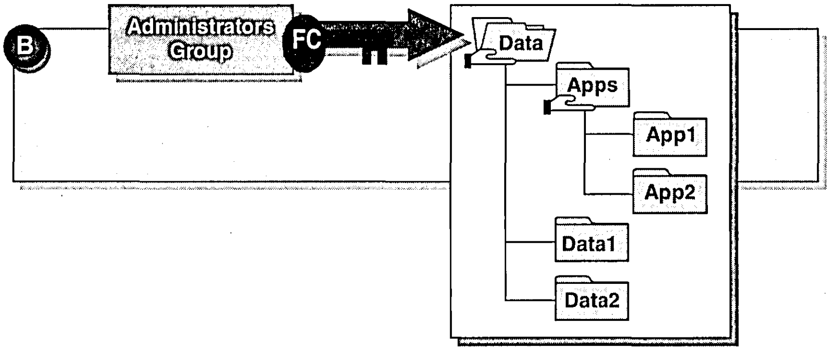
The following illustrations show two examples of how to share folders to secure multiple folder hierarchies.

Example A shows program folders organized in the same hierarchy. In this example, the top-level folder, Apps, is shared. The built-in Users group is assigned the Read permission. When members of the Users group connect to the Apps shared folder, they automatically gain access to App1 and App2 because they are in the same hierarchy. Users will not gain access to the Data, Data1, and Data2 folders because the Data folder is in a different hierarchy.

When users connect to Apps, the Apps shared folder appears to users as a root folder. Users will not be able to see folders that are at a higher level or at the same level as the shared folder to which they are connected.



Example B shows how grouping folder hierarchies can simplify administrative access. For example, if you share the Data folder and assign only the built-in Administrators group the Full Control permission, members of the Administrators group can connect to directly to Data and gain access to the entire hierarchy, including the Apps hierarchy.



Guidelines for Assigning Permissions

When you assign share permissions to users and groups, use the following general guidelines:

- Determine which groups need access to each resource and what level of access they require. For example, for a Sales Data folder, the Sales group may require Change permission, the Administrators group may require Full Control permission, and the Executives group may require Read permission.
- Create a local group on the computer for each shared resource. If the resource resides on a member server or computer running Windows NT Workstation, the local group for the resource is created on that computer. If the resource resides on a domain controller, the local group is created from any computer running User Manager for Domains.
- Assign permissions to only the groups that need access to the resource.
- Assign the most restrictive permission (but one that allows users to perform required tasks) for the resource to the local group.

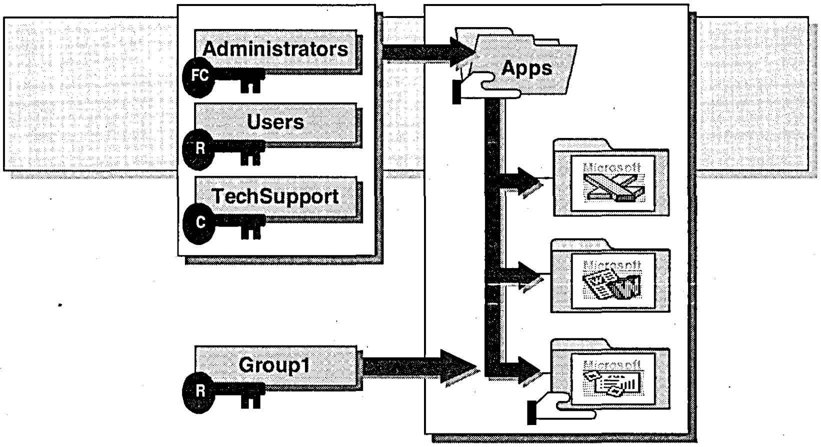
  For example, if users need only to read information in a folder, and they will never delete or create files, then assign the Read permission for those users.
- For greater security, remove the Full Control permission from the Everyone group because the Everyone group contains all user accounts who have access to your network, and Everyone includes the Guest account. If you want all users to have access to the resource, use the Users group instead. In a domain, the Users group only contains domain user accounts that you created. In a workgroup, the Users group contains local user accounts.

Guidelines for Sharing Network Program Folders

In a large network, one or more servers may be dedicated to storing programs. In a small network, one server may be used for both programs and data. The program folders that you share will vary with each network.

Consider these guidelines when planning network program folders:

- Create a shared folder for organizing your programs—for example, Apps.
- Assign the Administrators group Full Control permission to the Apps folder for administrative access.
- Remove the Full Control permission from the Everyone group and assign Read permission to the Users group to provide tighter security.
- Assign the Change permission to groups responsible for upgrading and troubleshooting software.
- Share individual program folders to the appropriate groups only when you need to restrict access to those folders. For example, to give members of Group1 access to only the spreadsheet program, share the folder for the spreadsheet program and assign Group1 the appropriate permission.



Guidelines for Sharing Data Folders

Data folders are used by network users to exchange or share common files. In planning shared data folders, consider creating shared folders for keeping information that is public to employees of the company. Also, consider creating shared folders that employees can use to exchange files with others.

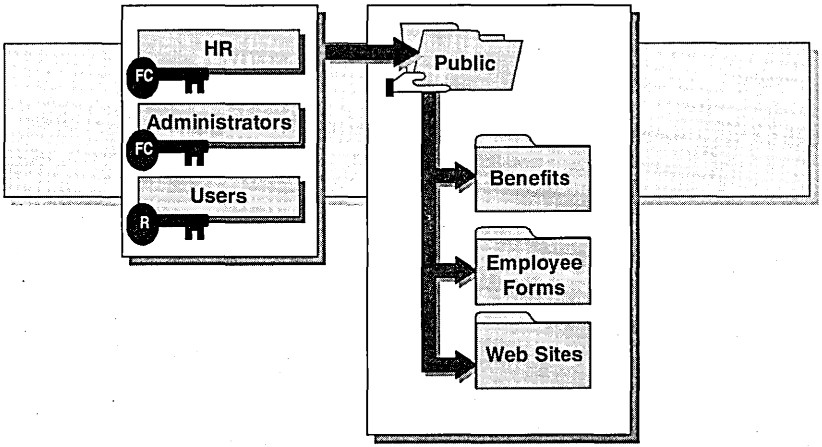
If your hard disk has more than one volume, create and share a data folders on a volume separate from the operating system and programs. Having data folders in one location streamlines backup procedures. Additionally, in the unlikely event that the operating system volume needs to be reformatted, public data will remain intact.

Public Data Folders

Public data folders contain files that employees need to gain access to for reading purposes only—for example, employee benefits information or blank expense report forms.

Consider these guidelines when sharing a public folder:

- Assign the Full Control permission to the users who provide the information in the public folders and to the Administrators group (for administrative access).
- Assign the Read permission to all users who need to gain access to the data.



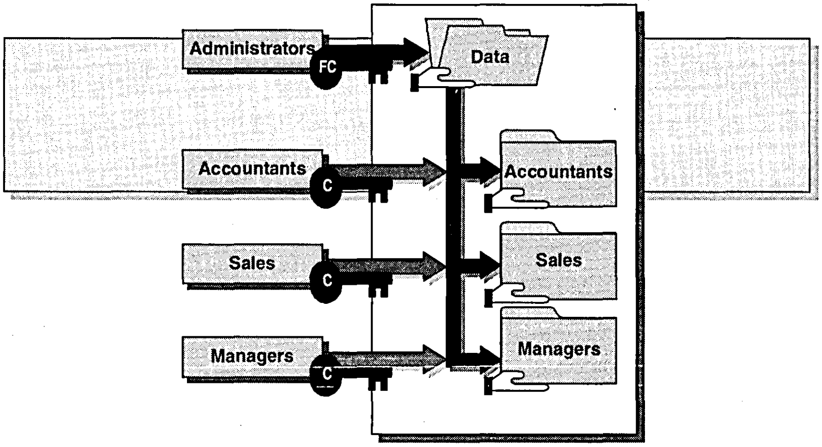
Working Data Folders

Working data folders give employees a central location for storing and exchanging working files. Typically, employees need the ability to add and remove files from common working data folders.

Consider these guidelines when sharing a data folder for working files:

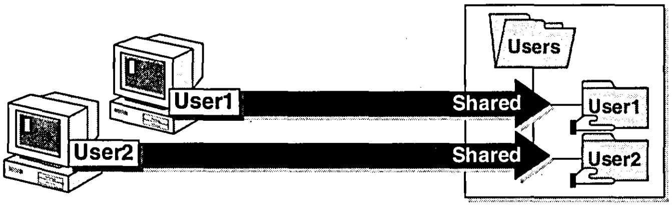
- Assign the Change permission to all users who need to exchange files with others.
- Assign the Full Control permission to the Administrators group.
- Share lower-level data folders to the appropriate groups when you need to restrict access to those folders.

  For example, to protect data in the Accountants folder, share that folder to only the Accountants group and assign that group Change permission. Then, members of the Accountants group can access the Accountants shared folder. Administrators have access by connecting to the Data shared folder.



Guidelines for Sharing Home Folders

On FAT volumes, when you create a user account and you want that user to have a home folder, you must first create a home folder structure on the server. You share individual home folders on a FAT volume because share permissions are the only way to restrict access.



To create home folders for users on a FAT volume using only share permissions to restrict access, follow these general guidelines:

1. Create a central folder named Users on a volume separate from the operating system and programs.

   This streamlines backup and restore procedures. If the operating system volume requires reformatting, the volume containing the home folders will remain intact.

2. Create a folder in the Users folder for each user account, with the same name as his or her user name. For example, for the user name Ericb, create a folder named Ericb.

   Note On a FAT volume, you need to create and share home folders before you specify the home folder path in User Manager for Domains. On an NTFS volume, this step is not necessary.

3. Share each user's home folder and assign *only* the respective user Full Control permission to his or her home folder. This guarantees privacy to the user because he or she is the only person who can connect to his or her home folder. This is the only way to protect users' folders on a FAT volume.
4. In User Manager for Domains, assign a home folder to each user account.
5. Only shared the top-level folder to the Administrators group.

   You will also be able to perform administrative tasks on home folders by logging on to the server locally, or by connecting to an administrative share (C$, D$, and so on), which provides access to the root of the respective volume.

Note Creating home folders on an NTFS volume is covered in Chapter 6, "Securing Network Resources with NTFS Permissions."

▸ To plan shared folders

Scenario: World Wide Importers has opened its first office in Istanbul. As the administrator, you plan how to share resources on servers in the new Istanbul office and make them available to Istanbul office network users as appropriate.

As the administrator, you need to determine:

- Which folders to share and the share name for each folder.
- Whether to create a local group for the resource or to use a built-in local group.
- The appropriate permissions for the members of the local groups.

Record your planning decisions on the "Shared Folders Planning Worksheet" located at the end of this lesson. After completing the exercise, turn to Appendix A, "Planning Worksheets," and compare your worksheet to the sample provided. (The sample presents only one set of possible answers. You may have planned your folders differently.)

To complete the "Shared Folders Planning Worksheet," you need to:

1. Specify the name of the folder that you want shared and record it under Folder Name.
2. Specify the server name and share name for each shared folder, and record it under UNC Name using the universal naming convention format (\\server_name\share_name).
3. Specify a local group for each shared folder. Record it in the Local Group column. For some shared resources, you may want to use the following built-in local groups.

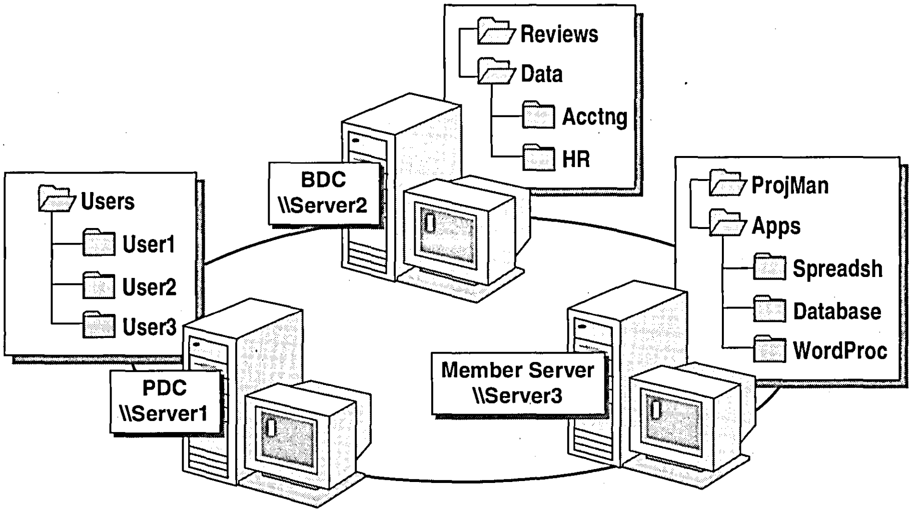
Group	Description
Users	Built-in local group that contains all domain user accounts on each computer.
Administrators	Built-in local group that gives members administrative privileges.

4. List the group accounts that require access to the shared folders and that will become members of the local groups. Record them under Members. The following table describes the group accounts for the Istanbul office.

Group	Description
Managers	Global group that contains all user accounts for the managers.
Executives	Global group that contains all user accounts for the executives.
HR	Global group that contains all user accounts in the Human Resources department.
Accountants	Global group that contains all user accounts for the accountants.

5. Specify the appropriate permissions for members of each local group. Record them under Share Permissions (for example, specify permissions as Read, Change, Full Control, or No Access).

Base your implementation plan on the following illustration and criteria. This illustration shows the PDC, the BDC, and the member server in the Istanbul office along with the folder structure on each server.



Use the following criteria to make your decisions:

- All employees need to run the spreadsheet, database, and word processing programs. Administrators need to administer all folders.
- The managers need to exchange project management files. Administrators need to administer the data.
- The Accounting and Human Resources departments require their own network location to store their working files. Each department will handle its own administration tasks. Executives will need to review the working files.
- Managers and Executives require a network location to store employee performance review forms. All employees need access to these forms. Administrators need to administer the forms.
- User1, User2, and User3 each need a home folder. Each folder must be accessible only by that user. Administrators need to administer all folders.

Note Share names must be accessible from Microsoft Windows NT, Microsoft Windows 95, and non-Windows NT platforms.

Lesson Summary

The following information summarizes the key points in this lesson:

- Determine what resources need to be shared and with whom prior to sharing folders.
- Use intuitive share names so that users can easily recognize and locate resources.
- Use share names and folder names that are readable by all client operating systems.
- Organize disk resources so that folders with the same security requirements are located within one folder hierarchy.
- Create a local group for each shared resource. If the resource resides on a member server or a computer running Windows NT Workstation, create the local group on that computer. If the resource resides on a domain controller, create the local group from any computer running User Manager for Domains.
- Follow the general guidelines provided in this lesson provided in this lesson for assigning permissions to users and groups for shared folders.

For more information on	See
Procedures for sharing a folder	Windows NT Help.
Differences between NTFS and FAT volume security	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
Controlling access to files and folders	Chapter 3, "Disk Management Basics," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*
Protecting files and directories in Windows NT Workstation	Chapter 6, "Windows NT Security," in the *Microsoft Windows NT Workstation Resource Kit.*
Choosing a file system	Chapter 18, "Choosing a File System," in the *Microsoft Windows NT Workstation Resource Kit.*

Shared Folders Planning Worksheet

Folder Name	UNC Name	Local Group	Members	Share Permissions

Lesson 3: Sharing Folders

This lesson guides you through the steps to share folders and assign permissions.

After this lesson, you will be able to:

- Describe the requirements for sharing folders.
- Create and modify shared folders.
- Assign share permissions to users and groups.

Estimated lesson time: 20 minutes

Requirements for Sharing a Folder

To share a folder, you must be a member of the built-in Administrators, Server Operators, or Power Users groups on the computer where the shared folder is being shared.

Note On NTFS volumes, you can give a user the ability to share folders by assigning the user the List permission to the folder.

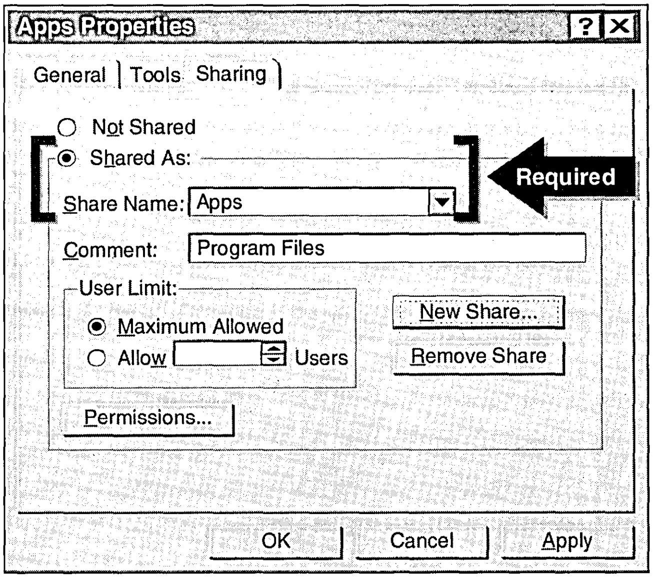
Administrative Shares

Windows NT provides administrative shares to make it easy to gain access to the root of a volume. The root of each volume on a hard disk is automatically shared, using the drive letter appended with a dollar sign ($)—for example C$, D$, E$, and so on. The dollar sign hides the shared folder from users who browse the computer. When you connect to this folder, you have access to the entire volume. You use the administrative shares to remotely connect to the computer to perform administrative tasks.

Note Windows NT also shares the *systemroot* folder as Admin$. This is a special shared folder that is required by the system only during remote administration.

Sharing a Folder

The first step in sharing a folder is to assign it a share name. Share names are assigned on the **Sharing** tab in the *folder_name* **Properties** dialog box.



Apps Properties

○ Not Shared

● Shared As:

Share Name: Apps

Comment: Program Files

User Limit:

● Maximum Allowed

○ Allow ___ Users

The following table describes the **Sharing** tab options.

Option	Description
Share Name	Provides the name that network users will use to connect to the folder. You must enter a share name. If you append a $ to the share name, the share will be hidden from users when they browse network resources.
Comment	Provides a description for the share name. The comment appears in the **Map Network Drive** dialog box when users browse shared folders on a server. It is helpful if this comment clearly identifies the contents of the shared folder.
User Limit	Sets the number of users that can simultaneously connect to the shared folder. Limiting the number of connections can reduce network traffic. The Windows NT Workstation maximum is 10. Windows NT Server is unlimited.
Permissions	Sets the permissions on the folder *only* when it is accessed over the network. The Everyone group is automatically assigned Full Control permission for all new shared folders.
New Share	Appears when the selected folder is already shared. A folder can be shared multiple times with different names and permissions. However, keeping track of multiple share names requires more administration, and in most situations, it is unnecessary.

▸ To share a folder for programs

1. Log on as Administrator, and start Windows NT Explorer.
2. Expand *drive*:\LabFiles, right-click the Apps folder, and then click **Properties**.

   The **Apps Properties** dialog box appears.
3. Click the **Sharing** tab.

   Tip When you right-click the Apps folder, notice that the **Sharing** command appears on the shortcut menu. If you click **Sharing** on this menu, you will switch directly to the **Sharing** tab of the **Apps Properties** dialog box.

4. Click **Shared As.**

   Notice that the default share name is the name of the folder.
5. In the **Comment** box, type **Shared Productivity Programs** and then click **OK.**

   Notice that in Windows NT Explorer, a hand appears under the Apps folder. The hand indicates that the folder is shared.

▸ To share a folder for public data

1. In the LabFiles folder, right-click the Public folder, and then click **Sharing.**

   The **Public Properties** dialog box appears with the **Sharing** tab active.
2. Click **Shared As.**

   Notice that the default share name is the name of the folder.
3. In the **Comment** box, type **Public Files** and then click **OK.**

   Notice that in Windows NT Explorer, a hand appears under the Public folder. The hand indicates that the folder is shared.

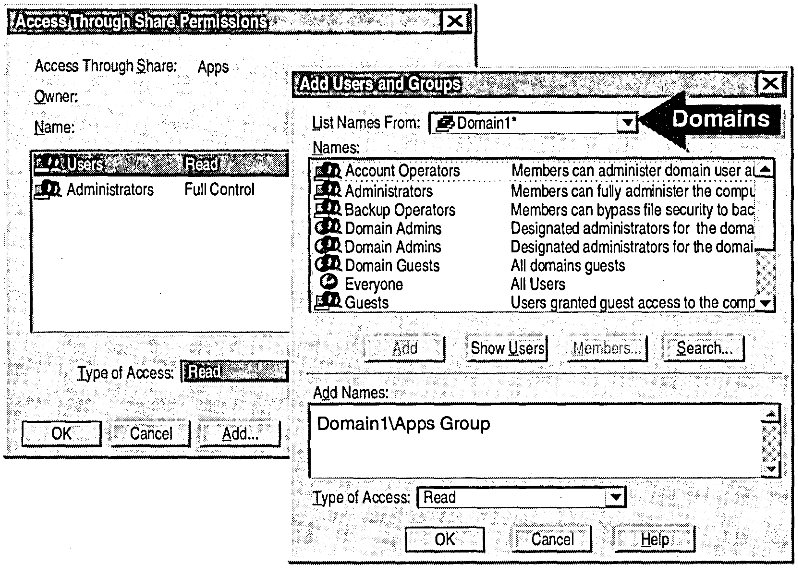
▸ To create a hidden shared folder

1. In the LabFiles folder, create a folder named Secret.
2. Right-click the Secret folder and then click **Sharing.**
3. Click **Shared As.**
4. In the **Shared Name** box, type **secret$** and then click **OK.**

   Notice in Windows NT Explorer that a hand appears under the Secret folder, indicating that the folder is shared.

Assigning Share Permissions

After you assign a share name, the next step is to specify which users can access the shared folder by assigning permissions to selected users or groups. By default, when a folder is shared, the Everyone group is assigned the Full Control permission. For most folders, you will want to remove the Full Control permission from Everyone and assign permissions to specific user and group accounts.



Access Through Share Permissions

Access Through Share: Apps
Owner:
Name:

Users	Read
Administrators	Full Control

Type of Access: Read

Add Users and Groups

List Names From: Domain1*

Names:

Account Operators	Members can administer domain user a
Administrators	Members can fully administer the compu
Backup Operators	Members can bypass file security to bac
Domain Admins	Designated administrators for the doma
Domain Admins	Designated administrators for the domai
Domain Guests	All domains guests
Everyone	All Users
Guests	Users granted guest access to the comp

Add Names:
Domain1\Apps Group

Type of Access: Read

If you want to assign permission to a user or group in a different domain:

- A trust must exist between your computer's domain and another domain on your network. To verify that your computer fits this criteria, log off, press CTRL+ALT+DELETE, and then view the names that appear in the **Domain** box. If more than one domain name appears, a trust relationship exists with the other domains that appear.
- You must have Administrator privileges for that domain. To enable the Administrators group to perform administration tasks in other domains, add the global group Domain Admins to the local Administrators group on the computer in the domain that you want Administrators to administer.

▸ To determine the current permissions for the Apps shared folder

1. In Windows NT Explorer, right-click the LabFiles\Apps folder, and then click **Sharing**.

   The **Apps Properties** dialog box appears.

2. Click **Permissions**.

   The **Access Through Share Permissions** dialog box appears.

   What are the default permissions for the Apps shared folder?

   ____

▸ To remove permissions from a group

- In the **Access Through Share Permissions** dialog box, under **Names**, make sure that **Everyone** is selected, and then click **Remove**.

  The entry disappears.

▸ To assign the Full Control permission to the Administrators group

1. In the **Access Through Share Permissions** dialog box, click **Add**.

   The **Add Users and Groups** dialog box appears.

   Note In a multiple-domain network, click the **List Names From** arrow to reveal other domains from which you can list user and group names for assigning permissions.

2. Under **Names**, click **Administrators**, and then click **Add**.

   Notice that *domain*\Administrators appears in the **Add Names** box. It indicates the location of the directory database where the selected name resides.

3. In the **Type of Access** box, click **Full Control**, and then click **OK**.

   The **Access Through Share Permissions** dialog box reappears. Notice that the Administrators group has Full Control permission.

▸ To assign the Read permission to the Users group

1. In the **Access Through Share Permissions** dialog box, click **Add.**
2. Under **Names**, click **Users**, and then click **Add.**

   The *domain*\Users group appears in the **Add Names** box.
3. In the **Type of Access** box, click **Read**, and then click **OK**.
4. Click **OK** to return to the **Apps Properties** dialog box, and then click **OK** to return to Windows NT Explorer.

▸ To test share permissions by starting a program

1. Log off and log on as SalesRep5.
2. Click the **Start** button, and then click **Run**.
3. In the **Open** box, type \\computer_name\apps (where *computer_name* is the name of your computer).

   The Apps on *computer_name* window appears.
4. Expand the LabFiles\Apps\Games folder, and then double-click Kolumz.exe to start it.

   Were you successful? Why or why not?

   ____

   ____
5. Quit Kolumz.exe.

▸ To test share permissions

1. In the Games window, delete Kolumz.exe.

   Were you successful? Why or why not?

   ____

   ____
2. Quit Windows NT Explorer and log off.

Modifying Shared Folders

You can modify all shared folder options on the *folder_name* **Properties** dialog box.

The following table lists the steps to stop sharing a folder, to modify the share name, and to modify permissions.

To	Do this
Stop sharing a folder	Click **Not Shared** to stop sharing the folder, and then click **OK**. If you stop sharing a folder when a user has a file open, the user may lose data. When you click **Not Shared**, a message appears to notify you that a user is connected to the shared folder.
Modify the share name	Click **Not Shared** to stop sharing the folder. Click **Apply** to apply the change. Then, click **Shared As**, and type in a new share name.
Modify share permissions	Click **Permissions**. In the **Access Through Share Permissions** dialog box, select the user or group whose permissions are to be modified. In the **Type of Access** box, click the permission that you want to apply, and then click **OK**.

Lesson Summary

The following information summarizes the key points in this lesson:

- To share a folder, you must be a member of the built-in Administrators, Server Operators, or Power Users groups on the computer where the shared folder is being shared.
- The first step in sharing a folder is to assign a share name.
- The next step is to assign permissions to users or groups to provide access to the shared folder.
- All shared folder options are set and modified in the *folder_name* **Properties** dialog box.

For more information on	**See**
Organizing disk resources	Chapter 3, "Disk Management Basics," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*
Windows NT security features overview	Chapter 6, "Windows NT Security," in the *Microsoft Windows NT Workstation Resource Kit.*
Trust relationships	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning.*
	Chapter 2, "Network Security and Domain Planning," in the *Networking Guide* of the *Microsoft Windows NT Server Resource Kit.*
Centralizing administration	Chapter 3, "Setting Up Group Accounts," in this book.
Browsing network resources	Chapter 3, "Windows NT Browser Service," in the *Networking Guide* of the *Microsoft Windows NT Server Resource Kit.*

Lesson 4: Connecting to Shared Folders

There are two ways to locate and connect to shared folders. This lesson guides you through the steps to connect to shared folders, and it also explains the differences between the two methods.

This lesson requires that you have completed Lesson 3.

After this lesson, you will be able to:

- Connect to a shared folder using the **Map Network Drive** command.
- Connect to a shared folder using the **Run** command.

Estimated lesson time: 10 minutes

Once you share a folder, network users can connect to it using the **Map Network Drive** command in Windows NT Explorer or the **Run** command on the **Start** menu.

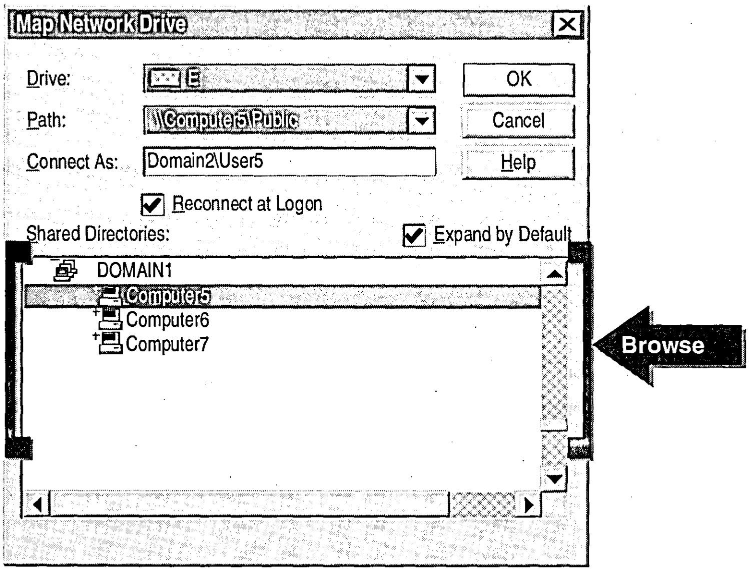
Using the Map Network Drive Command

Using the **Map Network Drive** command to connect to a network resource provides a connection that is retained until the drive letter is manually disconnected, giving you the ability to select the drive from within a program.

You can use the **Map Network Drive** command in Windows NT Explorer, My Computer, and Network Neighborhood. In Windows NT Explorer, on the **Tools** menu, click **Map Network Drive.** In My Computer or Network Neighborhood, right-click the My Computer or Network Neighborhood desktop icons, and then click **Map Network Drive**.

When you connect to a shared folder using the **Map Network Drive** command, the shared folder appears as a drive on your computer, and the contents of the shared folder can be viewed as if they were on your computer. Because the drive letter is saved in a user profile, you can have the connection re-established each time you log on.

You specify the path to a shared folder in the **Map Network Drive** dialog box.



Map Network Drive

Drive: E

Path: \\Computer5\Public

Connect As: Domain2\User5

☑ Reconnect at Logon

Shared Directories: ☑ Expand by Default

DOMAIN1
Computer5
Computer6
Computer7

The following table describes the **Map Network Drive** dialog box options.

Option	Purpose
Drive	Assigns a drive letter to the shared folder so that it appears and functions like a local drive. The user can assign up to 26 drive letters. Drive letters that are used by local devices do not appear in the **Drive** list. If a drive letter is not selected, Windows NT assigns the next available drive.
Path	Specifies the computer where the shared folder resides and the share name assigned to the folder. Use the following format: \\server_name\share_name
Connect As	Connects to a shared folder using a different user account. For example, the administrator is at another user's computer and needs to connect to a resource that the user does not have access to. The **Connect As** option requires the domain name and the user account name in the following format: *domain\user_name* If there is a password on the user account, the user is prompted for it.
Reconnect at Logon	If selected, will reconnect the user to the shared folder each time the user logs on.
Shared Directories	Provides the ability to browse computers in the local and trusted domains for shared folders.

▸ **To connect to a shared folder using Map Network Drive**

1. Log on as SalesRep5.
2. On the desktop, right-click either the My Computer icon or the Network Neighborhood icon, and then click **Map Network Drive**.
3. In the **Drive** box, click **P**.
4. In the Path box, type \\*computer_name***public** (where *computer_name* is the name of your computer).
5. Clear the **Reconnect at Logon** check box, and then click **OK**.
6. Close the Public on '*computer_name*' (P:) window if it appears.
7. Start Windows NT Explorer and view the drives under My Computer.

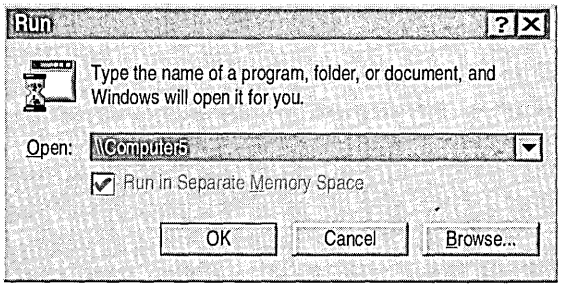
   Notice that drive P has been added as Public on '*computer_name*' (P:).
8. If your computer is connected to a network, use the **Map Network Drive** command to search for and connect to a shared folder on another computer in your network.

Using the Run Command

Using the **Run** command you user can browse all shared folders on a computer without knowing the share name assigned to a specific shared folder. You only need to know the name of the computer.

The Run command does not assign a drive letter to the shared folder, so the connection does not appear within a program.

To use the **Run** command, click the **Start** button, and then click **Run**. In the **Open** box, type the name of the computer where the shared folder resides and the share name assigned to the folder (for example, \\*computer_name**share_name*), or type only the computer name (for example, \\*computer_name*), and then click **OK**.



Type the name of a program, folder, or document, and Windows will open it for you.

Open: \\Computer5

☑ Run in Separate Memory Space

If you only type the computer name, Windows NT opens the *computer_name* window, containing all shared folders on the computer. Clicking a shared folder completes the connection.

▸ **To connect to a network drive using the Run command**

1. Click the **Start** button, and then click **Run**.
2. In the **Open** box, type \\computer_name (where *computer_name* is the name of your computer), and then click **OK**.

   The *computer_name* window appears.
3. Double-click any folder to connect to it.
4. Close the *computer_name* window.
5. If your computer is connected to a network, use the **Run** command to view the shared folders on another computer in your network.
6. Quit Windows NT Explorer.

▸ **To connect to a hidden shared folder using the Run command**

1. Click the **Start** button, and then click **Run**.
2. In the **Open** box, type \\*computer_name***secret$** (where *computer_name* is the name of your computer), and then click **OK**.

   The Secret$ on *computer_name* window appears.
3. Quit Windows NT Explorer.

▸ **To disconnect a network drive using Windows NT Explorer**

1. Start Windows NT Explorer, and then right-click drive P.
2. Click **Disconnect**.

   Drive P is removed from the left pane of Windows NT Explorer and from the User Profile.
3. Quit Windows NT Explorer and log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- You can connect to shared folders using the **Map Network Drive** command or the **Run** command.
- Using the **Run** command, you can browse all shared folders on a computer using only the name of the computer. You do not need to know the share name assigned to a specific shared folder.

For more information on	See
Procedures for opening a shared folder	Windows NT Help.
Mapping a network drive	Windows NT Help.

Best Practices

The following checklist provides the best practices for sharing folders. Review this checklist before you begin to share folders:

□ Organize disk resources so that folders with the same security requirements are located within one folder hierarchy. This simplifies administration by streamlining how you assign permissions.

□ Store all data and home folders on volumes separate from the operating system and programs. This separates data files from system and program files and therefore streamlines backup and restore procedures. In the unlikely event that the operating system volume requires reformatting, the volume containing the data will remain intact.

□ Remove the Everyone group from the permissions list to prevent resource access. Instead, use the local Users group, which provides more security because the group only contains accounts that you created.

□ Create shortcuts for network resources that users will connect to often.

□ Document decisions made about shared folders and assigned permissions. Update this document when changes are made to the server, such as upgrades of software, changes to shared folder names, and changes to assigned permissions.

Note If you want to remove the account that was created by running the Chapter5.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter5.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. What are the requirements to share a folder?

   ____

   ____

2. When a folder is shared, a user with the appropriate permissions has access to: (Circle all that apply.)

   a. All folders in the shared folder.

   b. All files in the shared folder.

   c. Any resource within the network.

   e. Any folder on a volume separate from the operating system.

3. Which, if any, permissions can be assigned to a shared folder? (Circle all that apply.)

   a. Full Control

   b. Change

   c. Read

   d. No Access

   e. All of the above

4. What is the default permission on a shared folder? What group is assigned this permission?

   ____

   ____

Answer Key

Procedure Answers

Page 178

- In Example A, what are User1's effective permissions for Folder-A?

  User1's effective permissions for Folder-A is Full Control. This is because User1 is a member of Group2, which has Read, and Group3, which has Change, and Group4, which has Full Control. Full Control includes the permissions Read and Change, so that when they are combined, User1's permissions equal Full Control. Although Group1 has no specified permissions, User1 still has permission to Folder-A through membership of the other groups.

Page 179

- In Example B, what are User1's effective permissions for Folder-B?

  User1's effective permission for Folder-B is No Access. This is because User1's account has been assigned No Access, which overrides all other permissions.

Page 188

▸ **To plan shared folders**

Strategy used in sample planning worksheet (see Appendix A, "Planning Worksheets"):

Create a local group for each resource that will be restricted to certain users.

Use the built-in local Users group whenever all users require access to a resource. In a domain, the Users group contains all domain user accounts. In a workgroup, the Users group contains all user accounts local to the computer where the folder is located.

Assign the built-in Administrators group the Full Control permission for any folders that its members will manage.

Assign the Change permission to all local group members that need the ability to add, delete, and make changes to working files.

Assign the Read permission to all local group members that only need to review and get copies of files, such as blank expense report forms.

Page 196

▸ **To determine the current permissions for the Apps shared folder**

2. What are the default permissions for the Apps shared folder?

   The group Everyone has Full Control permission.

Page 197

▸ **To test share permissions by starting a program**

4. Were you successful? Why or why not?

   Yes, because SalesRep5 user account is a member of the Users group that has Read access to the Apps share. The Read permissions allows users to run program files.

Page 197

▸ **To test share permissions**

1. Were you successful? Why or why not?

   No, because SalesRep5 has Read permission (as a member of Users) for the Apps folder and therefore cannot delete files.

Page 206

Review Answers

1. What are the requirements to share a folder?

   You must be a member of the built-in Administrators, Server Operators, or Power Users group on the computer where the shared folder is being shared.

2. When a folder is shared, a user with the appropriate permissions has access to: (Circle all that apply.)

   Answers a and b are correct.

3. Which, if any, permissions can be assigned to a shared folder? (Circle all that apply.)

   Answer e is correct.

4. What is the default permission on a shared folder? What group is assigned this permission?

   Full Control is the default permission on a shared folder. The Everyone group is assigned this permission.

CHAPTER 6

Securing Network Resources with NTFS Permissions

About This Chapter

NTFS permissions secure folders and files on the local computer. This chapter explains how NTFS permissions secure local resources. It also explains how NTFS permissions, when they are combined with share permissions, secure resources from users who connect to resources over the network. The hands-on procedures give you an opportunity to plan and implement NTFS permissions, and to troubleshoot common permission-related problems.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- Knowledge and skills covered in Chapter 3, "Setting Up Group Accounts."
- The knowledge and skills covered in Chapter 5, "Securing Network Resources with Share Permissions."
- Shared the LabFiles\Public folder as Public. If the Public folder is not shared, click the **Start** button, click **Run**, type **net share public=***drive***:\labfiles\public** (where *drive* is the location of the LabFiles folder), and then click **OK.**
- Shared the LabFiles\Apps folder as Apps. If the Apps folder is not shared, click the **Start** button, click **Run**, type **net share apps=***drive***:\labfiles\apps** (where *drive* is the location of the LabFiles folder), and then click **OK.**
- Three user accounts created that are named User6, SalesMgr6, and CustomerService6, three global groups created that are named Accountants6, Executives6, and Managers6, and three local groups created that are named Spreadsheet6, Database6, and Library6.

  Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter6.cmd to create these accounts.

Lesson 1: Introduction to NTFS Permissions

On NTFS volumes, you can set NTFS permissions on folders and files. NTFS permissions secure resources on the local computer and when users connect to resources over the network. This lesson provides an introduction to securing resources through NTFS permissions.

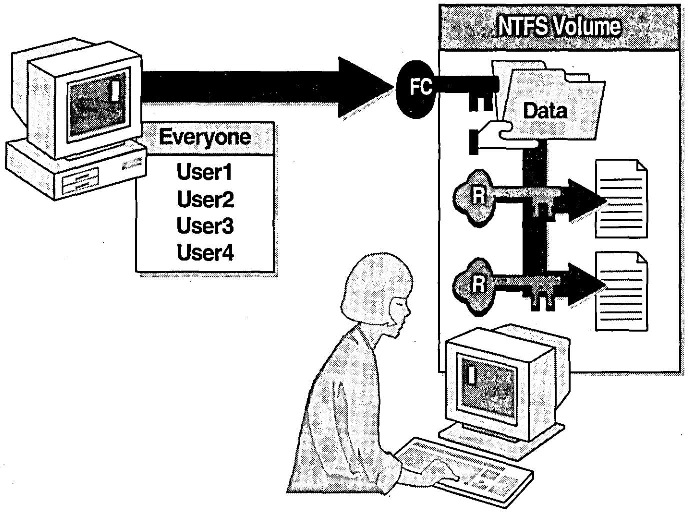
After this lesson, you will be able to:

- Describe the situations that require Microsoft Windows NT file system (NTFS) folder and file permissions.
- Define NTFS folder and file permissions.
- Describe the result when multiple NTFS permissions are applied to a resource.

Estimated lesson time: 20 minutes

What Are NTFS Permissions?

NTFS permissions are permissions that are only available on a volume that has been formatted with the Windows NT file system (NTFS). NTFS permissions provide a greater degree of security because they can be assigned to folders and to individual files. NTFS folder and file permissions apply both to users working at the computer where the folder or file is stored and to users accessing the folder or file over the network by connecting to a shared folder.



Why Use NTFS Permissions?

You use NTFS permissions to protect resources from users who can access the computer in the following ways:

- Locally, by sitting at the computer where the resource is stored.
- Remotely, by connecting to a shared folder.

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

Note When a volume is formatted with NTFS, the Everyone group is automatically assigned Full Control permission to the volume. Folders and files created on the volume inherit this default permission.

Individual NTFS Permissions

Windows NT provides six individual NTFS permissions. Each permission specifies the access that a user or group can have to the folder or file.

The following table describes the actions that a user can take when individual permissions are assigned for a folder or file.

NTFS individual permissions	For a folder, a user can	For a file, a user can
Read (R)	Display folder names, attributes, owner, and permissions.	Display file data, attributes, owner, and permissions.
Write (W)	Add files and folders, change a folder's attributes, and display owner and permissions.	Display owner and permissions, change file attributes, create data in, and append data to, a file.
Execute (X)	Display folder attributes, make changes to folders within a folder, and display owner and permissions.	Display file attributes, owner, and permissions. Run a file if it is an executable.
Delete (D)	Delete a folder.	Delete a file.
Change Permissions (P)	Change a folder's permissions.	Change a file's permissions.
Take Ownership (O)	Take ownership of a folder.	Take ownership of a file.

Note On an NTFS volume, the user who creates a folder or file becomes the owner. If the user is a member of the Administrators group, the Administrators group becomes the owner. The owner can always assign and change permissions on a folder or file.

Standard Permissions

In most situations, you will use the NTFS standard permissions. Standard permissions are combinations of individual NTFS permissions and allow you to assign multiple NTFS permissions at one time.

By assigning combinations of individual permissions at one time, you can simplify your administrative tasks. When you set a standard permission, the abbreviations for the individual permissions appear in the interface beside the standard permission. For example, when you set the standard permission Read on a file, the abbreviation RX appears beside it.

Standard Folder Permissions

The following table lists the standard folder permissions and the individual NTFS permissions that each standard permission represents.

Standard permission	Individual permissions on folders	Individual permissions on files in the folder
No Access	None	None
List	RX	Not specified
Read	RX	RX
Add	WX	Not specified
Add & Read	RWX	RX
Change	RWXD	RWXD
Full Control	All	All

Note No Access means that the user cannot access the folder or file in any way, even if the user is a member of a group that has been granted access to the folder. “Not specified” means that the standard permission does not apply to files.

Standard File Permissions

The following table lists the standard file permissions and the individual NTFS permissions that each standard file permission represents.

Standard permission	Individual permissions
No Access	None
Read	RX
Change	RWXD
Full Control	All

Note The difference between the Full Control permission and the Change permission is that Change does not include the ability to modify permissions or to take ownership of folders and files.

How NTFS Permissions Are Applied

NTFS permissions are assigned to user and group accounts in the same way that share permissions are assigned—a user can be assigned NTFS permissions directly or as a member of one or more groups.

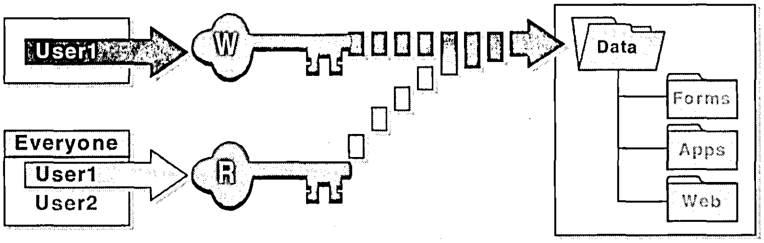
NTFS folder permissions are applied as follows:

- Like share permissions, NTFS permissions provide effective permissions for users that are the combination of the user and group permissions, with the exception of No Access. The No Access permission overrides all other permissions.
- Unlike share permissions, NTFS permissions protect local resources and can be assigned to other folders and files in the same folder hierarchy.

NTFS file permissions take precedence over the permissions assigned for the folder that the file is contained in. For example, if a user has Read permission to a folder and Write permission to a file in that folder, then the user will be able to write to the file, but will be unable to create a new file in the folder.

Example of NTFS Folder Permissions

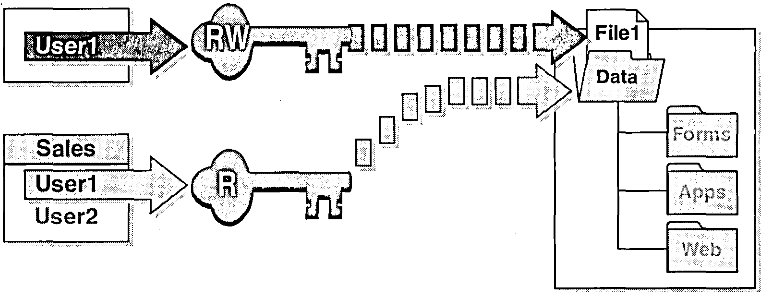
In the following illustration, User1 is assigned the Write permission to the folder named *Data*. User1 is also a member of the Everyone group to which the Read permission is assigned. Therefore, User1's effective permissions are both Read and Write to the Data folder only.



Unlike share permissions, NTFS permissions do not automatically allow User1 to gain access to the other folders within the hierarchy.

Example of NTFS File Permissions

In the following illustration, User1 is assigned the Read and Write permissions to File1 in the folder named *Data*. User1 is also a member of the Sales group to which a different permission, Read, is assigned for the Data folder. User1's effective permission to the Data folder is Read, but is Read and Write to File1 because NTFS file permissions override NTFS folder permissions.



Lesson Summary

The following information summarizes the key points in this lesson:

- NTFS permissions provide a high degree of security to folders and individual files on volumes that have been formatted with the Windows NT file system (NTFS).
- NTFS folder and file permissions apply both to users working at the computer where the folder or file is located and to users accessing the folder or file over the network.
- Like share permissions, NTFS permissions can be assigned to a user directly or as a member of one or more groups.
- Like share permissions, a user's effective permissions are the combination of the user and group permissions, with the exception of No Access. The No Access permission overrides all other permissions.
- Unlike share permissions, NTFS permissions can be assigned to other folders and files in the same folder hierarchy.
- NTFS file permissions take precedence over the permissions assigned for the folder that the file is contained in.

For more information on	**See**
NTFS permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
FAT and NTFS volumes	Chapter 17, "Disk and File System Basics," in the *Microsoft Windows NT Workstation Resource Kit.*
Group accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 2: Combining Share Permissions and NTFS Permissions

Share permissions for NTFS volumes work in combination with file and folder permissions. This lesson explains how share permissions are combined with NTFS permissions to secure disk resources.

After this lesson, you will be able to:

- Describe the result when folder permissions are different from those of the files in the folder.
- Describe the result when share permissions and NTFS permissions are combined.

Estimated lesson time: 20 minutes

To provide users with network access to disk resources, the folders containing those resources must be shared. Once the folder is shared, you can protect it by assigning share permissions to users and groups. However, share permissions offer limited security because they:

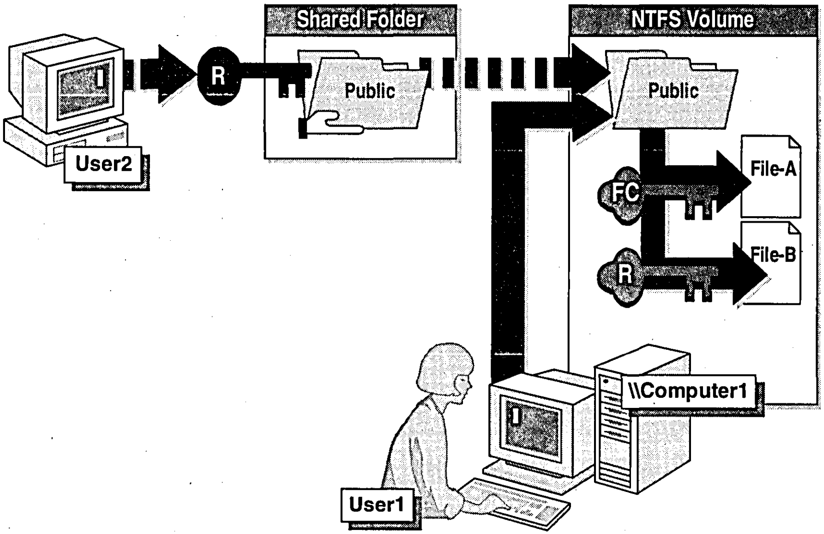
- Give the user the same level of access to all folders and files within the shared folder.
- Have no effect when a user gains access to the resource locally by sitting at the computer where the resource is located.
- Cannot be used to secure individual files.

If the shared folder is on an NTFS volume, you can use NTFS permissions to effectively block or change a user's access to other folders or files in the shared folder hierarchy. You gain the greatest degree of security by combining NTFS permissions with share permissions.

Note The easiest way to combine share permissions and NTFS permissions is to leave the default share permission Full Control assigned to the Everyone group, and then to assign NTFS permissions to specific user and group accounts for the folders and files within the shared folder hierarchy.

When combining share permissions with NTFS permissions, the most restrictive permission *always* becomes the effective permission. For example, if the share permission for a folder is Full Control and the NTFS permission for the same folder is Read, the effective permission is Read because it is the most restrictive.

The following illustration shows that User2 has the share permission Read for the shared folder named Public on Computer1 (when connecting over the network), and the NTFS Full Control permission to File-A. User2's effective permission for File-A is Read because Read is the most restrictive permission. User2's effective permission for File-B is Read because the NTFS Read permission has the same restrictions as the share permission Read.



When User1 sits at Computer1, User1 is not restricted by the share folder permission for the Public folder. However, User1 has the Full Control permission for File-A and the Read permission for File-B because those are NTFS permissions. If User1 connects to the shared folder Public, User1 has the share permission Read to the Public folder just like User2.

Video: Permissions

This five minute video shows the effective permissions when shared folder and NTFS permissions are combined.

▸ **To start the video from the Start menu**

1. Insert the Supplemental Material compact disc into the CD-ROM drive.
2. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Permissions Video**.

▸ To start the video from the compact disc

1. Start Windows NT Explorer.
2. In the root of the Supplemental Material compact disc, double-click Open.htm.
3. Click the center of the screen to continue to the home page.
4. Click **Course Materials.**
5. Under **Contents**, click **Permissions.**
6. Follow the instructions in the text box to install the required DLL files and to start the video.

Note If you completed the Setup procedures described in "About This Book," or if you have run a video on this computer before, you do *not* need to install the DLL files.

▸ To review the video

The following study guide highlights the main points of the video. Complete the guide as you view the video, or use the guide as a follow-up test (recommended).

1. What do shared folders provide access to?

   ____

2. What can share permissions be assigned to?

   ____

3. What can NTFS permissions be assigned to?

   ____

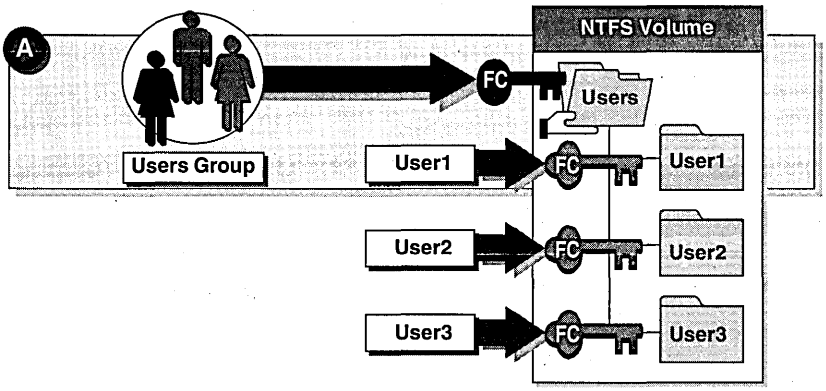
4. When you combine a share permission with an NTFS permission what permission becomes the *effective* permission?

   ____

Example of Combined NTFS Permissions and Share Permissions

The following illustrations show two examples of shared folders that contain folders or files that have been assigned NTFS permissions. Examine each illustration and determine the effective permissions for User1 and User2.

Example A shows that the Users folder has been shared. The Users group has been assigned the share permission Full Control for the Users folder. User1, User2, and User3, however, have been assigned the NTFS permission Full Control for only their own home folder. These users are all members of the Users group.

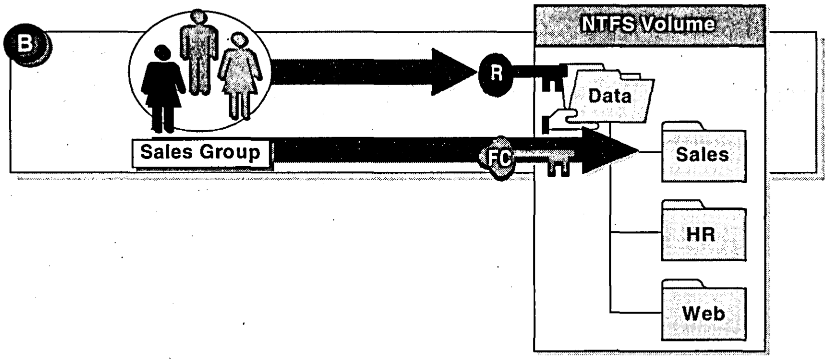


- In Example A, what is User1's effective permission when he or she accesses the User1 folder by connecting to the Users shared folder? What is User2's effective permission for the User1 folder?

____

____

Example B shows that the Data folder has been shared. The Sales group has been assigned the share permission Read for the Data shared folder and the NTFS permission Full Control for the Sales folder.



- In Example B, what are the Sales group's effective permissions when they access the Sales folder by connecting to the Data shared folder?

____

____

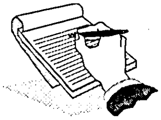
Lesson Summary

The following information summarizes the key points in this lesson:

- You gain the greatest degree of security by using a combination of share permissions and NTFS permissions.
- The easiest way to combine share and NTFS permissions is to leave the default share permission Full Control assigned to the Everyone group, and then assign NTFS permissions to specific user and group accounts for the folders and files within the shared folder hierarchy.
- The most restrictive permission is always the effective permission when share permissions are combined with NTFS permissions.

For more information on	See
Share permissions	Windows NT Help.
NTFS file system	Chapter 3, "Disk Management Basics," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.* Chapter 17, "Disk and File System Basics," in the *Microsoft Windows NT Workstation Resource Kit.*

Lesson 3: Guidelines for Assigning NTFS Permissions



Before you begin assigning NTFS permissions to folders and files, it is best to determine what permissions are required and to whom they should be assigned. This lesson presents guidelines for planning NTFS permissions.

After this lesson, you will be able to:

- Plan what permissions to assign to users or groups for network programs, data, and home folders.
- Outline the tasks required to create home folders on NTFS volumes.

Estimated lesson time: 20 minutes

Guidelines for Planning Program Folders

The following are general guidelines for assigning NTFS permissions to program folders:

- Remove the default NTFS permission Full Control from the Everyone group and assign it to the Administrators group.
- Assign groups that are responsible for upgrading and troubleshooting software the Full Control or Change permission for the appropriate folders.
- If network programs are contained in shared folders, assign the Users group the Read permission.

Guidelines for Planning Data Folders

The following are general guidelines for assigning NTFS permissions to data folders:

- Remove the default permission Full Control from the Everyone group and assign it to the Administrators group.
- Assign the Users group the Add & Read permission and the Creator Owner group the Full Control permission. This gives users who log on locally the ability to delete and modify only the folders and files that they copy or create on the computer.

Guidelines for Planning Home Folders

The following are general guidelines for assigning NTFS permissions to home folders:

- Centralize home folders on an NTFS volume (on a network server) that is separate from programs and the operating system to streamline administration and the backing up of data.
- Use %Username% to automatically assign a user's account name to the folder and to automatically assign the NTFS permission Full Control to the respective user.

Creating Home Folders on an NTFS Volume

A big advantage to storing home folders on an NTFS volume is that you can organize them in one hierarchy and restrict access to the respective users without sharing each folder.

Follow these steps to create home folders on NTFS volumes:

1. Create a folder named *Users* on a volume that is separate from the operating system and programs. By doing so, the home folders will remain intact if the operating system volume requires reformatting.
2. Share the Users folder to provide a single access point for network users and a single administration point for administrators.
3. Remove the default permission Full Control from the Everyone group and assign the share permission Full Control to the Users group.
4. Use the %Username% variable to automatically name home folders using users' user account names. The %Username% variable also automatically assigns the NTFS permission Full Control to the respective user. (On FAT volumes, home folders can only be restricted by share permissions.)
   a. In User Manager for Domains, create a new user account or double-click an existing account.
   b. In the **New User** or **User Properties** dialog box, click **Profile**, and then, in the **Home Directory To** box, type \\*server_name***Users\%Username%**

Tip Educate users to store their personal and work data in their home folders. If users' home folders are stored on a network server and are moved to a different server, only the home folder path will require modification.

▸ To plan NTFS folder and file permissions

Scenario: As the administrator for World Wide Importers, you need to secure disk resources for their Quebec office. In this exercise, you plan your NTFS permissions for a server that all employees need to access. Your goal is to create a plan that will make the needed resources available to network users, and secure these resources according to the needs of the company. You will secure the folders in the hierarchy by using NTFS permissions. (In this scenario, the volume has been formatted with NTFS.)

As the administrator, you need to determine:

- Whether to create a local group for the resource or use a built-in local group.
- What NTFS permissions users will require to gain access to the appropriate folders and files.

Record your planning decisions on the "NTFS Permissions Planning Worksheet" located at the end of this lesson. After completing the exercise, turn to Appendix A, "Planning Worksheets," and compare your worksheet to the sample provided. (The sample represents only one set of possible answers. You may have planned your permissions differently.)

To complete the "NTFS Permissions Planning Worksheet," you need to:

1. Specify the folder or file that requires NTFS permissions. Record it in the Folder or File column.
2. Specify a local group for each resource. Record it under Local Group. For some folders, you may want to use the following built-in groups.

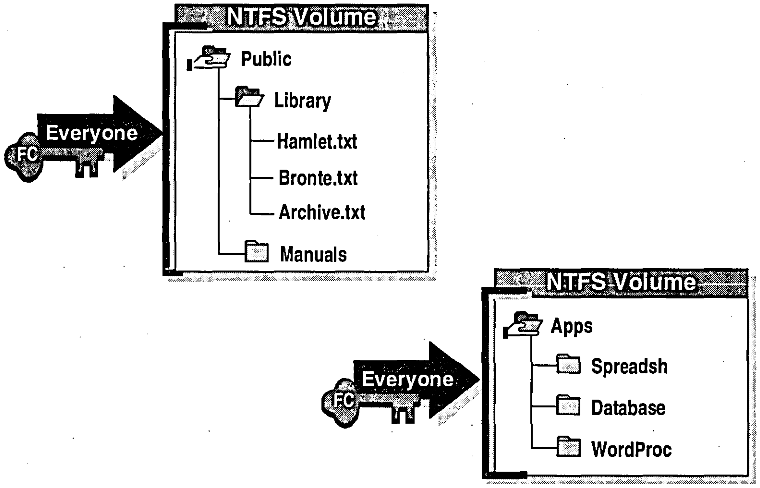
Built-in group	**Description**
Users	Built-in local group that contains all domain user accounts on each computer.
Administrators	Built-in local group that gives members administrative privileges.
Creator Owner	Built-in system group that is used to assign access to the creator and owner of a resource.

3. List the group accounts that require access to the folders and that will become members of the local groups. Record them under Members. The following table describes the group accounts for the Quebec office.

Group	Description
Accountants6	Global group that contains all user accounts for the accountants.
Executives6	Global group that contains all user accounts for the executives.
Managers6	Global group that contains all user accounts for the managers.
Spreadsheet6	Local group for the Spreadsheet program.
Database6	Local group for the Database program.
Library6	Local group for the Library information.

4. Specify the appropriate standard NTFS permissions for members of each local group. Record them under NTFS Permissions (for example, List, Read, Add, Add & Read, Change, Full Control, or No Access).

Base your implementation plan on the following illustration and criteria. The illustration shows the folder hierarchies. Notice that the Public folder and the Apps folder have been shared. The Everyone group has the share permission Full Control.



Use the following criteria to make your decisions:

- Administrators need to administer all folders and files.
- All users need to run programs in the WordProc folder, but they should not be able to modify the files in the WordProc folder.
- Only members of the Accountants6, Managers6, and Executives6 global groups need to run the programs in the Spreadsh and Database folders, but they should not be able to modify the files in those folders.
- All users need to copy their files to the Public folder and then modify only their own files as needed. They all need to read each others files.
- Members of the Managers6 global group need to contribute new files to the Library folder.
- All users need to open and view files in the Library and Manuals folders.
- User6 needs to update the Archive.txt file whenever a new file is added to the Library folder.
- User6 needs to modify files in the Manuals folder, including assigning permissions for files to other users and groups.

Lesson Summary

The following information summarizes the key points in this lesson:

- Determine what permissions are required and to whom they should be assigned before you begin to assign NTFS permissions to folders and files.
- For program folders, assign the Full Control permission to the Administrators group and to groups responsible for upgrading and troubleshooting software. Assign the Read permission to the Users group.
- For data folders, assign the Full Control permission to the Administrators group only. Assign the Users group the Add & Read permission, and assign the Creator Owner group the Full Control permission. This will give users the ability to delete and modify only the folders and files that they copy or create.
- Use %Username% to automatically assign a user's account name to a home folder and to automatically assign the NTFS permission Full Control to the respective user.

For more information on	See
Creating home folders on FAT volumes	Chapter 5, "Securing Network Resources with Share Permissions," in this book.
%Username%	Chapter 2, "Setting Up User Accounts," in this book.
Creator Owner	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.

NTFS Permissions Planning Worksheet

Folder or File	Local Group	Members	NTFS Permissions

Lesson 4: Assigning NTFS Permissions

This lesson guides you through the steps to assign NTFS permissions.

After this lesson, you will be able to:

- Describe the requirements for assigning NTFS permissions.
- Assign NTFS folder and file permissions to user and group accounts.

Estimated lesson time: 30 minutes

Requirements for Assigning NTFS Permissions

To assign NTFS permissions, you need to be the owner of the folder or file, or have one of the following permissions:

- Standard permission: Full Control
- Special access (or individual) permission: Change Permissions
- Special access (or individual) permission: Take Ownership (With this permission a user can take ownership of a folder or file, and then change permissions on the resource.)

Default NTFS Permissions

The following are the default NTFS permissions:

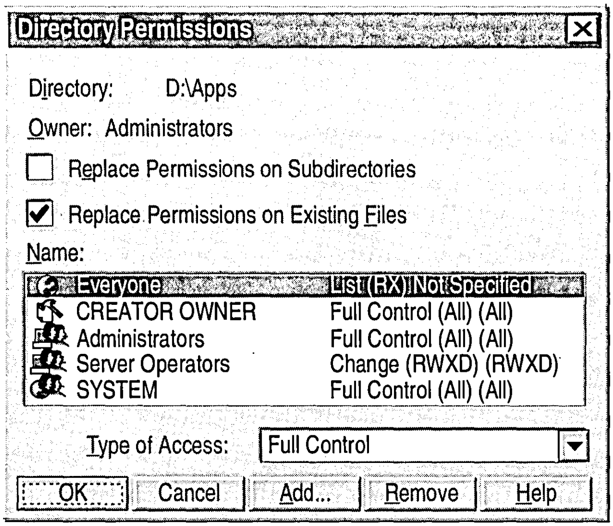
- When a volume is formatted with NTFS, the permission Full Control is automatically assigned to the Everyone group. This gives all users with the Log on locally user right complete access to the volume.
- When a new folder or file is created on an NTFS volume, the folder or file inherits the permissions of the folder that contains it.

Caution When Windows NT is installed on an NTFS volume, NTFS permissions are automatically assigned to some system folders. Do not modify the permissions on system files. For a complete list of these permissions, see Microsoft Windows NT Server *Concepts and Planning*.

Assigning NTFS Folder and File Permissions

You modify permissions by right-clicking the folder or file in Windows NT Explorer, clicking **Properties**, clicking the **Security** tab, and then clicking **Permissions**.

If you are modifying files, the **File Permissions** dialog box appears. If you are modifying folders, the **Directory Permissions** dialog box appears.



Directory: D:\Apps

Owner: Administrators

□ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

Everyone	List (RX) (Not Specified)
CREATOR OWNER	Full Control (All) (All)
Administrators	Full Control (All) (All)
Server Operators	Change (RWXD) (RWXD)
SYSTEM	Full Control (All) (All)

Type of Access: Full Control

The following table describes the **Directory Permissions** or *file_name* **Permissions** dialog box.

Option	Purpose
Replace Permissions on Subdirectories	If selected, changes existing permissions for all folders within the selected folder's hierarchy. This option does not change permissions on existing files in the folder hierarchy. This check box is cleared by default and is an option *only* when assigning folder permissions.
Replace Permissions on Existing Files	If selected, changes existing permissions for all files within the selected folder only. It does not change file permissions for folders within the same folder hierarchy. This check box is cleared by default and is an option only when assigning folder permissions.
Name	Displays the folder or file permissions assigned to a group or user for the resource. The first set of parentheses indicates the folder permissions, and the second set of parentheses indicates the permissions for any new files created in the folder.
Type of Access	Displays the folder or file permissions for the selected group or user in the **Name** box and allows you to change the permission assigned to the selection.

▸ To assign permissions to Users for the Public folder

In this procedure, you assign the Add & Read permission to the Users group and remove the default permissions from the Everyone group.

1. Log on as Administrator and start Windows NT Explorer.
2. Expand the LabFiles folder, right-click the Public folder, and then on the shortcut menu click **Properties.**
3. Click the **Security** tab, and then click **Permissions.**

   The **Directory Permissions** dialog box appears.

   Notice that the Everyone group is assigned the NTFS permission Full Control by default.
4. In the **Directory Permissions** dialog box, click **Add.**

   The **Add Users and Groups** dialog box appears.
5. Make sure that your domain name appears in the **List Names From** box.
6. Under **Names**, click **Users**, and then click **Add.**

   Users appears under **Add Names.**
7. In the **Type of Access** box, click **Add & Read**, and then click **OK.**

   Users appears in the **Directory Permissions** dialog box. Notice that (RWX) (RX) appears next to Add & Read. The first set of parentheses indicates the permissions that apply to the folder; the second set of parentheses indicates the permissions that apply to the files in the folder.
8. Under **Name**, click **Everyone** (if it is not already selected), and then click **Remove.**

   The Everyone group is removed from the list.

▸ To assign permissions to Creator Owner for the Public folder

In this procedure, you assign the Full Control permission to the Creator Owner group so that users will have the ability to modify their own files.

1. In the **Directory Permissions** dialog box, click **Add.**

   The **Add Users and Groups** dialog box appears.
2. Make sure that your domain name appears in the **List Names From** box.
3. Under **Names**, click **CREATOR OWNER**, and then click **Add.**
4. In the **Type of Access** box, click **Full Control**, and then click **OK.**

   The Creator Owner group appears with the Full Control permission in the **Directory Permissions** dialog box.

▸ To assign permissions to Administrators for the Public folder

1. In the **Directory Permissions** dialog box, click **Add**.

   The **Add Users and Groups** dialog box appears.
2. Make sure that your domain name appears in the **List Names From** box.
3. Under **Names**, click **Administrators**, and then click **Add**.
4. In the **Type of Access** box, click **Full Control**, and then click **OK**.

   In the **Directory Permissions** dialog box, notice that the Administrators group and the Creator Owner group have Full Control permission, and that the Users group has the Add & Read permission.
5. Select the **Replace Permissions on Subdirectories** check box so that the permissions will be applied to all folders in the hierarchy.
6. Verify that the **Replace Permissions on Existing Files** check box is selected, and then click **OK**.

   The following message appears:

   ```
   Do you want to replace the security information on all existing
   subdirectories within drive:\LabFiles\Public?
   ```
7. Click **Yes** to return to the **Public Properties** dialog box, and then click **OK** to apply your changes.
8. Use Notepad to create a file named Chapter6.txt in LabFiles\Public.

▸ To test the NTFS permissions assigned for the Public folder

In this procedure, you test NTFS permissions by attempting to open, modify, and delete a file created by two different users.

1. Log on as CustomerService6, and then start Windows NT Explorer.
2. Expand the LabFiles\Public folder.
3. Attempt to create a file in the Public folder.

   Were you successful? Why or why not?

   ____

   ____
4. Attempt to perform the following tasks for the file that you just created. In the following list, mark those which you are able to complete:

   ☐ Open the file

   ☐ Modify the file

   ☐ Delete the file

5. Attempt to perform the following tasks for the Chapter6.txt file created by Administrator. In the following list, mark the task or tasks that you are able to complete:

   ☐ Open the file

   ☐ Modify the file

   ☐ Delete the file

6. Quit all programs and log off.

▶ To assign NTFS permissions

In this procedure, you assign NTFS permissions based on the sample "NTFS Permission Planning Worksheet" plan provided in Appendix A, "Planning Worksheets."

1. In Appendix A, "Planning Worksheets," locate the "NTFS Permission Planning Worksheet."
2. Log on as Administrator.
3. Start Windows NT Explorer, and then expand the LabFiles folder.
4. In the LabFiles folder, right-click a folder or file (from those listed on the "NTFS Permission Planning Worksheet"), and then click **Properties**.

   The *folder_name* **Properties** or *file_name* **Properties** dialog box appears.
5. In the *folder-name* **Properties** or *file_name* **Properties** dialog box, click the **Security** tab, and then click **Permissions**.

   The **File Permissions** or **Directory Permissions** dialog box appears.
6. If you are assigning permissions for a folder, configure the following options. Otherwise, skip this step.

For this option	Do this
Replace permissions on subdirectories	Click to select this check box.
Replace permissions on existing files	Verify that this check box is selected.

7. To add permissions for users or local groups to the folder or file, click **Add**.

   The **Add Users and Groups** dialog box appears.
8. Click **Show Users**.
9. Under **Names**, click a user or local group (from those listed on the "NTFS Permissions Planning Worksheet") and then click **Add**.

   The user or local group appears in the **Add Names** box.
10. In the **Type of Access** box, click the appropriate permissions.

11. Assign the appropriate permissions to the remaining users and groups for all of the folders and files on the "NTFS Permissions Planning Worksheet." (This applies to all but the Public folder; permissions for Public were assigned in a previous procedure.)
12. Quit Windows NT Explorer and log off.

▸ **To test permissions for the Manuals folder when User6 connects over the network**

In this procedure, you connect to your own computer to test permissions for the Manuals folder. Connecting to your own computer mimics connecting over the network.

1. Log on as User6.
2. Click the **Start** button, click **Run**, and then in the **Open** box, type \\*computer_name***Public** (where *computer_name* is the name of your computer), and then click **OK**.

   The Public on *computer_name* window appears.
3. Open the Manuals folder and then attempt to create a file in it.

   Were you successful? Why or why not?

   ____

   ____
4. Quit Windows NT Explorer and log off.

▸ **To test permissions for the Manuals folders when CustomerService6 connects over the network**

In this procedure, you connect to your own computer to test permissions for the Manuals folder. Connecting to your own computer mimics connecting over the network.

1. Log on as CustomerService6.
2. Click the **Start** button, click **Run**, and then in the **Open** box, type \\*computer_name***Public** (where *computer_name* is the name of your computer), and then click **OK**.
3. Start Windows NT Explorer and expand the LabFiles\Public\Manuals folder.
4. Attempt to create a file in the Manuals folder.

   Were you successful? Why or why not?

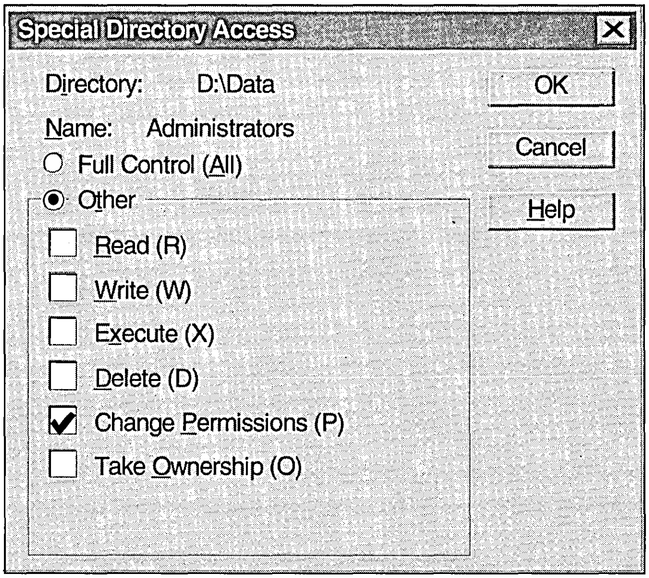
   ____

   ____
5. Quit Windows NT Explorer and log off.

Assigning Special Access Permissions

In most situations, standard permissions are all you need to secure folders and files. However, in a few situations, you will need to assign special access permissions, which give you the ability to assign individual permissions to user and group accounts. For example, you need to assign special access permissions to do the following:

- To allow another user to manage permissions for files that you own, assign that user the permission Change Permissions (P).
- To protect program files from being deleted accidentally or infected by viruses, assign all user accounts, including administrative accounts, the permission Read (R) for executable files.
- To allow administrators to modify executable files, assign the Administrators group the permission Change Permissions (P). This permission gives administrators the ability to change the permissions on Read only files if necessary.



Special Directory Access

Directory: D:\Data

Name: Administrators

○ Full Control (All)

● Other

□ Read (R)

□ Write (W)

□ Execute (X)

□ Delete (D)

☑ Change Permissions (P)

□ Take Ownership (O)

Note The special access permissions are identical for both files and folders.

▸ To assign standard permissions for the Games folder

In this procedure, you assign the standard permission Read to the local Administrators and Users groups.to prepare for the next procedure.

1. Log on as Administrator.
2. Start Windows NT Explorer, and expand the LabFiles\Apps folder.
3. Right-click the Games folder, and then click **Properties**.
4. In the **Games Properties** dialog box, click the **Security** tab, and then click **Permissions**.

   The **Directory Permissions** dialog box appears.
5. Select **Everyone** (if it is not already selected), click **Remove**, and then click **Add**.
6. Make sure your domain name appears in the **List Names From** box.
7. In the **Names** box, click **Administrators**, and then click **Add**.
8. In the **Names** box, click **Users**, and then click **Add**.
9. In the **Type of Access** box, click **Read** and then click **OK**.

   Administrators and Users appear in the Directory Permissions dialog box with Read (RX) (RX) as the permission. This is because the standard permission Read includes the special access permissions Read and Execute.

▸ To assign special access permissions for files

In this procedure, you assign the special access permission Change Permissions to the Administrators group to give its members the ability to change the permissions on the files in the Games folder.

1. In the **Directory Permissions** dialog box, select **Administrators**, and then in the **Type of Access** box, click **Special File Access**.

   The **Special File Access** dialog box appears.

   Notice that the Read and Execute permissions are selected. These are the special file access permissions included with the standard permission Read.
2. Select **Change Permissions (P)**, and then click **OK**.

   Notice that the permissions for Administrators is now indicated by Special Access (RX)(RXP). The first set of parentheses specifies the permissions for the folder and the second set of parentheses specifies the permissions for the files within the folder.
3. Verify that the **Replace Permissions on Existing Files** check box is selected. This applies the selected permission to all the files in the folder.
4. Click **OK** twice to return to Windows NT Explorer.

- **To test special access permissions for files**

1. In Windows NT Explorer, expand the LabFiles\Apps\Games folder.
2. Attempt to run Kolumz.exe.

   Were you successful? Why or why not?

   ____

   ____

3. Attempt to delete Kolumz.exe.

   Were you successful? Why or why not?

   ____

   ____

4. Attempt to assign the Administrators group the Full Control permission for Kolumz.exe.

   Were you successful? Why or why not?

   ____

   ____

Lesson Summary

The following information summarizes the key points in this lesson:

- To assign NTFS permissions, you must be the owner of the folder or file, have the standard permission Full Control, or have the special access permission Change Permissions or Take Ownership.
- When a volume is formatted with NTFS, the permission Full Control is automatically assigned to the Everyone group.
- Special access permissions are used when you need to assign a combination of individual permissions.

For more information on	**See**
Strategies for using NTFS file permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning.*
Setting customized special access permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning.*
Controlling access to files and folders	Chapter 3, "Disk Management Basics," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*

Lesson 5: Taking Ownership of Folders and Files

By default, the user who creates a folder or file is the owner. As owner, a user can assign permissions to control what others can do with the folder or file. In some situations, it may be necessary for an administrator to remove control from a user by taking ownership of the folder or file. This lesson outlines the requirements and procedures to take ownership of a folder or file.

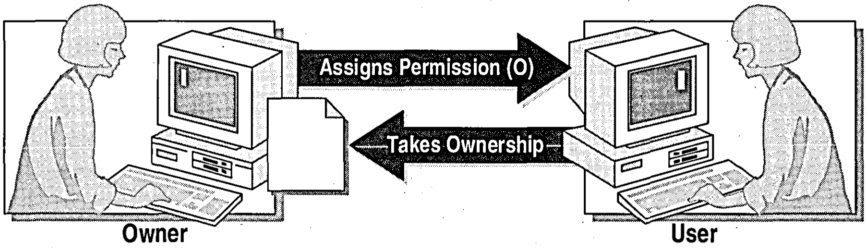
After this lesson, you will be able to:

- Explain the concept of taking ownership of a folder or file.
- Explain how to give users the ability to take ownership of a folder or file.
- Determine the current owner of a folder or file.
- Take ownership of a folder or file.

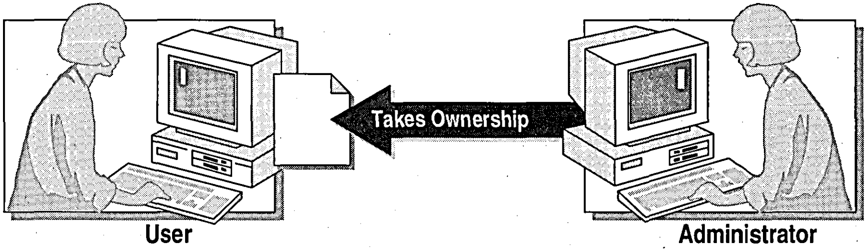
Estimated lesson time: 20 minutes

The user who creates a folder or file is the owner of that folder or file. As the owner of a folder or file, a user can share the folder and assign the Take Ownership permission (O) to other users and groups.

The owner can always control access to the folder or file by changing the permissions set on it. A user cannot share folders or assign permissions for folders that he or she does not own.



If a user has denied others from gaining access to a file and then leaves the company, the administrator can take ownership of the file and change the permissions so that others can gain access to the file.



How to Take Ownership

By default, users who are members of the Administrators group always have the ability to take ownership of a folder or file. If a member of this group takes ownership of a resource, the Administrators group becomes the resource's owner and any member of the Administrators group can gain access to the resource.

The following checklist provides an overview of the tasks that you will need to do if you take ownership of a file:

□ Log on as Administrator.

□ On the **Security** tab of the *folder_name* **Properties** or the *file_name* **Properties** dialog box, click **Ownership** (to determine the current owner).

□ In the **Owner** dialog box, click **Take Ownership**.

Giving Users the Ability to Take Ownership

An owner cannot change the ownership of a resource that they own. The owner can only give another user or group permission to take ownership of a resource. Security of the resource is maintained by preventing users from creating or editing files and then making them look as if they belonged to someone else.

The owner can assign another group or user the *ability* to take ownership of a folder or file by assigning one of the following permissions:

- Standard permission: Full Control
- The special access permission: Take Ownership
- The special access permission: Change Permissions (With this permission, users can assign the Take Ownership permission to themselves or to another user or group.)

▸ **To determine the owner and permissions of a file**

1. Log on as Administrator.
2. Start Windows NT Explorer, and then in the LabFiles folder, create a text file named Owner.txt.
3. Right-click Owner.txt, and then click **Properties**.

   The **Owner.txt Properties** dialog box appears.
4. Click the **Security** tab, and then click **Ownership**.

   Notice that the current owner is the Administrators group.
5. Click **Close**, and then click **Permissions**.

   The **File Permissions** dialog box appears. The Everyone group has the Full Control permission.

▸ To assign the Take Ownership permission to a user

1. In the **File Permissions** dialog box, click **Add.**

   The **Add Users and Groups** dialog box appears.
2. Make sure that your domain name appears in the **List Names From** box.
3. Click **Show Users.**
4. Select SalesMgr6, and then click **Add.**
5. In the **Type of Access** box, click **Read** (if is does not already appear), and then click **OK.**

   SalesMgr6 appears in the **File Permissions** dialog box and has Read permission.
6. Click SalesMgr6, and then in the **Type of Access** box, click **Special Access.**

   The **Special Access** dialog box appears.

   Notice that the special access permissions Read and Execute are selected, because the standard Read permission assigned to the SalesMgr6 for the Owner.txt file includes both Read and Execute.
7. Select the **Take Ownership (O)** check box, click **OK** three times to apply your changes, and then exit to Windows NT Explorer.
8. Quit Windows NT Explorer, and then log off.

▸ To take ownership of a file

1. Log on as SalesMgr6, and start Windows NT Explorer.
2. In the LabFiles folder, right-click Owner.txt, and then click **Properties.**

   The **Owner Properties** dialog box appears.
3. On the **Security** tab, click **Ownership.**

   Notice that the Administrators group is the owner of the file. When any member of the Administrators group creates a file, the entire group becomes the owner of the file.
4. In the **Owner** dialog box, click **Take Ownership.**
5. On the **Security** tab, click **Ownership.**

   Notice that SalesMgr6 is the new owner of the Owner.txt file. By assigning SalesMgr6 the special access permission Take Ownership, SalesMgr6 was able to take ownership away from the Administrators group.
6. Click **Close** to return to the **Security** tab.

▸ To test file permissions as the owner

1. Assign SalesMgr6 the permission Full Control for the Owner.txt file.
2. Remove permissions for all other users and groups from the Owner.txt file.

   Were you successful? Why or why not?

   ____

   ____

3. Close the **Owner Properties** dialog box.
4. Quit Windows NT Explorer, and then Log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- By default, the person who creates a folder or file is the owner.
- By default, members of the Administrators group always have the ability to take ownership of a folder or file.
- The owner can assign another group or user the *ability* to take ownership of a folder or file by assigning the Full Control permission, or by assigning the special access permissions Change Permissions or Take Ownership.

For more information on	See
The procedure to take ownership	Windows NT Help.
Take Ownership permission	Windows NT Help.
Taking ownership of folders and files	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 6: Copying or Moving Folders and Files

Copying and moving folders or files within and between NTFS volumes can affect the original permissions on a folder or file. This lesson explains what happens to permissions when a folder or file is copied or moved.

After this lesson, you will be able to:

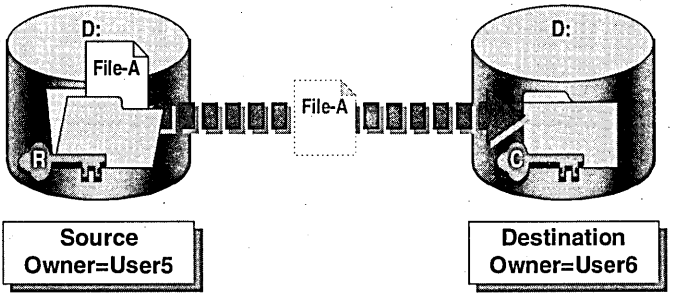
- Describe what happens to permissions on folders and files that are copied or moved within the same or to different volumes.
- Describe what happens to the ownership of folders and files that are copied or moved within the same or to different volumes.
- List the required permissions for copying or moving folders or files.

Estimated lesson time: 20 minutes

Copying a Folder or File

When you copy a folder or file within the same NTFS volume or to a different NTFS volume, the folder or file inherits the permissions of the destination folder, and the user who copies a folder or file becomes the owner.

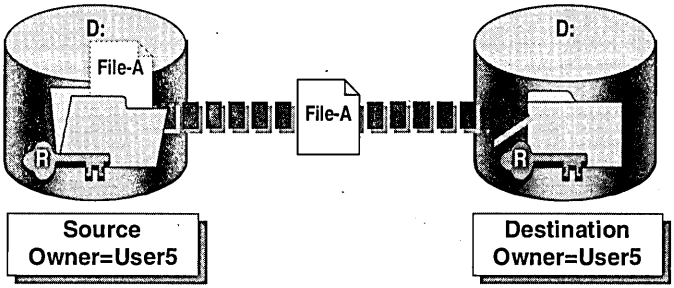
In the following illustration, File-A will inherit the Change permission at the destination folder even though the permission at the source folder is Read. User6 copied the file and will become the new owner of it at the destination folder.



Moving a Folder or File

When you move a folder or file within the same NTFS volume, the folder or file retains its original permissions and owner. However, if you move a folder or file to a different NTFS volume, the folder or file inherits the permissions of the destination folder and the new owner is the user who moved it, just like when a user copies a folder or file.

In the following illustration, File-A will retain the Read permission because it is being moved within the same volume. User6 moved the file, but User5 remains the owner of it at the destination folder.



Permission Requirements

A user cannot copy or move folders or files within or between NTFS volumes, unless the user has the correct permissions.

The following table describes the required permissions to copy or move a folder or file to another folder on an NTFS volume or to another NTFS volume.

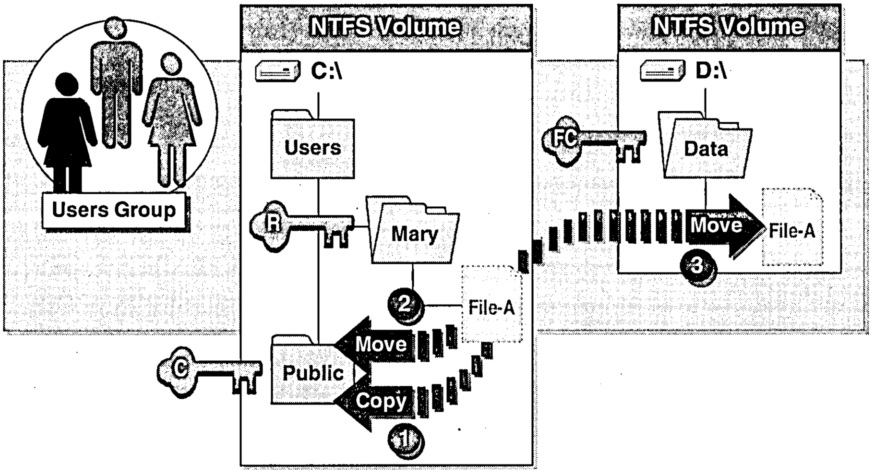
Action	Permission required
Copy	The Add permission for the destination folder.
Move	The Add permission for the destination folder and the Delete permission for the source folder. Delete is required because when a folder or file is moved, it is deleted from the source folder after it is placed in the destination folder.

Important Folders and files that are copied or moved to FAT volumes lose their permissions because FAT volumes do not support NTFS permissions.

Example of Copying and Moving Folders and Files

In the following illustration, File-A is stored in the C:\Users\Mary folder. The Users group has the following NTFS permissions to folders on drives C and D:

- Read permission for C:\Users\Mary and the files contained within it.
- Change permission for C:\Public.
- Full Control permission for D:\Data.



1. What permission does the Users group have to File-A after it is copied to the C:\Public folder?

2. What permission does the Users group have to File-A after it is moved to the C:\Public folder?

3. What permission does the Users group have to File-A if it is moved to the D:\Data folder?

To create a folder while logged on as a user

In this procedure, you create a folder and view its default properties. This folder will be used in subsequent procedures to see how the permissions and ownership are affected when it is moved or copied.

1. Log on as SalesMgr6.
2. In Windows NT Explorer, expand the LabFiles folder.
3. In LabFiles, create a folder named Temp1.
4. Right-click the folder, click **Properties**, and then click **Permissions.**

   What are the permissions assigned to the folder?

5. Click **Cancel.**
6. Click **Ownership.**

   Who is the owner? Why?

7. Click **Close**, and then click **OK.**
8. Log off.

To create a folder while logged on as Administrator

1. Log on as Administrator.
2. Start Windows NT Explorer, and expand the LabFiles folder.
3. In LabFiles, create the following folders:
   - Temp2
   - Temp3
4. View each folder's properties.

   What are the permissions assigned to the folders that you just created?

   Who is the owner of the Temp2 and Temp3 folders?

5. Remove the Everyone group from the permissions list for both folders and then assign the following permissions to the Temp2 and Temp3 folders.

Folder	Assign these permissions
Temp2	Administrators: Full Control
	Users: Read
Temp3	Backup Operators: Read
	Users: Full Control

▸ To copy a folder within the same NTFS volume

1. Copy the Temp2 folder into the Temp1 folder. (Hint: Hold down the CTRL key and use the mouse to drag the Temp2 folder to the Temp1 folder.)
2. Select LabFiles\Temp1\Temp2 and compare the permissions and ownership with LabFiles\Temp2, created by Administrator. Then, compare the permissions of LabFiles\Temp1\Temp2 with LabFiles\Temp1, created by SalesMgr6.

   Who is the owner of LabFiles\Temp1\Temp2 and what are the permissions? Why?

   ____

   ____

3. Log off Windows NT.

▸ To move a folder within the same NTFS volume

1. Log on as the SalesMgr6 and start Windows NT Explorer.
2. Expand the LabFiles folder.
3. Move the LabFiles\Temp3 folder to the LabFiles\Temp1 folder. (Hint: Use the mouse to drag the Temp3 folder to the Temp1 folder.)

   Who is the owner of the LabFiles\Temp1\Temp3 folder and what are the permissions? Why?

   ____

   ____

Lesson Summary

The following information summarizes the key points in this lesson:

- When a folder or file is copied from one folder to another, it inherits the permissions of the destination folder and the user who performed the copy becomes the owner of the folder or file in its new destination.
- When a folder or file is moved within the same volume, the permissions and owner are retained. If a folder or file is moved to a different volume, the same rules apply as when a folder or file is copied.
- To copy a folder or file, a user needs the Add permission for the destination folder. To move a folder or file, a user needs the Add permission for the destination folder and the Delete permission for the source folder.

Lesson 7: Troubleshooting Permission Problems

One of the most common problems that users encounter is the inability to gain access to resources. This lesson describes common permission-related problems and their solutions.

After this lesson, you will be able to:

- Recognize common reasons why users cannot gain access to resources.
- Solve common permission-related problems.

Estimated lesson time: 20 minutes

The following information provides solutions to common permission-related problems.

Problem 1

A user cannot gain access to a resource.

Solution

Check the permissions assigned to the user's account and to groups to which the user is a member. If the No Access permission is assigned to the user or to a group that the user is a member of, then the user does not have permission for the resource.

If a file was copied within an NTFS volume, or copied or moved to another NTFS volume, the file permissions may have changed by inheriting new permissions from the destination folder.

Problem 2

A user deletes a file, even though that user was assigned the No Access permission for the file.

In UNIX file systems, users who have the Write permission to a folder can delete files in the folder. Because Windows NT supports POSIX programs that are designed to run on UNIX file systems, the NTFS Full Control permission allows users to delete files in a folder even if the user has the No Access permission for the file. Therefore, a user with the Full Control permission to a folder can delete a file in the folder, even though the user was assigned the No Access permission to the file.

Solution

Remove the standard NTFS permission Full Control from the user for the folder. Instead, assign the user all of the individual special access permissions for the folder. This gives the user all of the abilities of the Full Control permission for the folder, but prevents the user from deleting files in the folder (for which he or she has been assigned the No Access permission).

Note The scenario described in Problem 2 is the only exception to the rule that file permissions override folder permissions.

Problem 3

You add a user to a group to give that user permission for a resource, but the user still cannot gain access to the resource.

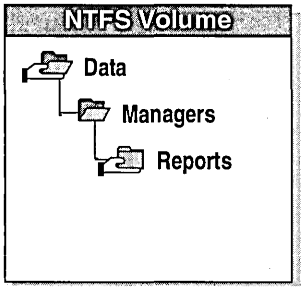
Solution

Have the user log off and then log back on or ask the user to disconnect completely from the remote computer and attempt to connect again. This will update the list of groups that the user is identified as being a member of.

An object called an *access token* is created for a user every time that user logs on and is authenticated by a computer running Windows NT. The access token contains information about the groups to which the user belongs. For the access token to be updated to include the new group to which you have added the user, the user must log off and then log on again, or disconnect completely from the remote computer and then reconnect.

▸ To identify incorrect permissions

Scenario: You are the administrator for a server that contains the following folder hierarchy.



The following share permissions have been assigned to the Data and Reports folders.

Folder	Share name	User or group	Share permissions
Data	Data	Administrators	Full Control
		Managers	Read
Data\Managers\Reports	Mgr_Reports	Administrators	Full Control
		Managers	Full Control

The following NTFS permissions have been assigned.

Folder	User or group	NTFS permissions
Data	Administrators	Full Control
	Managers	Read
Managers	Managers	Add & Read
	Creator Owner	Full Control
Reports	Managers	Add & Read
	Creator Owner	Full Control

User1 calls you, saying that she does not have proper access to the Reports folder. She is a member of the Managers group. When she connects to the shared Data folder, she can browse the Managers and Reports folders. She cannot create new files or modify files that she owns. What is the problem and how would you solve it?

____

____

Deleting a File That Has the No Access Permission

In this exercise, you simulate the scenario described in Problem 2 of this lesson to observe the result when a user has Full Control permission for a folder and No Access permission to a file in that folder. To do this, you first assign these permissions.

▶ To create a folder with the Full Control permission

1. Log on as Administrator, and then start Windows NT Explorer.
2. In LabFiles, create a folder named FullAccess.
3. Verify that the Everyone group has the NTFS permission Full Control for the LabFiles\FullAccess folder.

▶ To create and assign the No Access permission for the NoAccess.txt file

1. In the FullAccess folder, create a text file named NoAccess.txt.
2. Assign the Everyone group No Access permission for the NoAccess.txt file.

   The following error message appears:

   ```
   You have denied access to drive:\LabFiles\FullAccess\NoAccess.txt.
   Nobody will be able to access drive:\LabFiles\FullAccess\NoAccess.txt
   and only the owner will be able to change the permissions. Do you
   wish to continue?
   ```

3. Click **Yes**, and then click **OK** to return to Windows NT Explorer.

▶ To view the result of the Full Control permission for the FullAccess folder

1. In the LabFiles\FullAccess folder, double-click the NoAccess.txt file to open it.

   Were you successful? Why or why not?

2. Click the **Start** button, point to **Programs**, and then click **Command Prompt**.
3. Change to the *drive*:\LabFiles\FullAccess folder.
4. Delete NoAccess.txt by typing the following command:

   delete noaccess.txt

   Were you successful? Why or why not?

   How would you prevent users with Full Control permission for a folder from deleting a file in that folder to which they have been assigned the No Access permission?

▶ To create and assign special directory access permissions to a folder

In this procedure, you assign special access permissions for the FullAccess folder to the Everyone group.

1. Switch to Windows NT Explorer, right-click the FullAccess folder, and then click **Properties**.
2. Click the **Security** tab, and then click **Permissions**.

   Notice that Everyone is selected by default.
3. In the **Type of Access** box, select **Special Directory Access**.

   The **Special Directory Access** dialog box appears.
4. Click **Other**, click to select the check boxes for all individual permissions, and then click **OK**.
5. Click **OK** to return to the **FullAccess Properties** dialog box, and then click **OK** to apply your changes.

   The Everyone group now has permission for the FullAccess folder.

▶ To create a file and assign it the No Access permission

1. In the FullAccess folder, create a text file named NoDelete.txt.
2. Assign the Everyone group the No Access permission for the file NoDelete.txt.

   The following error message appears:

   ```
   You have denied access to drive:\LabFiles\FullAccess\NoDelete.txt.
   Nobody will be able to access drive:\LabFiles\FullAccess\NoDelete.txt
   and only the owner will be able to change the permissions. Do you
   wish to continue?
   ```
3. Click **Yes**, and then click **OK**.

▸ **To view the result of the Full Control permission for the FullAccess folder**

1. Double-click to open LabFiles\FullAccess\NoDelete.txt.

   Were you successful? Why or why not?

   ____

   ____

2. Click the **Start** button, point to **Programs**, and then click **Command Prompt**.
3. Change to the *drive*:\LabFiles\FullAccess folder.
4. Delete NoDelete.txt by typing the following command:

   delete nodelete.txt

   Were you successful? Why or why not?

   ____

   ____

Lesson Summary

The following information summarizes the key points in this lesson:

- If a user has a problem gaining access to a resource, check the permissions on the user account and on any groups to which the user is a member.
- The NTFS folder permission Full Control allows users to delete files in the folder, even if they have the No Access permission for the file. To avoid this, remove the Full Control permission and, instead, assign the user all of the special directory access permissions for the folder.
- If a user cannot gain access to a resource after being added to a group that has permission to the resource, have the user log off and then log back on, or have the user disconnect from the resource and then reconnect.

For more information on	**See**
NTFS permissions	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
FAT and NTFS volumes	Chapter 17, "Disk and File System Basics," in the *Microsoft Windows NT Workstation Resource Kit*.
NTFS file system	Chapter 3, "Disk Management Basics," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit*.
NTFS file system overview	Chapter 17, "Disk and File System Basics," in the *Microsoft Windows NT Workstation Resource Kit*.
Access tokens	Chapter 2, "Network Security and Domain Planning," in the *Networking Guide* of the *Microsoft Windows NT Server Resource Kit*.

Best Practices

The following checklist provides best practices for implementing NTFS permissions. Review this checklist before you begin to assign NTFS permissions:

□ Assign NTFS permissions before sharing a folder. In this way, you avoid the issue of users connecting to and gaining access to folders and files before you fully secure them.

□ Assign permissions to groups rather than to individual users. If the user is a member of a group that has access to certain files, you can end the user's access by removing the user from the group rather than by changing the permissions on each of the files.

□ Assign the Read permission to the Users and Administrators groups for all program executable files.

□ Educate users that share a computer to assign NTFS permissions to the folders and files that they own.

□ Damage to program files is usually a result of accidents and viruses. To prevent this type of file damage, assign the Read permission to all user accounts, including Administrator, for program files. By doing so, you prevent users and viruses from modifying or deleting these files. In addition, assign the Administrators group the special access permission Change Permissions (P) so that members can assign themselves less restrictive permissions when changes to the program files are required.

□ Use the %Username% variable to create home folders—this simplifies administration by automatically assigning each user the NTFS permission Full Control for his or her home folder.

□ Assign the Creator Owner group the Full Control permission for Data folders. This gives users the Full Control permission for only the folders or files that they create in the Data folder.

□ Use long, descriptive names if the resource will only be accessed locally. If a folder will eventually be shared, then use folder and file names that are accessible by all client computers.

Note If you want to remove the accounts that were created by running the Chapter6.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter6.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. Which of the following statements are true about NTFS permissions? (Circle all that apply.)
    a. They are available only on NTFS volumes.
    b. They protect resources from users who sit at the computer where the resource is located.
    c. They protect resources from users who connect to them over the network.
    d. They can be assigned to folders and files.
    e. A user's effective permissions are the combination of the user and group permissions.
    f. All of the above.
2. Complete this sentence. When share permissions are combined with NTFS permissions the ______________________________ permission becomes the effective permission.
3. How would you create a home folder to which the respective user is automatically assigned the NTFS permission Full Control?

    ____

    ____

4. Which of the following are requirements for assigning NTFS permissions? (Circle all that apply.)
    a. Must be owner of the folder or file.
    b. Must have the standard permission Full Control, or either the Change Permissions or the Take Ownership special access permission.
    c. Must have the standard permission Change.
5. What is the default permission once a volume is formatted with NTFS?

    ____

    ____

6. Which of the following statements are true? (Circle all that apply.)
   a. Whenever a folder or file is copied, the folder or file inherits the permissions of the destination folder and the user who performed the copy becomes the owner of the copied folder or file.
   b. Whenever a folder or file is copied, the folder or file inherits the permissions of the destination folder and the ownership is retained.
   c. Whenever a folder or file is moved within the same volume, the folder or file retains its permissions and owner.
   d. Whenever a folder or file is moved to a different volume, the folder or file inherits the permissions of the destination folder and the user who performed the move becomes the owner of the moved folder or file.
   e. All of the above.

7. What should you always check when a user cannot access a resource?

____

____

Answer Key

Procedure Answers

Page 219

▶ **To review the video**

1. What do shared folders provide access to?

   Network resources.

2. What can share permissions be assigned to?

   Folders only.

3. What can NTFS permissions be assigned to?

   To folders and to individual files.

4. When you combine a share permission with an NTFS permission what permission becomes the *effective* permission?

   The most restrictive permission becomes the effective permission.

Example of Combined NTFS Permissions and Share Permissions

Page 220

- In Example A, what is User1's effective permission when he or she accesses the User1 folder by connecting to the Users shared folder? What is User2's effective permission for the User1 folder?

  User1 has Full Control permission to the Users folder and to the User1 folder.

  User2 does not have permission to gain access to the User1 folder, because the NTFS permission Full Control has been assigned to only the individual user for his or her home folder; therefore, only the individual user has Full Control permission to his or her home folder.

Page 221

- In Example B, what are the Sales group's effective permissions when they access the Sales folder by connecting to the Data shared folder?

  Read, because when share permissions are combined with NTFS permissions, the most restrictive permission applies.

Page 225

▸ **To plan NTFS folder and file permissions**

Strategy used in sample planning worksheet (see Appendix A, "Planning Worksheets):

Create a local group for each resource that will be restricted to certain users—for example, Spreadsheet, Database, and Library.

Use the built-in local Users group whenever all users require access to a resource. In a domain, the Users group contains all domain user accounts. In a workgroup, the Users group contains all user accounts local to the computer where the folder is located.

Assign the built-in Administrators group the Full Control permission for any folders that its members will manage.

Assign the Change permission to all local group members that need the ability to add, delete, and make changes to folders or files, but do not need to assign permissions to other users and groups.

Assign the Read permission to all local group members that only need to run programs or read files.

Assign the built-in Creator Owner system group the Full Control permission. This will give users with the Add & Read permission who copy or create a file the ability to modify the files they add to the Public folder. As a result, when a user copies or creates a file in the Public folder, the new file will have the following permission.

User or group	**Permission**
Users	Read
User account that copied or created the file	Full Control

Page 233

▸ **To test the NTFS permissions assigned for the Public folder**

3. Were you successful? Why or why not?

   Yes, because the Users group has been assigned the NTFS permission Add & Read for the LabFiles\Public folder.

4. Attempt to perform the following tasks for the file that you just created. In the following list, mark those which you are able to complete:

   CustomerService6 was successful at all three tasks because when CustomerService6 created the file, the account was added to the Creator Owner group, which has the NTFS permission Full Control for the LabFiles\Public folder.

5. Attempt to perform the following tasks for the Chapter6.txt file created by Administrator. In the following list, mark the task or tasks that you are able to complete:

   CustomerService6 can only open the file because the account is a member of the Users group, which has the NTFS permission Add & Read for the LabFiles\Public folder, and because the file was created by another user.

Page 235

▸ **To test permissions for the Manuals folder when User6 connects over the network**

3. Were you successful? Why or why not?

   Yes, because the Everyone group has the share permission Full Control for the Public folder and User6 has the NTFS permission Full Control for the Manuals folder. If the Everyone group had the share permission Read, User6 would not have been able to create a file in the Manuals folder, because the share permission Read would be the effective permission.

Page 235

▸ **To test permissions for the Manuals folders when CustomerService6 connects over the network**

4. Were you successful? Why or why not?

   No, because CustomerService6, as a member of the Users group, only has the NTFS permission Read for the Manuals folder. CustomerService6 does have the ability to create a file in the Public folder because the share permission on Public is Full Control.

Page 238

▸ **To test special access permissions for files**

2. Attempt to run Kolumz.exe.

   Were you successful? Why or why not?

   Yes, because Users and Administrators have Read access to the Games folder and the files it contains.

3. Attempt to delete Kolumz.exe.

   Were you successful? Why or why not?

   No, because Users and Administrators only have Read access to the Games folder and the files that it contains.

4. Attempt to assign the Administrators group the Full Control permission for Kolumz.exe.

   Were you successful? Why or why not?

   Yes, because Administrators have the special access permission Change Permissions (P) for Kolumz.exe.

Page 243

▸ **To test file permissions as the owner**

2. Remove permissions for all other users and groups from the Owner.txt file.

   Were you successful? Why or why not?

   Yes, because SalesMgr6 is the owner of Owner.txt, and the owner of a folder or file always has the ability to change the permissions on folders and files that he or she owns.

Page 247

Example of Copying and Moving Folders and Files

1. What permission does the Users group have to File-A after it is copied to the C:\Public folder?

   The Users group has Change permission to File-A, because File-A inherits the Change permission after it is copied.

2. What permission does the Users group have to File-A after it is moved to the C:\Public folder?

   The Users group has Read permission, because permissions are retained for files that are moved between folders on the same NTFS volume.

3. What permission does the Users group have to File-A if it is moved to the D:\Data folder?

   The Users group has Full Control permission to File-A once it is moved to D:\Data, because moving a file to a different NTFS volume is treated as a copy; the file permissions are inherited from the destination folder.

Page 248

▸ **To create a folder while logged on as a user**

4. What are the permissions assigned to the folder?

   The Everyone group has Full Control (by default).

6. Who is the owner? Why?

   SalesMgr6, because the user who creates a folder or file is the owner.

Page 248

▸ **To create a folder while logged on as Administrator**

4. What are the permissions assigned to the folders that you just created?

   The Everyone group is assigned the Full Control permission by default.

   Who is the owner of the Temp2 and Temp3 folders?

   The Administrators group is the owner because a member of the group created the folders.

Page 249

▶ To copy a folder within an NTFS volume

2. Who is the owner of LabFiles\Temp1\Temp2 and what are the permissions? Why?

   The Administrators group became the owner of the folder when it was copied to its new location even though SalesMgr6 was the owner of Temp1, because whoever copies a folder or file becomes the owner. However, the folder inherited the permissions set by SalesMgr6 (Everyone: Full Control) because when a folder or file is copied within a volume, it always inherits the permissions of the destination folder.

Page 249

▶ To move a folder within the same NTFS volume

3. Who is the owner of the LabFiles\Temp1\Temp3 folder and what are the permissions? Why?

   The Administrators group retained ownership of the folder because when a folder or file is moved within the same volume, the ownership stays the same.

   The permissions were also retained (Backup Operators: Read; Users: Full Control) because when a folder or file is moved within the same volume the permissions also stay the same.

Page 252–253

▶ To identify incorrect permissions

User1 calls you, saying that she does not have proper access to the Reports folder. She is a member of the Managers group. When she connects to the shared Data folder, she can browse the Managers and Reports folders. She cannot create or modify any files that she owns. What is the problem and how would you solve it?

The problem is that User1 is connecting to the shared Data folder. She only has Read permission to this folder. To solve this problem, User1 needs to connect to the shared folder Mgr_Reports. Because she is a member of the Managers group, she has Full Control permission to access the Mgr_Reports shared folder.

Page 254

▸ **To view the result of the Full Control permission for the FullAccess folder**

1. Were you successful? Why or why not?

   No, because the Everyone group has the No Access permission for FullAccess\NoAccess.txt. The Administrator is a member of the Everyone group.

4. Were you successful? Why or why not?

   Yes, because the NTFS folder permission Full Control includes a hidden permission for POSIX compliance that allows users to delete files in the root of a folder to which the user has been assigned the Full Control permission. This hidden permission overrides No Access.

   How would you prevent users with Full Control permission to a folder from deleting a file in that folder to which they have been assigned the No Access permission?

   Assign users all of the individual special directory access permissions. These permissions provide the same level of access as the Full Control permission, but they do not allow the user to delete a file with the No Access permission.

Page 256

▸ **To view the result of the Full Control permission for the FullAccess folder**

1. Were you successful? Why or why not?

   No. Everyone has had all permissions removed for LabFiles\FullAccess\NoDelete.txt. The Administrator is a member of the Everyone group.

4. Were you successful? Why or why not?

   No, because the hidden permission for POSIX compliance that allows users to delete files in the root of a folder is only included with the standard permission Full Control.

Page 259

Review Answers

1. Which of the following statements are true about NTFS permissions? (Circle all that apply.)

   Answer f is correct.

2. Complete this sentence. When share permissions are combined with NTFS permissions the ____ permission becomes the effective permission.

   "Most restrictive" is the correct answer.

3. How would you create a home folder to which the respective user is automatically assigned the NTFS permission Full Control?

   Use %Username% to assign the user's account name to the home folder and to automatically assign the NTFS permission Full Control for the respective user's home folder.

4. Which of the following are requirements for assigning NTFS permissions? (Circle all that apply.)

   Answers a and b are correct.

5. What is the default permission once a volume is formatted with NTFS?

   The Everyone group is assigned Full Control permission.

6. Which of the following statements are true? (Circle all that apply.)

   Answers a, c, and d are correct.

7. What should you always check when a user cannot access a resource?

   You should always check the permissions for the resource to ensure that the user has the proper permissions or that the user is a member of a group with the proper permissions.

CHAPTER 7

Setting Up a Network Print Server

About This Chapter

This chapter introduces you to Microsoft Windows NT printing. It explains procedures and guidelines for setting up and configuring a network print server. The hands-on procedures give you an opportunity to implement and practice these tasks.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- Knowledge about user accounts.
- Knowledge about the Administrators, Print Operators, Server Operators, and Power Users groups.
- The Microsoft Windows NT Server compact disc.
- Two user accounts created named User7-A and User7-B. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter7.cmd to create these accounts.

Lesson 1: Introduction to Windows NT Printing

Windows NT offers several advanced printing features. For example, as an administrator, you can remotely administer Windows NT print servers. Another advanced feature is the fact that you do not have to install a printer driver on a Windows NT client computer to enable it to use a Windows NT print server.

This lesson introduces Windows NT printing by defining key concepts and terms, and describes the requirements to set up printing.

After this lesson, you will be able to:

- Define Windows NT printing terms.
- Describe the requirements for setting up Windows NT printing.

Estimated lesson time: 10 minutes

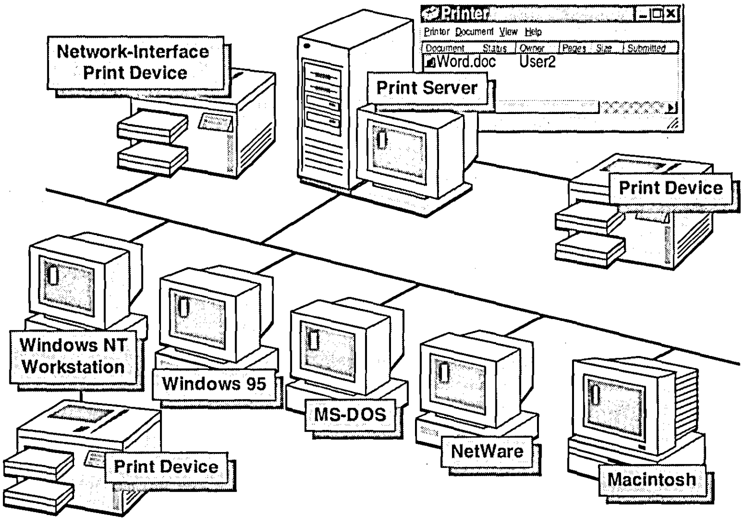
Windows NT Printing Terms

In Windows NT, a *print device* refers to the actual hardware device that produces printed documents.

A *printer* is a software interface between the operating system and the print device. The printer defines where the document will go before it reaches the print device (to a local port, to a file, or to a remote print share), when it will go, and various other aspects of the printing process.

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

A *print server* is the computer that runs the printer software, and that receives and processes documents from clients.



Document	Status	Owner	Pages	Size	Submitted
Word.doc		User2			

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

The *print spooler* is a collection of dynamic-link libraries (DLLs) that receive, process, schedule, and distribute documents. *Spooling* is the process of writing the contents of a print job to a file on disk. This file is called a spool file.

Requirements

Setting up printing on a Windows NT network requires:

- At least one computer configured as a *print server,* and running Windows NT Server or Windows NT Workstation.

  Both Windows NT Workstation and Windows NT Server can operate in either client or print server roles. However, Windows NT Workstation is limited to 10 concurrent connections from other computers and does not support Macintosh and NetWare clients.
- 16 megabytes (MB) of RAM for *x*86-based print servers controlling a small number of print devices. Managing a large number of printers or managing many large documents requires more memory.
- Sufficient disk space, especially in cases where documents are large or many of them are likely to accumulate. For example, if 10 users print large documents at the same time, the print server must have enough disk space to spool all of the documents.
- A dedicated print server, if the server is to manage many heavily used printers. When you use Windows NT for both file and print sharing, file operations have first priority. Printing transactions never slow access to files. Moreover, file operations have negligible impact on print devices attached directly to the server; parallel and serial ports are always the primary bottleneck.
- Client computers running any of the following network operating systems:
  - Windows NT
  - Windows 95
  - Windows for Workgroups
  - LAN Manager 2.*x*
  - OS/2
  - UNIX
  - NetWare*
  - Macintosh*

Note *NetWare and Macintosh clients can only access network printers on print servers running Windows NT Server. Windows NT Workstation does not support these clients.

Lesson Summary

The following information summarizes the key points in this lesson:

- In Windows NT, a *print device* refers to the actual hardware device that produces printed documents; a *printer* is a software interface between the operating system and the print device.
- Setting up printing on a Windows NT network requires one computer configured as a *print server*, running Windows NT Server or Windows NT Workstation.

Lesson 2: Setting Up a Network Print Server and Client

This lesson guides you through the steps needed to set up a network print server and client. Setting up a network print server allows multiple clients to centralize printing by using a single, high-quality print device.

After this lesson, you will be able to:

- Add and share a printer.
- Set up clients for printing.
- Access a network printer.
- Assign printer permissions to users and groups.

Estimated lesson time: 30 minutes

When setting up a network print server, you need to complete the following four key tasks:

❑ Check to see if the print device is on the Windows NT 4.0 hardware compatibility list (HCL). The HCL is included with Windows NT Workstation and Windows NT Server.

- If your print device is on the list, then the required printer driver is included with Windows NT.
- If the print device is not on the list, you will need to get a printer driver from the manufacturer of the print device, or you may be able to use a driver for a supported print device that your print device can emulate.

❑ Log on as a user who has the Full Control print permission.

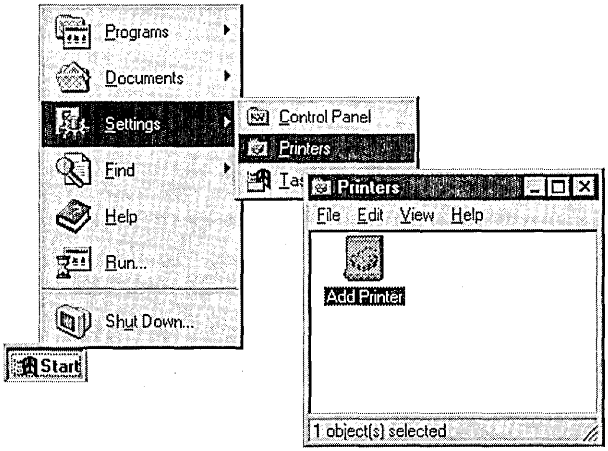
The following table lists the built-in groups with the Full Control print permissions and their printer administration capabilities.

A member of this group	Can administer a printer
Administrators	On any computer in the domain running Windows NT Workstation or Windows NT Server.
Print Operators	On any domain controller.
Server Operators	On any domain controller.
Power Users	On any local computer in the domain in which the group exists.

- □ Add a printer—this installs the *printer driver* for the print device on the print server. The printer driver is a program that converts graphics commands into a specific printer language, such as PostScript or PCL. Windows NT supplies drivers for most of the available print devices.
- □ Share a printer—this allows users to connect to the printer over the network, and print to the print device. You can share a printer when you add it for the first time, or you can share a printer that was previously added but not shared.

Adding and Sharing a New Printer

If the print device is on the HCL, and you are logged on as a member of the appropriate group, you can add and share a printer. Users can then connect to it over the network.



You add and share a new printer using the Add Printer Wizard. The wizard guides you through the steps needed to add a printer. The following table describes the options to add and share a new printer.

Option	Use this option to
My Computer	Designate the computer as the print server for the print device.
Available ports	Specify which port on the print server is attached to the print device.
Manufacturers and **Printers**	Install the correct printer driver on the print server. If the driver that you want is not listed, click **Other**, and then provide a driver.
Printer name	Identify the printer to the users. Type a name that is intuitive and descriptive of the print device.

(continued)

Option	Use this option to
Default printer	Set the default printer for all Windows-based programs on the local computer. When you add the first printer on the print server, it is automatically set as the default, and therefore, this option does not appear in the wizard until you add another printer.
Shared	Make it possible for users with the appropriate permission to connect to the printer over the network.
Share Name	Assign a share name. Select a name that tells users the type of print device or its location. Try to make this name compatible with all client computers on the network. The default share name is the printer name truncated to 8.3 characters. If you use a share name longer than an 8.3 name, not all clients will be able to connect to it.
Operating systems	Identify the types of clients, such as Windows NT and Windows 95, that will use the printer. This ensures that the appropriate printer drivers are installed on the print server.
Would you like to print a test page?	Print a test page to verify that the printer is installed correctly.

▸ To add and share a printer

In this procedure, you add a new printer for an HP LaserJet 4Si print device and then share it so that network clients can access it. You do not need the actual print device to do this procedure; however, if you have a printing device connected to your computer, you can substitute your print device information for the HP LaserJet 4Si.

1. Log on as Administrator.
2. Click the **Start** button, point to **Settings**, and then click **Printers**.

   The Printers window appears.
3. Double-click the Add Printer icon.

   The Add Printer Wizard starts. Notice that My Computer is selected by default. This option must be selected to set up a print server.
4. Click **Next** to add a printer on this computer.
5. Under **Available ports**, select the **LPT1** check box, and then click **Next.**
6. Under **Manufacturers**, click **HP**.

7. Under **Printers**, click **HP LaserJet 4Si**, and then click **Next**.

Note If a printer driver for the selected print device is already installed on your computer, the Add Printer Wizard will prompt you to either keep or replace the existing driver. Replacing the existing driver is useful if you want to update it with a later version.

In the **Printer name** box, notice that the name defaults to the selected print device. This name will appear at the top of the printer window that you will use for administering the printer. If you had multiple print devices of the same type, you would assign a printer name that easily distinguishes one printer from another. Also, if you have previously added a printer, notice that the wizard asks you if you want this new printer to be the default printer.

8. To accept the default settings, click **Next**.
9. Click **Shared**.
10. In the **Share Name** box, type **hplaser4**

    Notice the box with a list of operating systems. If you want clients to be able to automatically copy the correct printer driver when they access this printer, you must select all of the operating systems that will be printing to this computer.

    For example, select Windows 95 so that the 16-bit driver is installed on the print server. When a Windows 95 client connects to the printer, the driver is copied to the client automatically. This means that you will not need to install the driver manually on the client.

11. Click **Windows 95**, and then click **Next**.
12. When asked if you want to print a test page, click **No**, and then click **Finish**.

    If the printer driver is not already on the print server, you are prompted for the path to the files. You will find these files on both the Windows NT Server and the Windows NT Workstation compact discs.

13. If prompted for the path to the files, insert the Windows NT Server compact disc into the CD-ROM drive, and then in the **Copy files from** box, type *cd_drive***i386** (or Alpha, MIPS, or PPC if you are running Windows NT on a different platform than i386), and click **OK**.

    The printer files are copied.

    The shared printer is created, and an icon for the HP LaserJet 4Si printer appears. Notice that an open hand appears under the printer icon. This indicates that the printer is shared.

▸ To add a second printer

In this procedure, you add a second printer, but you do not share it.

1. In the Printers window, double-click the Add Printer icon.

   The Add Printer Wizard starts.
2. Click **My Computer**, and then click **Next**.
3. Under **Available ports**, select the **LPT3** check box, and then click **Next**.
4. Under **Manufacturers**, click **Canon**.
5. Under **Printers**, click **Canon Bubble-Jet BJC-600e**, and then click **Next**.

   In the **Printer name** box, notice that Windows NT automatically defaults to the printer name Canon Bubble-Jet BJC-600e.
6. Click **Next** to accept the default printer name and to avoid making this the default printer.
7. Verify that **Not Shared** is selected, and then click **Next** again.
8. When asked if you want to print a test page, click **No**, and then click **Finish**.

   If the printer driver is not already on the print server, you are prompted for the path to the files. You will find these files on the Windows NT Server and the Windows NT Workstation compact discs.
9. If prompted, in the **Copy files from** box, type the path to the files, and then click **OK**.

   An icon for the Canon Bubble-Jet BJC-600e printer appears. Notice that there is no hand under the icon, which indicates that it is not shared.

▸ To set an existing printer as the default printer

In this procedure, you set the HP LaserJet 4Si as the default printer. When a user prints a document from a program, the document will automatically be sent to this printer.

1. In the Printers window, select the HP LaserJet 4Si icon.
2. On the **File** menu, click **Set As Default**.

▸ To pause the HP LaserJet 4Si printer

In this procedure, you pause the printer to prevent it from trying to communicate with a non-existent print device. Doing this will eliminate error messages in later procedures when documents are sent to the printer.

1. In the Printers window, double-click the HP LaserJet 4Si icon.

   The HP LaserJet 4Si window appears.
2. On the **Printer** menu, click **Pause Printing**.

- **To print a test document to the HP LaserJet 4Si printer**

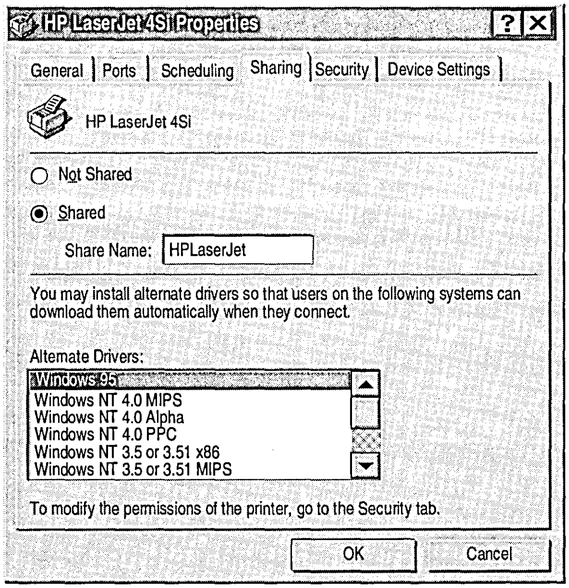
1. Click the **Start** button, point to **Programs**, point to **Accessories**, and then click **Notepad**.
2. In Notepad, type some text.
3. Arrange the Notepad window and the HP LaserJet 4Si window so that you can see the contents of each.
4. On the **File** menu, click **Print**.

   You receive a message stating that the document is printing.

   The document appears in the HP LaserJet 4Si window while it is waiting to be printed.
5. Close Notepad without saving the file.

Sharing an Existing Printer

If your computer has an existing, non-shared printer, all you have to do to share it is assign it a share name and specify the client platforms that will use the printer.



○ Not Shared

● Shared

Share Name: HPLaserJet

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

Alternate Drivers:

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

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

▸ **To share an existing printer**

1. In the Printers window, select the Canon Bubble-Jet BJC-600e icon.
2. On the **File** menu, click **Sharing**.

   The **Canon Bubble-Jet BJC-600e Properties** dialog box appears.
3. Click **Shared**, and then in the **Share Name** box, type **BubbleJet**
4. Click **OK**.

   An open hand appears under the printer icon in the Printers window. This indicates that the printer is shared.

▸ **To delete a printer**

1. In the Printers window, select the Canon Bubble-Jet BJC-600e icon.
2. On the **File** menu, click **Delete**.

   You receive a message asking you to confirm that you want to delete the printer.
3. Click **Yes**.

   The printer disappears from the Printers folder.

Setting Up a Network Client

You need to make sure that users can print after you add and share a printer. The tasks that you need to perform to ensure that users can print depend on which client computers are in your network.

Windows NT and Windows 95 clients

Once you have a shared printer, and you have specified that Windows NT and Windows 95 clients will be using the printer, you do not need to do anything further. The user only needs to connect to the shared printer; the correct printer driver is automatically copied to the client.

Other Microsoft Clients

For the following clients to print to a Windows NT shared printer, you must install the appropriate printer driver locally on the client computer.

- LAN Manager 2.*x*
- Windows for Workgroups
- Windows 3.1, MS-DOS, and OS/2 (each with LAN Manager Client version 2.2c installed)

Non-Microsoft-based Clients

For non-Microsoft-based clients, you must install the appropriate printer driver locally on the client computer. Also, the print server must have the appropriate service installed.

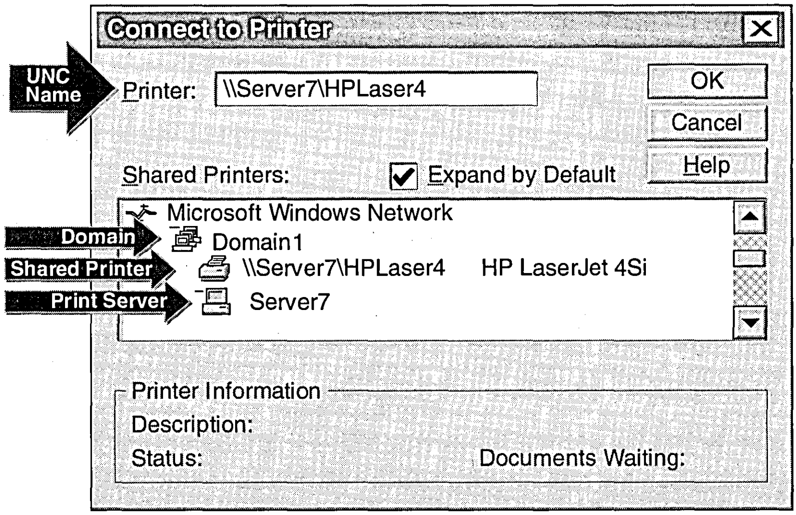
The following table lists the non-Microsoft-based clients and their required services.

Client computer	Service
Macintosh	Services for Macintosh
NetWare	File and Print Services for NetWare (FPNW)
UNIX	TCP/IP Printer Service

Note For more information about setting up non-Microsoft-based clients, see Microsoft Windows NT Server *Concepts and Planning*.

Accessing a Network Printer

When users connect to printers, they are connecting to logical printer names that represent one or more print devices. Clients use different interfaces depending on which operating systems are used. The following illustration shows the interface for Windows NT and Windows 95 clients.


Connect to Printer

Printer: \\Server7\HPLaser4

Shared Printers: ☑ Expand by Default

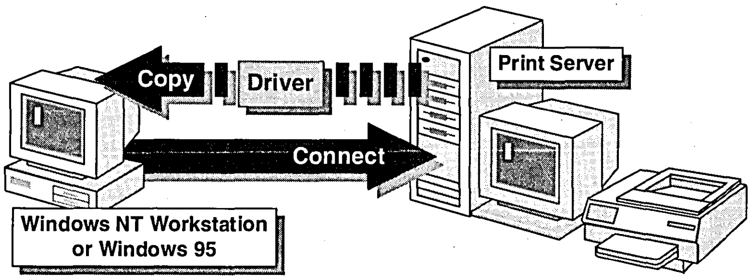
Microsoft Windows Network
Domain1
\\Server7\HPLaser4 HP LaserJet 4Si
Server7

Printer Information
Description:
Status: Documents Waiting:

The default print permission for all users is Print, which makes it possible for them to access any network printer.

Connecting from Clients Running Windows NT 4.0 and Windows 95

Clients running Windows NT 4.0 and Windows 95 use the Add Printer Wizard to connect to a shared printer. When they first connect, the appropriate printer driver is automatically installed into client memory.



Thereafter, Windows NT–based clients and Windows 95–based clients do the following:

- A Windows NT–based client checks the printer driver each time it reconnects. If the driver is not current, a copy of the new driver is downloaded automatically.
- The printer driver for a Windows 95–based client is not automatically kept current. If you update the driver on the print server, you must manually install the driver on the Windows 95–based client.

Note Windows version 3.1 and Windows for Workgroups clients use Print Manager to connect to a printer.

▶ **To connect to a printer**

If you have two computers, do this procedure from the secondary computer.

1. In the Printers window, double-click the Add Printer icon.

   The Add Printer Wizard starts.

2. Click **Network printer server**, and then click **Next**.

   The **Connect to Printer** dialog box appears.

3. In the **Printer** box, type \\*print_server***hplaser4** and then click **OK**.

   –or–

   In the **Shared Printers** box, double-click \\print_server\hplaser4.

   Note If the **Expand by Default** check box is not selected, you will need to double-click your domain name to display your print server.

   The Add Printer Wizard prompts you to use the printer as the default printer. **No** is selected by default.

4. Click **Next**.

   A message indicates that the network printer has been successfully installed. This means that the printer driver was copied to the client computer. An icon for the connected printer appears in the Printers window.

5. Click **Finish**.

Connecting from Other Clients

To connect to a printer from clients running operating systems other than Windows NT and Windows 95, use the commands specific to the clients.

- For LAN Manager clients, (either MS-DOS-based or OS/2-based), use the **net use** command. For example, type:

  net use lpt*x* \*server_name**share_name*

- For NetWare clients configured with a Monolithic IPX and NetWare VLM, use the NetWare **capture** command. For example, type:

  capture *queue_name*

- For UNIX clients running TCP/IP, use the LPR utility. For example, type:

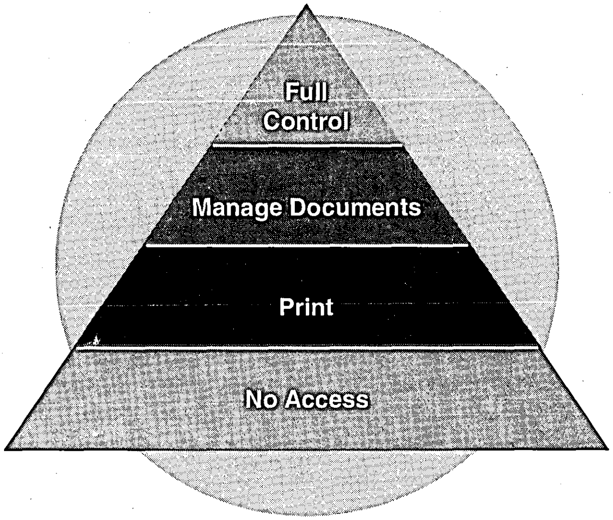
  lpr -S*server_name* **-P***share_name file_name*

- For the Apple Macintosh, use Chooser.

Assigning Printer Permissions

Once you have added and shared a printer, you need to verify that users have the appropriate permissions to print.

Printer permissions control not only who can print, but also which printing tasks a user can do. For security reasons, you may need to limit user access to certain printers. In large organizations, you may need to delegate printer administration.



There are four levels of printer permissions: No Access, Print, Manage Documents, and Full Control. By default, all users have the Print permission as members of the Everyone group.

The following table lists the capabilities of the four levels of permissions.

Capabilities	No Access	Print (default)	Manage Documents	Full Control
Print documents		X	X	X
Pause, resume, restart, and cancel the user's own document		X	X	X
Connect to a printer		X	X	X
Control job settings for all documents			X	X

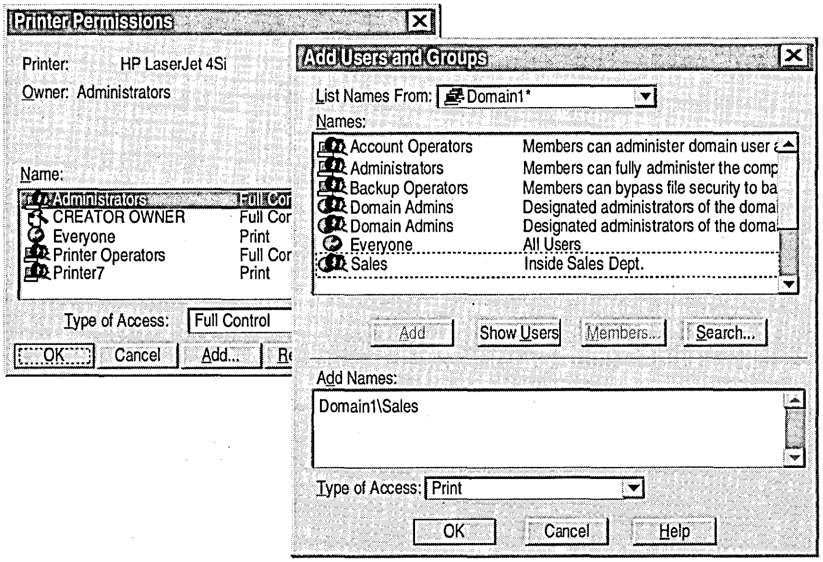
(continued)

Capabilities	No Access	Print (default)	Manage Documents	Full Control
Pause, restart, and delete all documents			X	X
Share a printer				X
Change printer properties				X
Delete printers				X
Change printer permissions				X

Guidelines for Assigning Permissions

Most users will only require the default Print permission. Use the following guidelines to assign other permissions:

- Remove the default Print permission from the Everyone group.
- Create a global group (or groups for larger organizations) to organize users with similar printing needs. Create a local group on the print server, add the global group to the local group, and then assign the local group the appropriate print permissions.
- Use the existing built-in Print Operators group for printer administration. Members of this group have the ability to create, delete, and manage printer shares (that is, they have the Manage Documents permission).



Printer Permissions

Printer: HP LaserJet 4Si
Owner: Administrators

Name:

Administrators	Full Cor
CREATOR OWNER	Full Cor
Everyone	Print
Printer Operators	Full Cor
Printer7	Print

Type of Access: Full Control

Add Users and Groups

List Names From: Domain1*

Names:

Account Operators	Members can administer domain user
Administrators	Members can fully administer the comp
Backup Operators	Members can bypass file security to ba
Domain Admins	Designated administrators of the domai
Domain Admins	Designated administrators of the doma
Everyone	All Users
Sales	Inside Sales Dept.

Add Names:
Domain1\Sales

Type of Access: Print

▸ To assign permissions to a group

In this procedure, you assign the Print permission to the local groups Users, and then you remove the Print permission from the built-in group Everyone.

1. In the Printers window, select the HP LaserJet 4Si icon, and then, on the **File** menu, click **Properties**.

   The **HP LaserJet 4Si Properties** dialog box appears.

2. Click the **Security** tab, and then click **Permissions**.

   The **Printer Permissions** dialog box appears.

   Under **Name**, which built-in local groups are assigned the Full Control permission by default?

   ____

   Under **Name**, which system groups are assigned the Manage Documents permission by default?

   ____

3. Select the Everyone group, and then click **Remove**.

   The Everyone group no longer appears under **Name**.

4. Click **Add**.

   The **Add Users and Groups** dialog box appears.

5. Click **Users**, and then click **Add**.

   The Users group appears in the **Add Names** box.

6. In the **Type of Access** box, verify that **Print** is selected, and then click **OK** to return to the **Printer Permissions** dialog box.

   Notice that the User group appears with the Print permission.

7. Click **OK** to return to the **HP LaserJet 4Si Properties** dialog box.

▸ To assign permissions to a user

In this procedure, you assign the User7-A and User7-B user accounts different print permissions. These user accounts were created in "Before You Begin" by running the Chapter7.cmd batch file located in the LabFiles folder. To distinguish these user accounts from user accounts you may have created in other chapters, the number 7 has been appended to each user name.

- Use the same steps that you used in the previous procedure to assign the following permissions for the HP LaserJet 4Si printer to each user:
  - User7-A: Manage Documents
  - User7-B: Full Control

Note In the **Add Users and Groups** dialog box, you may need to click **Show Users** to display the user names.

▸ To test the Manage Documents permission for User7-A

In this procedure, you test the permission assigned to User7-A to see the options that are available.

1. Log on as User7-A.
2. Make sure that the HP LaserJet 4Si printer is paused and that there is a document waiting to be printed.
3. In the Printers window, double-click the Add Printer icon.

   What options are available to User7-A in the first **Add Printer Wizard** dialog box?

   ____

4. Close the Add Printer Wizard by clicking **Cancel**.
5. In the Printers window, select the HP LaserJet 4Si icon, and then on the **File** menu, click **Properties**.
6. Click the **Security** tab, and then click **Permissions**.

   Can you change permissions?

   ____

7. Click the **Sharing** tab.

   Are the options to share a printer available?

   ____

8. Click the **Scheduling** tab.

   Are the options to change printing hours available?

   ____

9. Click the **Ports** tab.

   Can you add a port?

   ____

10. Close the **HP LaserJet 4Si Properties** dialog box.
11. In the Printers window, with the HP LaserJet 4Si icon selected, click **File** to view the available menu options, and then click **Purge Print Documents.**

    Can you purge documents from the printer?

    ____

▸ To test the Full Control permission for User7-B

In this procedure, you test the permission assigned to User7-B to see the options that are available.

1. Log on as User7-B.
2. Try to perform the following tasks. In the following list, mark the tasks that are available with the Full Control permission:

   □ Add a printer

   □ Change a permission

   □ Share a printer

   □ Schedule a printer

   □ Add additional ports

   □ Purge a printer
3. Log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- Windows NT includes printer drivers for all print devices on the Windows NT 4.0 hardware compatibility list (HCL).
- Setting up a network print server requires that you are a member of the built-in Administrators, Print Operators, Server Operators, or Power Users group.
- When you add a printer, specify all of the Windows NT and Windows 95 client operating systems (under **Alternate Drivers** on the **Sharing** tab) that will be connecting to the print server. Windows NT will then install the appropriate printer drivers on the print server for clients to download.
- If the appropriate printer drivers have been installed on the print server, Windows NT and Windows 95 clients download these automatically when they connect to the shared printer.
- There are four different print permissions—Full Control, Manage Documents, Print, and No Access. By default, the built-in Everyone group is assigned the Print permission.

For more information on	**See**
Setting up a print server and client	Chapter 5, "Setting Up Print Servers," in Microsoft Windows NT Server *Concepts and Planning*. Chapter 7, "Printing," in the *Microsoft Windows NT Workstation Resource Kit.*
Connecting to printers from non-Microsoft clients	The third-party product documentation specific to the client operating system.

Lesson 3: Configuring a Printer

This lesson shows you how to create a printing pool and set priorities between printers.

This lesson requires that you have completed Lesson 2.

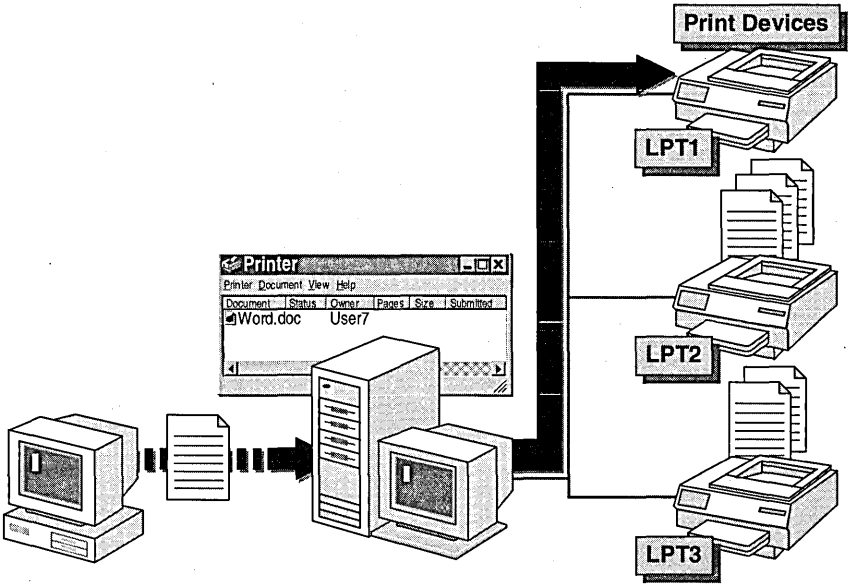
After this lesson, you will be able to:

- Create a printing pool.
- Set priorities between printers.
- Schedule printers to print during specified hours.
- Assign forms to paper trays.
- Set separator pages between print jobs.

Estimated lesson time: 20 minutes

Creating a Printing Pool

If a print device is heavily used, you can create a printing pool to automatically distribute the print jobs to an available print device. A printing pool is one printer connected to multiple print devices through multiple ports of the print server. A printing pool is useful in a network with a high volume of printing because it decreases the time that documents wait in the print queue. It also simplifies administration because multiple print devices can be managed from a single printer.


Print Devices
LPT1
LPT2
LPT3
Printer
Printer Document View Help
Document Status Owner Pages Size Submitted
Word.doc User7

With a printing pool created, the user prints a document without having to find out which print device is available. The printer checks for an available port and sends documents to ports in the order that they were added. Adding the port connected to the fastest print device first ensures that documents are sent to the device that can print the fastest before they are routed to slower print devices in the printing pool.

To create a printing pool, you must first enable printer pooling, and then specify the ports for the print devices that will be pooled on the **Ports** tab of the *printer_name* Properties dialog box. You can also enable printer pooling in the Add Printer Wizard when you add the printer. All print devices to be pooled must use the same printer driver.

Tip Locate the print devices in a printing pool in close proximity, so that users do not have to search several locations for their documents.

▸ To create a printing pool

In this procedure, you create a printing pool for three HP LaserJet 4Si print devices attached to LPT1, LPT2, and COM2.

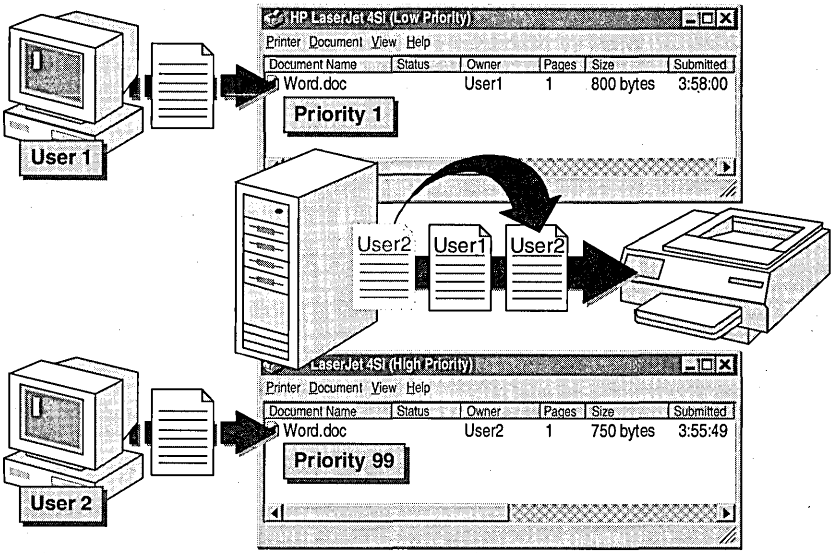
1. Log on as Administrator.
2. In the Printers window, select the HP LaserJet 4Si icon.
3. On the **File** menu, click **Properties.**

   The **HP LaserJet 4Si Properties** dialog box appears.
4. Click the **Ports** tab.

   The **Ports** tab appears, and **LPT1** is selected.
5. Select **Enable printer pooling.**
6. Click **COM2**, and then click **LPT2**.
7. Click **OK**.

Setting Priorities Between Printers

You may need to set priorities between groups of documents if a user prints time-sensitive documents (for example, a proposal for a sales meeting) after large documents have already been sent to the printer (for example, a weekly accounting report).


HP LaserJet 4SI (Low Priority)
Printer Document View Help
Document Name | Status | Owner | Pages | Size | Submitted
Word.doc User1 1 800 bytes 3:58:00
Priority 1
User 1
User2
User1
User2
LaserJet 4SI (High Priority)
Printer Document View Help
Document Name | Status | Owner | Pages | Size | Submitted
Word.doc User2 1 750 bytes 3:55:49
Priority 99
User 2

Setting priorities between printers makes it possible for you to set priorities between groups of documents. For example, you can set priorities so that all documents from executives print before other users, or so that critical documents always print before lower priority documents.

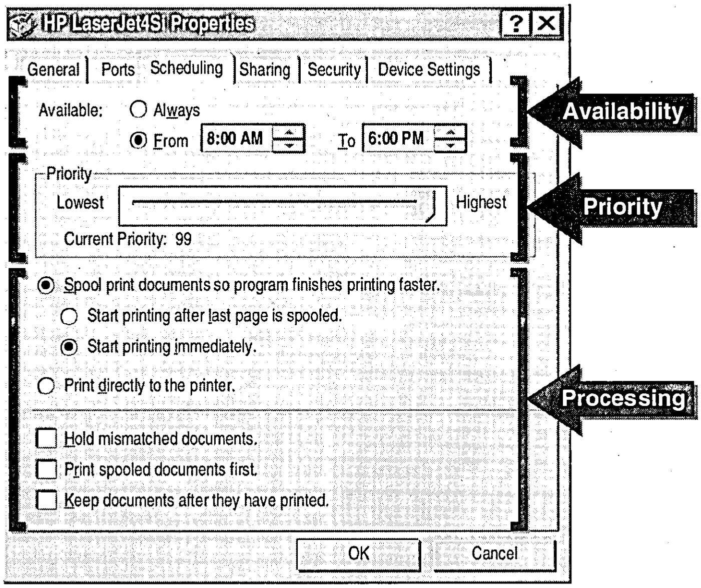
Setting priorities between printers requires that you do the following:

- Add two or more printers for the same print device. These printers must:
  - Be on the same print server.
  - Use the same port to connect to the print device. The port can be either a physical port on the print server or the UNC name of a network printer. For example: \\Server7\HPLaserJet
- Set a different priority for each printer connected to the print device. Then have users print to printers with the appropriate priority.

  For example, if User1 sends documents to a printer with the lowest priority, which is 1, while User2 sends documents to a printer with the highest priority, which is 99, User2's documents will always print before User1's.

Scheduling Printers

You can control when documents are printed by setting the priority on a printer, by setting the available printing times, and by changing how the printer processes documents. You perform these tasks in the *printer_name* **Properties** dialog box.



HP LaserJet4Si Properties

Available: ○ Always
● From 8:00 AM To 6:00 PM

Priority
Lowest Highest
Current Priority: 99

● Spool print documents so program finishes printing faster.
○ Start printing after last page is spooled.
● Start printing immediately.
○ Print directly to the printer.

□ Hold mismatched documents.
□ Print spooled documents first.
□ Keep documents after they have printed.

The following table describes tasks to schedule printers and under what circumstances you would set them.

Perform this task	If you want
Set available printing times	To print large documents during off-peak hours.
Set priorities between printers	To always print critical documents first. 1 is the lowest priority (and the default setting); 99 is the highest priority.
Change how the printer processes documents	To start printing large documents immediately, before they are completely processed.

The following table describes the options for scheduling a task.

Options	Description
Spool print documents so program finishes printing faster	Either this option or the **Print directly to the printer** option is selected. If you choose this option, the documents will spool. This option has two related options that you must choose between.
• **Start printing after last page is spooled**	The printer will not print a document until it is completely spooled. This is useful for documents that are assigned a low priority. Documents that are assigned a higher priority will start printing immediately.
• **Start printing immediately**	The printer starts printing a document before it is completely spooled, which means that it is printed sooner. This is useful for documents that are assigned a high priority.
Print directly to the printer	The document does not spool, which decreases printing time. Select this option only for a non-shared printer. This may be useful for third-party programs that use their own spooling process.
Hold mismatched documents	Documents that do not match the configuration of the printer will not be printed. This prevents errors resulting from documents that use paper sizes different than letter.
Print spooled documents first	A spooled document is printed before a partially spooled document.
Keep documents after they have printed	Documents remain in the print spooler after they are printed, and can be quickly resubmitted for printing.

▶ To set a printer priority

In this procedure, you set the priority on a printer to the highest priority, so that all documents sent to that printer will be printed before documents that are sent to a printer with a lower priority.

1. In the Printers window, select the HP LaserJet 4Si icon.
2. On the **File** menu, click **Properties**.

   The **HP LaserJet 4Si Properties** dialog box appears.
3. Click the **Scheduling** tab.

   Under **Priority**, notice that the default priority is set to 1, the lowest priority.
4. Move the slider to the highest priority.

   Notice that the highest priority is 99. Documents in a printer with this priority will be printed before documents in a printer with lower priorities.

   Leave the **HP LaserJet 4Si Properties** dialog box open for the next procedure.

▸ To set the available printing hours

In this procedure, you set the available printing hours so that print jobs are printed during off-peak hours.

1. In the **HP LaserJet 4Si Properties** dialog box, notice that by default, the printer is available during all hours.
2. Click **From.**
3. Set the available printer hours from 12:00 A.M. until 4:00 A.M.
4. Click **OK.**

▸ To test the available printing hours

1. In the Printers window, double-click the HP LaserJet 4Si icon.

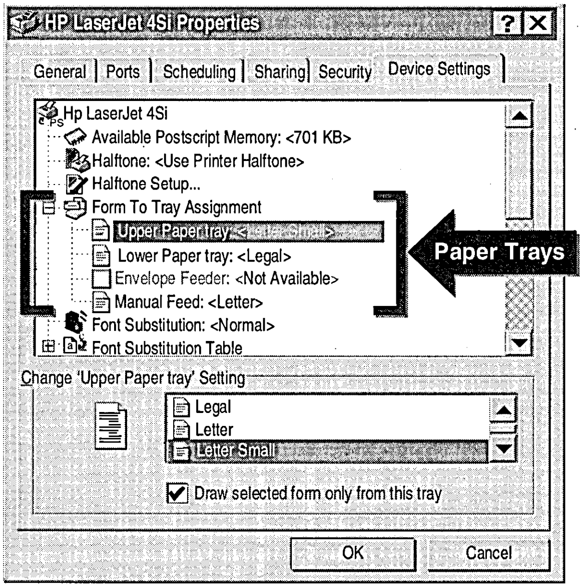
   The **HP LaserJet 4Si** window appears.
2. On the **Printer** menu, verify that the **Set As Default Printer** command is selected.
3. On the **Printer** menu, click **Pause Printing** to cancel the selection (remove the check mark).

   Note that if you already turned off the **Pause Printing** menu command for the printer in a previous procedure, this menu command will already appear without a check mark next to it.
4. In the LabFiles\Public\Library folder, double-click the file named Bronte.txt.
5. Arrange the Bronte–Notepad window and the HP LaserJet 4Si window so that you can see the contents of each.
6. Print Bronte.txt.

   Look at the status of the file to be printed in the HP LaserJet 4Si window and notice that the status of the document is blank (after it has finished spooling). This indicates that the printer is not attempting to print the document.
7. Close Notepad.

Assigning Forms to Paper Trays

In Windows NT, a *form* refers to the paper size and type used by a print device. If a print device has multiple trays that hold different types of forms, you can assign a form to a specific paper tray. Users can then select the form from within the program that they are using. When they print a document, the print job will be routed to the correct paper tray.



Hp LaserJet 4Si
Available Postscript Memory: <701 KB>
Halftone: <Use Printer Halftone>
Halftone Setup...
Form To Tray Assignment
Upper Paper tray: <Letter Small>
Lower Paper tray: <Legal>
Envelope Feeder: <Not Available>
Manual Feed: <Letter>
Font Substitution: <Normal>
Font Substitution Table

Change 'Upper Paper tray' Setting
Legal
Letter
Letter Small

☑ Draw selected form only from this tray

The default form setting for a paper tray is Letter. Examples of forms are:

- Legal size
- Envelopes #10
- Note size
- Letter small

▸ To assign a form type to a paper tray

In this procedure, you assign a paper type (form) to a paper tray so that when users print a document using a specified form, the print job will automatically be routed to and adjusted for the correct tray.

1. Make sure that the HP LaserJet 4Si window is open.
2. On the **Printer** menu, click **Properties**.

   The **HP LaserJet 4Si Properties** dialog box appears.

3. Click the **Device Settings** tab.

   Notice that there are multiple selections under **Form To Tray Assignment.** This is because no specific tray assignments have been configured.

4. Click **Upper Paper tray.**
5. Under **Change 'Upper Paper tray' Setting**, click **Letter Small.**

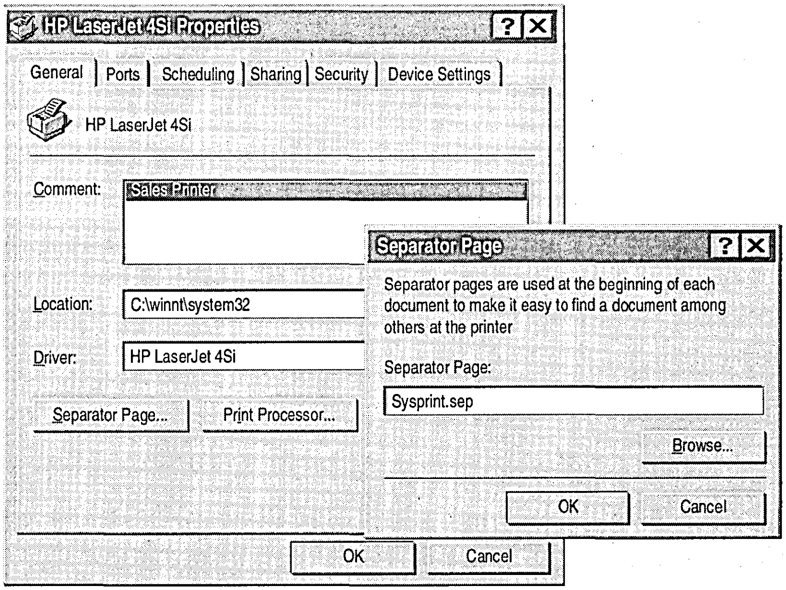
   Notice that **Upper Paper tray** indicates that Letter Small is the default paper size.

6. Click **OK.**

Setting a Separator Page

Separator pages have two functions:

- To identify and separate printed documents.
- To switch print devices between the different print modes. Print modes process documents into a format that the print device understands.



Comment: Sales Printer

Location: C:\winnt\system32

Driver: HP LaserJet 4Si

Separator pages are used at the beginning of each document to make it easy to find a document among others at the printer

Separator Page: Sysprint.sep

Windows NT includes three separator page files. They are located in the *systemroot*\System32 folder.

The following table describes the function of the default separator pages.

File name	Function
Sysprint.sep	Prints a page before each document. Compatible with PostScript printing devices.
Pcl.sep	Switches the printing mode to PCL for HP-series printing devices and prints a page before each document.
Pscript.sep	Switches the printing mode to PostScript for HP-series printing devices, but does not print a page before each document.

To set up a separator page

In this procedure, you set up a separator page to print between documents. This separator page includes the user's name and the date and time that the document was printed.

1. Make sure that the **HP LaserJet 4Si** window is open.
2. On the **Printer** menu, click **Properties**.

   The **HP LaserJet 4Si Properties** dialog box appears.
3. On the **General** tab, click **Separator Page**.

   The **Separator Page** dialog box appears.
4. Click **Browse**.

   Another **Separator Page** dialog box appears.

   Notice the three default separator page files in the System32 folder.
5. Click Sysprint.sep, and then click **Open**.

   The first **Separator Page** dialog box appears, and it has the path and file name of the selected separator page.
6. Click **OK** to return to the **HP LaserJet 4Si Properties** dialog box.
7. Click **OK**, and then log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- A printing pool is one printer connected to multiple print devices through multiple ports of the print server.
- You can create a printing pool to automatically distribute print jobs to an available print device. The distribution is transparent to users.
- Setting priorities between printers makes it possible for you to set priorities between groups' documents.
- Setting priorities between printers requires two or more printers for the same print device. The printers must be on the same print server.
- Documents can be scheduled to print between certain hours, reducing print device load during peak traffic hours.

For more information on	See
Configuring printers	Chapter 5, "Setting Up Print Servers," in Microsoft Windows NT Server *Concepts and Planning.* Chapter 7, "Printing," in the *Microsoft Windows NT Workstation Resource Kit.*

Best Practices

The following checklist provides best practices for setting up a network printer:

□ Use the same guidelines that apply to any shared resource. Create a local "*printer_name* Users" group with Print permissions and then put global groups into the local group.

□ Remove the Print permission from the default group Everyone. Instead, assign the Print permission to the built-in group Users. This will limit printer use to those users in the domain for which you have created accounts.

□ Distribute the administrative load. If security is not an issue, assign the "*printer_name* Users" group the Manage Documents or Full Control print permission, or add a user to the Print Operators group to manage the printer.

□ Secure the print device in a locked room if it is used for confidential information. Let only members of the Administrators group manage the printer.

□ For printing pools, place the print devices physically close to each other. Then users do not have to check separate locations for their printed documents.

□ Create multiple printers with different schedules to reduce printer traffic during peak hours. Have users send large documents, such as accounting reports, to a printer that is available only at night so that those documents will wait until off-peak hours to be printed.

□ Document information about printers and the users who have the ability to administer them.

□ Use the Windows NT auditing feature to keep track of changes made by users who manage network printers. Auditing is covered in Chapter 9, "Auditing Resources and Events."

Note If you want to remove the accounts that were created by running the Chapter7.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter7.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. What is the difference between a printer and a print device?

   ____

   ____

2. What is the default print permission for users?

   ____

   ____

3. Scenario: You have added and shared a printer. What do you do to set up clients running Windows NT 4.0 so that they can print, and why?

   ____

   ____

4. What can you do to make sure one user's documents are printed before another user's documents?

   ____

   ____

5. Why would you create a printing pool?

   ____

   ____

Answer Key

Procedure Answers

Page 286

▸ To assign permissions to a group

2. Under **Name**, which built-in local groups are assigned the Full Control permission by default?

   The Administrators, Print Operators, and Server Operators groups.

   Under **Name**, which system groups are assigned the Manage Documents permission by default?

   The CREATOR OWNER system group.

Page 287–288

▸ To test the Manage Documents permission for User7-A

3. What options are available to User7-A in the first **Add Printer Wizard** dialog box?

   User7-A can connect to a printer on another computer.

6. Can you change permissions?

   No, because User7-A only has permission to view security information.

7. Are the options to share a printer available?

   No, because the Manage Documents permission does not give you the capability to share a printer.

8. Are the options to change printing hours available?

   No, because the Manage Documents permission only allows you to control settings on all print jobs, not settings on the printer.

9. Can you add a port?

   No, because the Manage Documents permission does not give you the capability to change printer properties.

11. Can you purge documents from the printer?

    No, because the Manage Documents permission does not give you the capability to delete other user's print jobs.

Page 288

▸ To test the Full Control permission for User7-B

2. Try to perform the following tasks. In the following list, mark the tasks that are available with the Full Control permission:

   User7-B can perform all of these tasks except add a printer.

Page 301

Review Answers

1. What is the difference between a printer and a print device?

   A printer is the software interface between the operating system and the print device. The print device is the hardware that produces printed documents.

2. What is the default print permission for users?

   The Everyone group is assigned the Print permission. All users are automatically members of that group by default.

3. Scenario: You have added and shared a printer. What do you do to set up clients running Windows NT 4.0 so that they can print, and why?

   Do nothing to set them up to print. When the client connects to the shared printer, Windows NT automatically copies the printer driver to the client.

4. What can you do to make sure one user's documents are printed before another user's documents?

   Add an additional printer with a higher priority for the same print device. For the user whose documents you want printed first, set that user's default printer to be the one with the higher priority.

5. Why would you create a printing pool?

   To automatically distribute print jobs to multiple print devices so that they are printed faster. It is easier to manage one printer than to manage a printer for each print device.

CHAPTER 8

Administering a Network Print Server

About This Chapter

This chapter presents the post-installation and configuration print server administration tasks, including tasks related to managing documents and printers, and identifying printing problems. In the hands-on procedures, you will have an opportunity to perform many of these tasks on your own printer.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- The knowledge and skills covered in Chapter 7, "Setting Up a Network Print Server."
- Installed a printer on your computer. If your server does not have a printer installed, see Chapter 7, "Setting Up a Network Print Server," for instructions on how to install it.
- Knowledge about the Administrators, Print Operators, Server Operators, and Power Users groups.
- A user account created named User8 that is a member of the local Print Operators group. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter8.cmd to create the user account and add it to the Print Operators group.

Lesson 1: Introduction to Administering Print Servers

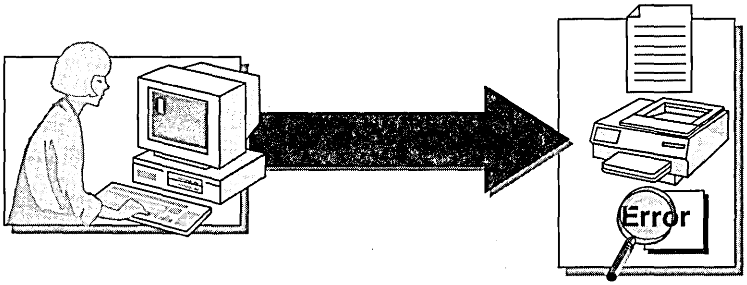
This lesson introduces you to print server administration tasks and the requirements for performing the tasks.

After this lesson, you will be able to:

- List the print server administration tasks.
- Describe the requirements for administering printers.

Estimated lesson time: 10 minutes

The term *administering a print server* refers to tasks that are done *after* the print server is installed and configured.



You can administer a print server locally or remotely over the network. Administration tasks include:

- Managing documents, which includes the following tasks:
  - Deleting a document
  - Setting a notification
  - Changing a document priority
  - Setting a printing time for a document
- Managing printers, which includes the following tasks:
  - Pausing and resuming a printer
  - Redirecting documents
  - Changing print device settings
  - Purging a printer
  - Taking ownership of a printer
- Identifying and solving common printing problems.

Print Server Administration Requirements

Print server administration can be done from any computer running Windows NT.

To perform administration tasks, you must meet one of the following requirements:

- You must be a member of the Administrators, Print Operators, Server Operators, or Power Users groups on the print server.

  The following table describes the built-in capabilities required for administration.

Group	Built-in capabilities
Print Operators and Server Operators	Add and remove printers Share printers Take ownership of a printer
Power Users (on Windows NT Workstation and member servers only)	Add and remove printers Share printers Take ownership of a printer

- You must have the Full Control print permission for the printer. The Full Control print permission is assigned to the Administrators, Print Operators, Server Operators, and Power Users group by default.

Note If you have the Manage Documents print permission for the printer, you can perform administration tasks on documents only.

Lesson Summary

The following information summarizes key points in this lesson:

- Print server administration tasks include administering documents and printers and troubleshooting printing problems.
- The term *administering a print server* refers to tasks that are done *after* the print server is installed and configured.
- Print server administration can be done from any computer running Windows NT as long as you have the appropriate permissions.
- To perform printer administration tasks, you must be a member of the Administrators, Print Operators, Server Operators, or Power Users group on the print server or have the Full Control print permission for the printer.
- Administering documents only requires the Manage Documents print permission for the printer.

For more information on	**See**
Administrators, Print Operators, Server Operators, or Power Users groups	Chapter 3, "Setting Up Group Accounts," in this book.
	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Print permissions	Chapter 7, "Setting Up a Network Print Server," in this book.

Lesson 2: Managing Documents

The term *managing documents* refers to tasks that control when users' documents are printed, and who gets notified when the documents are printed. This lesson explains how to control print jobs by setting the notification, priority, and available printing time for a document.

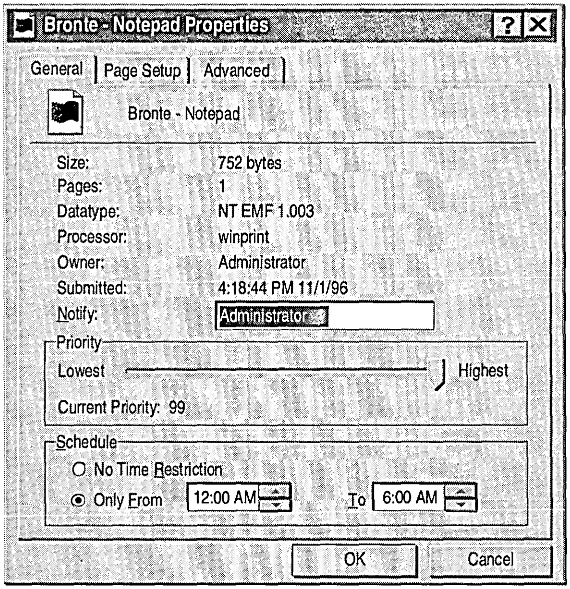
After this lesson, you will be able to:

- Set a notification for a document.
- Set the printing time for a document to print.
- Delete a document from a printer.

Estimated lesson time: 20 minutes

Setting a Notification, Priority, and Printing Time

You can control print jobs by setting the notification, priority, and printing hours. To set the notification, priority, and printing hours for a document, a user must have the Full Control or Manage Documents print permission for the appropriate printer.


Bronte - Notepad Properties

Bronte - Notepad

Size: 752 bytes
Pages: 1
Datatype: NT EMF 1.003
Processor: winprint
Owner: Administrator
Submitted: 4:18:44 PM 11/1/96
Notify: Administrator

Priority
Lowest — Highest
Current Priority: 99

Schedule
○ No Time Restriction
● Only From 12:00 AM To 6:00 AM

The following table describes the situations in which you would set a notification, change a document priority, or set available printing hours.

Do this	In this situation
Set a notification	Change the print notification when someone other than the user who printed the document needs to retrieve it—for example, to notify an editor when the document is ready for him or her to pick up.
Change a document priority	Change a priority so that a critical document is printed before other documents.
Set available printing hours	Set night hours for large documents that take a long time to be printed. This allows you to make sure that the document spools correctly during work hours, but that it is printed at night.

▸ To prepare the printer

In this procedure, you pause the printer and then print two documents to provide documents to manage.

1. Log on as Administrator.
2. Click the **Start** button, point to **Settings**, and then click **Printers**.

   The Printers window appears.
3. Double-click the icon for your printer.

   The *printer_name* window appears.
4. On the **Printer** menu, click **Set As Default Printer**.
5. On the **Printer** menu, click **Pause Printing** to pause the printer.

   Notice that the title bar now shows that your printer is paused.
6. Leave the *printer_name* window open, and switch to Windows NT Explorer.
7. Expand the LabFiles\Public\Library folder, hold down the SHIFT key, and then click both Hamlet.txt and Bronte.txt.
8. Right-click the selected documents, and then, on the shortcut menu that appears, click **Print**.
9. Switch back to the *printer_name* window.

   Both documents appear in the *printer_name* window.

▸ To set a notification

In this procedure, you set a notification so that User8 receives a message when a document has finished printing.

1. In the *printer_name* window, click Bronte.txt.
2. On the **Document** menu, click **Properties**.

   The **Bronte-Notepad Properties** dialog box appears.
3. In the **Notify** box, type **user8**

   Leave the dialog box open and continue to the next procedure.

▸ To change a document priority

In this procedure, you increase the priority of Bronte.txt for User8.

1. On the **General** tab of the **Bronte-Notepad Properties** dialog box, notice the default priority of 1, which is the lowest priority.
2. Use the slider to increase the priority of the document to 50, and then click **OK**.

   Nothing visibly changes in the *printer_name* window, but the document will be printed before other documents with a priority lower than 50, and after documents with a priority higher than 50.

   Leave the dialog box open and continue to the next procedure.

▸ To set available printing hours for a document

1. In the *printer_name* window, click Hamlet.txt.
2. On the **Document** menu, click **Properties**.

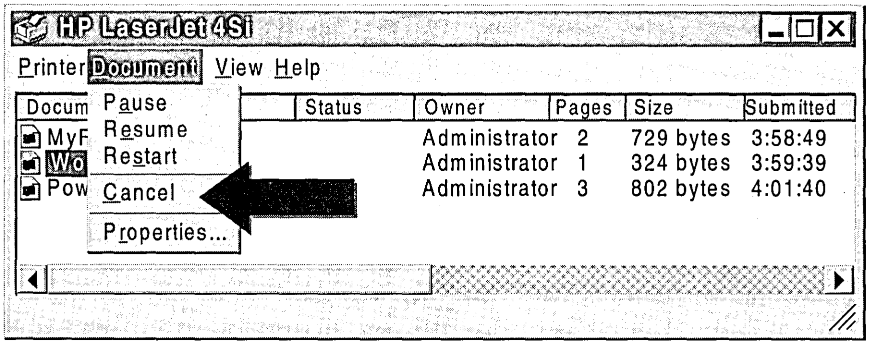
   The **Hamlet-Notepad Properties** dialog box appears.
3. Under **Schedule**, make sure that **Only From** is selected.
4. In the **Only From** box, type **12:30** AM
5. In the **To** box, type **3:30** AM and then click **OK**.

   Nothing changes visibly in the *printer_name* window, but the printer will not begin to print the Hamlet.txt file before 12:30 A.M. or after 3:30 A.M. If the printer has not completed printing the documents ahead of Hamlet.txt before 3:30 A.M., the Hamlet.txt will be held until 12:20 A.M. on the following day.

   Leave the *printer_name* window open and continue to the next topic.

Deleting a Document from a Printer

You may need to delete a document before it is printed. For example, if the document has the wrong printer settings, delete it before it is printed incorrectly.



Docum	Status	Owner	Pages	Size	Submitted
MyF		Administrator	2	729 bytes	3:58:49
Wo		Administrator	1	324 bytes	3:59:39
Pow		Administrator	3	802 bytes	4:01:40

To delete other users' documents, a user must have the Full Control or Manage Documents print permission. Users with the Print permission can delete their own documents.

▸ **To delete a document using the DELETE key**

1. In the *printer_name* window, click Bronte.txt.
2. Press the DELETE key.

   Notice that the document disappears from the window.

▸ **To delete a document using the Cancel command**

1. In the *printer_name* window, click Hamlet.txt.
2. On the **Document** menu, click **Cancel.**

   Notice that the document disappears from the window.
3. Close the *printer_name* window.
4. Log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- To set the notification, priority, and printing hours for a document, a user must have the Full Control or Manage Documents print permission for the appropriate printer.
- Users with the Print permission can delete their own documents. A user must have the Full Control or Manage Documents permission to delete other users' documents.
- Set a notification when someone other than the user who prints a documents needs to retrieve it.
- Increase a document's priority so that critical documents are printed before other documents.
- Set available printing hours to schedule large documents so that they are printed during off-peak hours.

For more information on	See
Print permissions	Chapter 7, "Setting Up a Network Print Server," in this book.

Lesson 3: Managing Printers

The term *managing printers* refers to tasks that affect the entire printer, not individual documents. This lesson guides you through the steps to perform printer management tasks and explains the situations in which these tasks are useful.

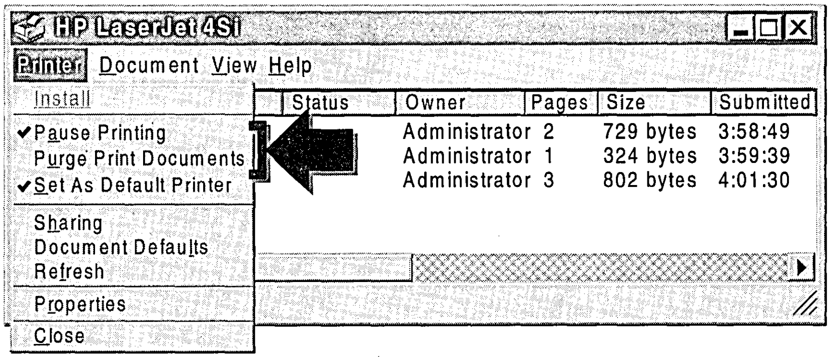
After this lesson, you will be able to:

- Redirect documents to a different printer.
- Pause and resume a printer.
- Purge all the documents in a printer.
- Take ownership of a printer.

Estimated lesson time: 20 minutes

Pausing, Resuming, and Purging a Printer

When you manage a printer, your actions affect all of the documents that are sent to the printer. Pausing, resuming, and purging a printer may be necessary if there is a printing problem.



Status	Owner	Pages	Size	Submitted
	Administrator	2	729 bytes	3:58:49
	Administrator	1	324 bytes	3:59:39
	Administrator	3	802 bytes	4:01:30

The following table describes the situations in which you would pause, resume, or purge a printer.

Do this	In this situation
Pause a printer	If there is a problem with the print device.
Resume a printer	When a non-operational print device is repaired.
Purge a printer	If you need to delete all documents, such as old documents in the spooler.

▸ To prepare the printer

In this procedure, you pause the printer and then print two documents to prepare the printer for the following procedures.

1. Log on as Administrator.
2. Click the **Start** button, point to **Settings**, and then select the icon for your printer.
3. On the **Printer** menu, make sure that **Pause Printing** is selected and that this printer is set as the default printer.
4. Switch to Windows NT Explorer, and then expand the LabFiles\Public folder.
5. Right-click Expenses.doc, and then on the shortcut menu that appears, click **Print.**
6. Repeat step 5 to print the document a second time.

▸ To purge a printer

1. Switch to the *printer_name* window.
2. On the **Printer** menu, click **Purge Print Documents.**

   Notice that all documents disappear from the *printer_name* window.

▸ To resume the *printer_name* printer

- On the **Printer** menu, click **Pause Printing** to resume the printer.

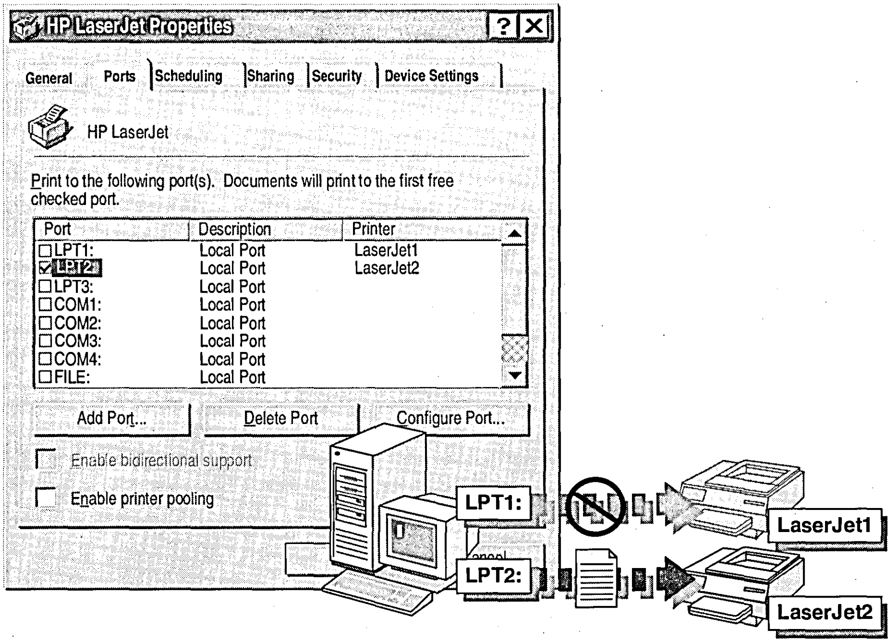
  The check mark next to the **Pause Printing** menu command is removed. Also, the title bar on the printer no longer says "Paused."

Redirecting Documents

If a print device becomes faulty, you may need to redirect documents in a printer to a different print device. This will prevent users from having to resubmit print jobs that are already in the printer. You can redirect documents to a print device on the local print server or on a different print server. However, both print devices must use the same printer driver.

Redirecting Documents on the Local Print Server

To redirect documents to a different print device on the same print server, you need to select the port of the other print device.



HP LaserJet Properties

General | Ports | Scheduling | Sharing | Security | Device Settings

HP LaserJet

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ LPT1:	Local Port	LaserJet1
☑ LPT2:	Local Port	LaserJet2
□ LPT3:	Local Port	
□ COM1:	Local Port	
□ COM2:	Local Port	
□ COM3:	Local Port	
□ COM4:	Local Port	
□ FILE:	Local Port	

□ Enable bidirectional support

□ Enable printer pooling

▸ **To redirect documents to a local print device**

In this procedure, you go through the steps to redirect documents to a different print device on the local print server even though you do not have a second print device.

1. In the *printer_name* window, on the **Printer** menu, click **Properties**.

   The *printer_name* **Properties** dialog box appears.

2. Click the **Ports** tab.

   The **Ports** tab displays the current configuration of the ports.

3. Select the **LPT2** check box, and then click **OK.**

Note You may need to remove the original port to ensure that the documents print to the redirected port.

---

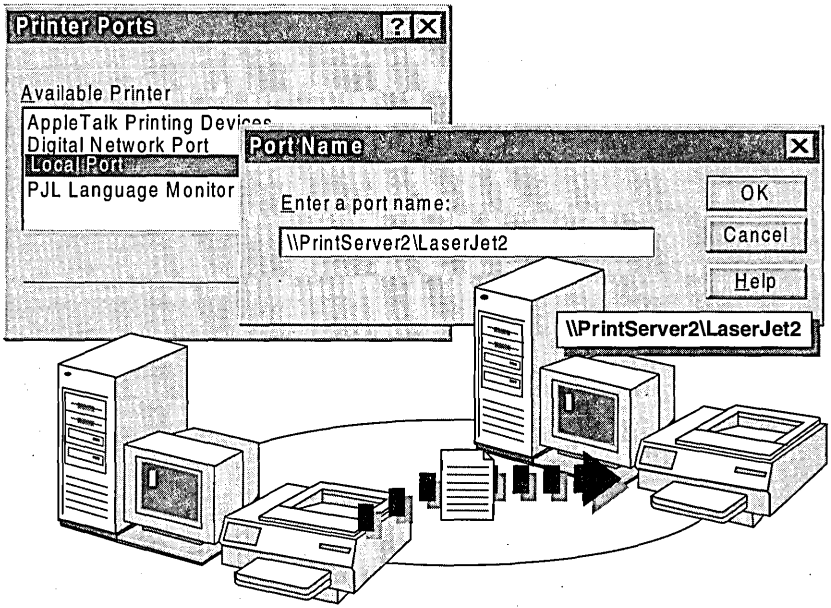
4. Click **OK.**

   If you had two print devices, the document would begin printing on the other print device.

5. Log off.

Redirecting Documents to a Different Print Server

To redirect documents to a print device on a different print server, you have to add a local port for the other print server and provide the print server name and the appropriate share name for the print device, as shown in the following illustration.



Enter a port name: \\PrintServer2\LaserJet2

\\PrintServer2\LaserJet2

To redirect documents to a different print server, the other print device must already exist and be shared on the print server.

The following checklist provides an overview of the tasks required to redirect documents to a different print server. These tasks must be performed on the original print server from any computer running Windows NT:

- □ On the **Ports** tab of the *printer_name* **Properties** dialog box, click to clear the check box of the port that you want to discontinue using, and then click **Add Port**.
- □ In the **Printer Ports** dialog box, click **Local Port**, and then click **New Port**.

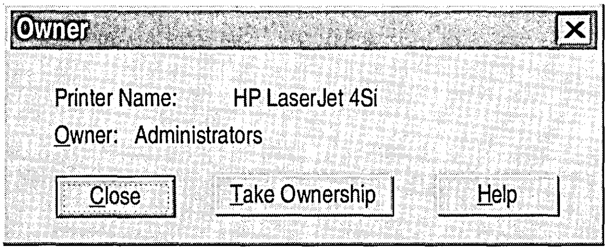
  When adding a network port, you can only add an existing port. Also, you cannot create, delete, or configure ports over the network. You must do this at the local print server.
- □ Type the name of the other print server and share name of the shared print device, click **OK,** and then click **Close**. (For example: \\other_print_server\share_name)

  The new port appears as the selected port for the printer.

Taking Ownership of a Printer

Taking ownership of a printer lets you change printer administrators. This is useful if the printer administrator leaves the company or if you need to change printer permissions.

Taking ownership of a printer is similar to taking ownership of a folder or file. The user who installed the printer owns it. If the user who installed the printer is a member of the Administrators group, the Administrators group owns it. Members of the Administrators group can take ownership of any printer.



Printer Name: HP LaserJet 4Si

Owner: Administrators

▸ **To take ownership of a printer**

In this procedure, you take ownership of a printer that is owned by another user.

1. Log on as User8.
2. In the Printers window, double-click the icon for your printer.

   The *printer_name* window appears.
3. On the **Printer** menu, click **Properties**.

   The *printer_name* **Properties** dialog box appears.

4. Click the **Security** tab, and then click **Ownership**.

   Notice the current owner of the printer. If the owner is Administrators, it is because the user who created the printer was either logged on as Administrator or as a user who was a member of the Administrators group.

5. Click **Take Ownership**.

   Were you able to take ownership? Why or why not?

   ____

6. Click **Owner** to verify that User8 is the new owner.
7. Click **OK** to close the *printer_name* dialog box.

Lesson Summary

The following information summarizes key points in this lesson:

- To redirect documents in a printer to a different print device, both print devices must use the same printer driver.
- To redirect documents to a different print device on the same print server, you need to select the port of the other print device.
- To redirect documents to a print device on a different print server, you have to add a local port for the other print server and provide the print server name and the appropriate share name for the print device.
- Taking ownership of a printer lets you change printer administrators. The user who installed the printer owns it.
- Members of the Administrators group can take ownership of any printer. If any member takes ownership of a printer, the Administrators group becomes the owner.

Lesson 4: Identifying Printing Problems

Printing problems are among the most common problems that users encounter. This lesson describes the printing process, and it also discusses common printing problems and possible solutions.

After this lesson, you will be able to:

- Describe how documents are printed.
- Recognize common reasons why users cannot print.

Estimated lesson time: 20 minutes

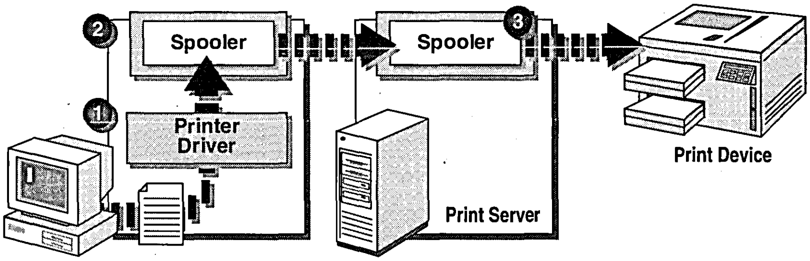
How Documents Are Printed

An overview of the printing process will help you understand how to manage a printer and identify problems. Windows NT has a *spooler* on the print server, which processes and schedules documents for printing. If a document becomes stuck in this spooler, you might need to stop and restart the spooler using the Services program in Control Panel.

Windows NT–based and Windows® 95–based Clients

Windows NT–based and Windows 95–based clients have an additional spooler, which helps to improve printing performance. After a user sends a document to the printer, the following occurs:

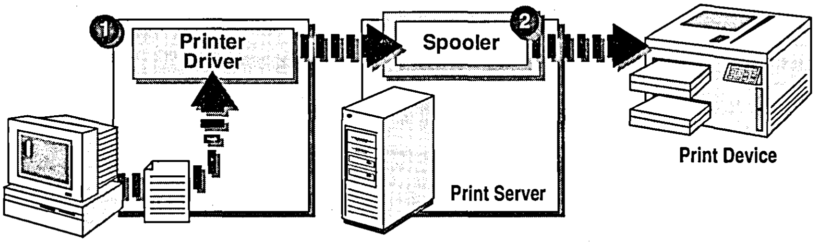
1. The printer driver partially processes the document to an acceptable format for the print device.
2. The document goes to the spooler on the client computer where it stays until there is room in the spooler on the print server.
3. When the print server is available, the spooler on the client sends the job to the print server, where the print server spooler finishes processing the document. The document waits in the spooler until a print device is available. Then, it is printed.



Other Clients

The printing process is the same for client computers that are not running Windows 95 or Windows NT operating systems. For non-Microsoft clients, there is a spooler only on the print server. After the user sends a document to be printed, the following occurs:

1. The printer driver completely processes the document to an acceptable format for the print device.
2. The document waits in the spooler until a print device is available. Then, it is printed.



Identifying and Troubleshooting Printing Problems

One of the most frequent administrative tasks is solving printing problems. Most printing problems can be identified quickly by using the following checklist:

□ Verify that the print device is operational. If some users can print normally, then the problem is not with the print server or print device.

□ Verify that the printer on the print server is using the correct printer driver.

□ Verify that the print server is operational and that there is enough disk space to spool files. For example, if 10 users are all printing large documents at the same time, the print server must have enough disk space to spool all of the documents.

□ If the client is running an operating system other than Windows 95 or Windows NT, verify that the client has the correct printer driver. Computers running Windows NT and Windows 95 automatically copy the correct printer driver when they connect to a network printer.

If a user still has printing problems after you complete the items in the previous checklist, refer to the following table for a description of common problems and solutions.

Problem	Solutions
User receives an Access Denied message when trying to configure a printer from within a program (for example, from within Microsoft Excel).	The user does not have the appropriate permission to change printer configurations. Change the user's permission, or configure the printer for the user.
The document does not print completely or comes out garbled.	Make sure that the correct printer driver is installed on the client.
The hard disk starts thrashing and the document does not reach the print server.	There may be insufficient hard disk space for spooling the document. Create more free space, or, in the registry, move the spooler location to another volume.
There are documents on the print server that will not print and that you cannot delete.	The print spooler may be stalled. On the print server, start the Services program in Control Panel, and then stop and restart the Spooler service.
A user cannot print a document.	Verify that the user's printer is not paused and that the correct default printer is set. Make sure that the print device is online and that it is not out of paper or toner. Verify that the available printing time is configured properly for the user.
A user cannot connect to a printer.	Make sure that the user has the Print permission (for computers running Windows NT or Windows 95). Make sure that the proper printer driver is installed on the computer (for non-Windows NT–based clients).
A 16-bit Windows-based program gives an out-of-memory error on startup.	A default printer is not selected. Create a printer and set it as the default printer.
A user sends a document from an MS-DOS-based program on a Windows NT–based client to the printer, but it is never printed.	Some programs will not print a document until the program terminates. Make sure that the printer driver is correctly installed and then quit the program.

Lesson Summary

The following information summarizes key points in this lesson:

- Knowing the basics of the printing process will help you understand how to manage a printer and identify problems.
- Printing problems may require you to install the correct printer driver, verify a user's print permissions, and perform the tasks of pausing, resuming, and purging a printer.

For more information on	See
Troubleshooting printing problems	http://www.microsoft.com/support/ Chapter 7, "Printing," in the *Microsoft Windows NT Workstation Resource Kit.* Chapter 2, "Printing," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*
The registry	Appendix A, "Windows NT Registry," in Microsoft Windows NT Server *Concepts and Planning.*
The Services program in Control Panel	Windows NT Help.
Print spooler	Chapter 7, "Printing," in the *Microsoft Windows NT Workstation Resource Kit.* Chapter 2, "Printing," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*

Review

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

1. Which of the following are true statements about the requirements for administering print servers? (Circle all that apply.)

   a. You must be a member of the Administrators or Print Operators groups on the print server.

   b. You must be a member of the Administrators, Print Operators, or Server Operators groups on the print server.

   c. You must have the Full Control or Manage Documents print permission for the printer.

   d. You must have the Full Control print permission for the printer.

2. What print permission does a user need to manage documents in a printer?

3. Scenario: The editor has a 1,000-page book that needs to be printed and sent to the printer by 8:00 A.M. tomorrow morning. The editor shares a printer with 10 sales people who are busy preparing and printing customer presentations that need to be ready by 5:00 P.M. today. What can you do to distribute the printing load so that everyone gets his or her documents printed on time?

4. Scenario: The Printer-A print device becomes faulty and needs to be repaired. There are 10 documents in the printer for Printer-A waiting to be printed. There are two other print devices: Printer-B is on the same print server, but it is a different type of print device than Printer-A. Printer-C is on a different print server, but it is the same type as Printer-A. What can you do to print the 10 documents without having users resubmit their print jobs? Please explain your decision.

   ____

   ____

5. Scenario: A user sends a document to a printer, but the printer does not print the document. Which of the following tasks would you perform to identify the problem? (Circle all that apply.)

   a. Verify that the user has the correct print permission.

   b. Verify that the print server and the client have the correct printer drivers.

   c. Check the available disk space on the print server to make sure that there is enough space to spool print jobs.

   d. Verify that the print device is online and that it is not out of paper or toner.

Answer Key

Procedure Answers

Page 319

▸ **To take ownership of a printer**

5. Were you able to take ownership? Why or why not?

   Yes, because User8 is a member of the Print Operators group.

Page 326

Review Answers

1. Which of the following are true statements about the requirements for administering print servers? (Circle all that apply.)

   Answers b and d are correct.

2. What print permission does a user need to manage documents in a printer?

   The Manage Documents or Full Control print permission for the printer.

3. Scenario: The editor has a 1,000-page book that needs to be printed and sent to the printer by 8:00 A.M. tomorrow morning. The editor shares a printer with 10 sales people who are busy preparing and printing customer presentations that need to be ready by 5:00 P.M. today. What can you do to distribute the printing load so that everyone gets his or her documents printed on time?

   You can schedule the 1,000-page book to be printed after 5:00 P.M., when the sales people have finished with their presentations.

4. Scenario: The Printer-A print device becomes faulty and needs to be repaired. There are 10 documents in the printer for Printer-A waiting to be printed. There are two other print devices: Printer-B is on the same print server, but it is a different type of print device than Printer-A. Printer-C is on a different print server, but it is the same type as Printer-A. What can you do to print the 10 documents without having users resubmit their print jobs? Please explain your decision.

   Redirect the printer on Printer-A to Printer-C. You can only redirect printers to print devices that use the same printer driver.

5. Scenario: A user sends a document to a printer, but the printer does not print the document. Which of the following tasks would you perform to identify the problem? (Circle all that apply.)

   Answers b, c, and d are correct.

CHAPTER 9

Auditing Resources and Events

About This Chapter

Through auditing, you can track selected activities of users. This chapter introduces auditing and provides guidance in planning and implementing a domain Audit policy. The hands-on procedures give you an opportunity to plan and implement an Audit policy, set up auditing on files and printers, and use Event Viewer to view audited events and to archive security logs.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- Knowledge about domains, domain controllers, and member servers.
- Knowledge and skills to create user accounts.
- Knowledge about group accounts, including Administrators, Server Operators, and Everyone.
- A printer installed. If you have not installed a printer, see Chapter 7, "Setting Up a Network Print Server."
- A user account named User9. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter9.cmd to create this account.

Lesson 1: Introduction to Auditing

Auditing is a function of Windows NT for maintaining network security. With auditing, you can track user activities and system-wide events on a network, such as:

- The action performed.
- The user who performed the action.
- The date and time of the action.

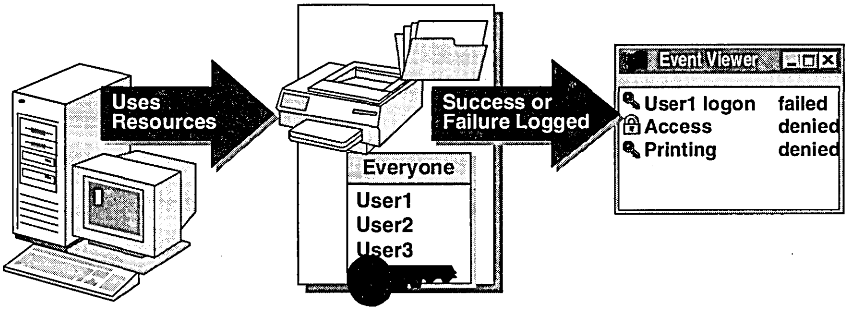
This lesson provides an introduction to Windows NT auditing.

After this lesson, you will be able to:

- Describe the purpose of the Audit policy.
- Describe the requirements to set up and administer the Audit policy.

Estimated lesson time: 10 minutes

You use the Audit policy to select the types of security events that will be audited. When such an event occurs, an entry is added to the computer's security log. The security log becomes your tool for tracking the events that you specify.



On a domain controller, the Audit polity determines the amount and type of security logging that Windows NT Server performs on all domain controllers in the domain. On computers running Windows NT Workstation or on member servers, the Audit policy determines the amount and type of security logging performed on the individual computer.

You can set up one Audit policy for a domain to:

- Track the success and failure of events, such as when users attempt to log on, read a file, make changes to user and group permissions, change the security policy, and make a network connection.
- Eliminate or minimize the risk of unauthorized use of resources.
- Track trends over time by maintaining an archive of security logs. Tracking these trends is useful in determining the use of printers or files.

Auditing Requirements

Auditing can be set up on any computer running Windows NT. However, to audit folders and files, the folders and files must be located on an NTFS volume.

To set up an Audit policy, you must meet the following requirements:

- You must be a member of the Administrators group on the computer where the Audit policy is being set.
- If you are not a member of the Administrators group, you must have the user right *Manage auditing and security log*. This user right is granted to the Administrators group by default.

Note Members of the Server Operators group are unable to set up an Audit policy; however, they can administer security logs—performing tasks such as viewing and archiving them.

Lesson Summary

The following information summarizes the key points in this lesson:

- Auditing is a function of Windows NT for maintaining network security that allows you to track user activities and system-wide events on a network.
- The Audit policy allows you to select the types of security events that will be recorded and will appear in the security log.
- On a domain controller, the Audit policy applies to all domain controllers in the domain.
- On a computer running Windows NT Workstation, or on a member server, the Audit policy applies only to that specific computer.
- To audit folders and files, the folders and files must be located on an NTFS volume.
- To set up an Audit policy, you must have administrative privileges for the computer.

For more information on	**See**
Overview of auditing	Windows NT Help.
Overview of Windows NT security	Chapter 6, "Windows NT Security," in the *Microsoft Windows NT Workstation Resource Kit.*
User rights and group accounts	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Domains, domain controllers, and member servers	Chapter 1, "Introduction to Windows NT," in this book.

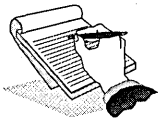
Lesson 2: Planning and Implementing the Audit Policy

This lesson provides guidelines for planning a domain Audit policy in networks that have minimum, medium, and high levels of security. The lesson also covers how to define the Audit policy and how to audit folders, files, and printers.

After this lesson, you will be able to:

- Plan an Audit policy and determine which events to audit.
- Set up an Audit policy for the domain in User Manager for Domains.
- Set up auditing on folders and files in Windows NT Explorer.
- Set up auditing on printers using menu commands in the Printers window.

Estimated lesson time: 30 minutes



Planning the Audit Policy

The Audit policy determines the types of events to audit and how to track each event—by its success or its failure. Before you implement the Audit policy, it is important to determine the following:

- Determine the events to audit for your network.

To track	Consider auditing
Unauthorized logon attempts	Users logging on and off
Unauthorized attempts to use resources	Use of folder and file resources
System tasks performed by a user	Use of user rights
Changes made to user and group accounts	User and group management
Changes made to the user rights or audit policy	Security policy changes
Tampering with a server	Restarting or shutting down the system
Which programs users are using	Process tracking

- Determine whether to audit the success or failure of an event, or both.
  - Tracking the success of events can tell you how often users gain access to specific files or printers. You can use this information in resource planning.
  - Tracking the failure of events will alert you to possible security breaches.

  In minimum-security networks, consider auditing:

  - Successful use of resources, only if you need this information for planning purposes.
  - Successful use of sensitive and confidential data, such as payroll files.

In medium-security networks, consider auditing:

- Successful use of key resources.
- Successful and unsuccessful administrative and security policy changes.
- Successful use of sensitive and confidential data, such as payroll files.

In high-security networks, consider auditing:

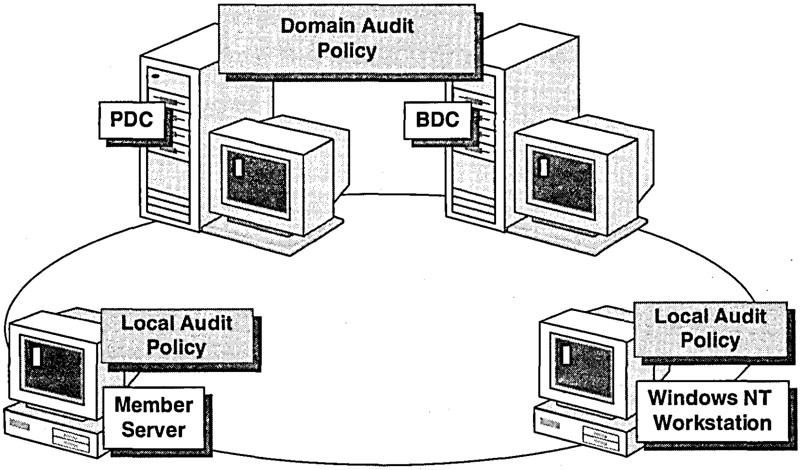
- Successful and unsuccessful user logons.
- Successful and unsuccessful use of all resources.
- Successful and unsuccessful administrative and security policy changes.

Important Because auditing creates overhead on the CPU and on the hard disk, always audit only those events that provide information that is useful in your network.

Implementing the Audit Policy

The Audit policy is set on a computer-by-computer basis. For example, to audit events that occur on the primary domain controller, such as user logon attempts and changes made to user accounts, you must set the Audit policy on the primary domain controller.

To audit events on any other computer in the domain, such as access to a file on a member server, you must set the Audit policy on that computer.



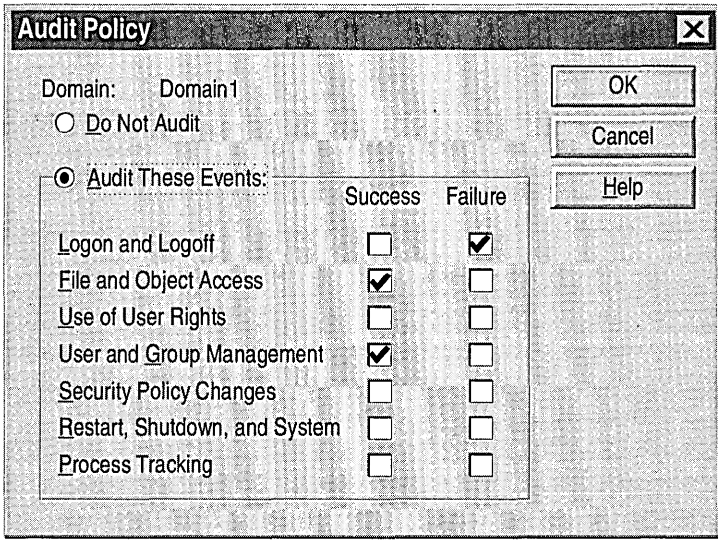
Events are recorded in the local computer's security log, but they can be viewed from any computer by a user who has administrative privileges on the computer where the events occurred.

Setting up auditing is a two-part process:

- Defining the Audit policy by selecting the events to audit in User Manager for Domains (or in User Manager on computers running Windows NT Workstation or on member servers).
- Specifying the files, folders, and printers to audit and the users and groups that you want to track. You use Windows NT Explorer to specify the folder and file events to audit. You use the Printers window to specify printer events to audit.

Defining the Domain Audit Policy

The first step of setting up the Audit policy is to select the events to audit in User Manager for Domains. To gain access to the **Audit Policy** dialog box, on the **Policies** menu, click **Audit.**



Domain: Domain1

○ Do Not Audit

● Audit These Events:

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

The following table describes the types of events that you can audit.

This event	Is used to track when
Logon and Logoff	A user logs on or off, or makes or breaks a network connection.
File and Object Access	A user accesses a folder, file, or printer that is set for auditing. This event must be selected to audit file or print resources.
Use of User Rights	A user exercises a right (except those rights related to logging on and logging off).
User and Group Management	A user account or group is created, modified (renamed, disabled, password changed, and so on), deleted, or when account restrictions, such as logon hours and workstation restrictions, are modified.
Security Policy Changes	A change is made to the user rights, audit, or trust relationship policies.
Restart, Shutdown, and System	A user restarts or shuts down the computer, causing an event to occur that affects system security. (For example, the audit log fills up and entries are discarded.)
Process Tracking	Events occur that cause programs to start—for example, selecting a program on the **Start** menu, or clicking a link on a Web page that starts a Setup program.

Note If you set up an Audit policy on a computer running Windows NT Workstation or on a member server, you use User Manager. All **Audit Policy** dialog box options in User Manager are identical to those in User Manager for Domains.

▶ To plan an Audit policy

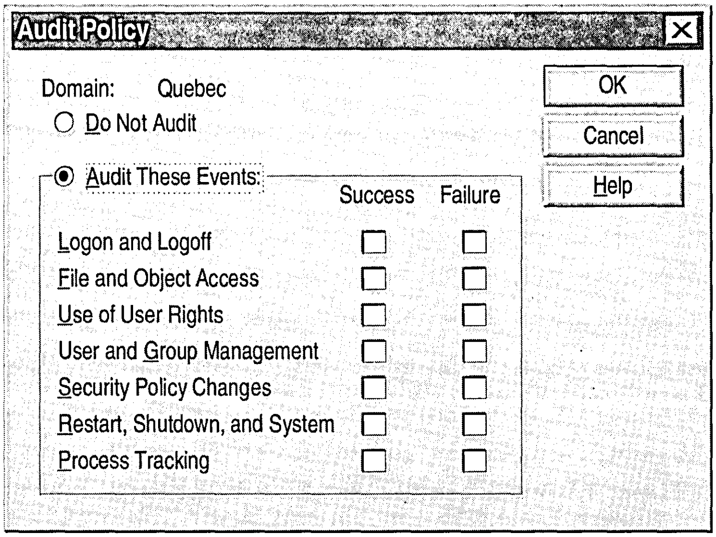
Scenario: As the administrator for the Quebec office of World Wide Importers, you need to plan the Audit policy for the Quebec domain. World Wide Importers is a medium-security to high-security network. You need to determine:

- Which types of events to audit.
- Whether to audit the success or the failure of an event, or both.

Use the following criteria to make your decisions:

- Record unsuccessful attempts to gain access to the network.
- Record unauthorized access to the database that contains the payroll and employee files.
- For billing purposes, track color printer usage.
- Track any time that someone tries to tamper with the server hardware.
- Keep a record of actions performed by an administrator to track unauthorized changes.
- Track backup procedures to prevent data theft.
- Track which users are playing computer games.

Record your decisions by marking them directly onto the following illustration of the **Audit Policy** dialog box.



Domain: Quebec

○ Do Not Audit

● Audit These Events:

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

▸ To define the Audit policy

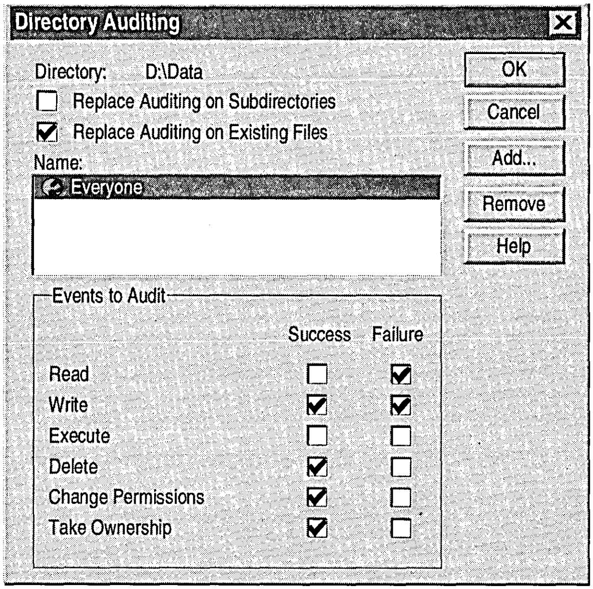
In this procedure, you define the Audit policy based on your plan in the previous procedure.

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **User Manager for Domains**.
3. On the **Policies** menu, click **Audit**.

   The **Audit Policy** dialog box appears.
4. Click **Audit These Events.**
5. Select the **Success** or **Failure** check box (or both) for the events that you planned.
6. Click **OK.**
7. Quit User Manager for Domains.

Auditing Folders and Files

Once you define the Audit policy, the next step is to specify the folders or files to audit, the events to audit for the folders or files, and which users and groups you want to track using them. To gain access to the **Directory Auditing** dialog box, in Windows NT Explorer, right-click the folder or file, click **Properties,** click the **Security** tab, and then click **Auditing**.



Directory: D:\Data

☐ Replace Auditing on Subdirectories

☑ Replace Auditing on Existing Files

Name:

Everyone

Events to Audit

	Success	Failure
Read	☐	☑
Write	☑	☑
Execute	☐	☐
Delete	☑	☐
Change Permissions	☑	☐
Take Ownership	☑	☐

The following table explains the options for auditing folders. These options do not appear if you are auditing files.

Do this	If you want to
Select the **Replace Auditing on Subdirectories** check box.	Have auditing changes apply to all folders within the folder. By default, auditing changes apply only to the selected folder and its files.
Click to clear the **Replace Auditing on Existing Files** check box.	Apply auditing changes to the folder only. This check box is selected by default. Clearing this check box means that existing files will not be modified.

The following table describes the events that you can audit for both folders and files.

Audit this event	To track
Read	When a user opens a file; views its attributes, permissions, or owner; or copies the file. When a user views a folder's content, attributes, permissions, or owner. Audit Read for all sensitive data.
Write	When a user changes a file's content or attributes; views its permissions or owner; or copies the file. When a user creates a folder or file, changes attributes, or views the permissions or owner. Audit Write for all sensitive data.
Execute	When a user views a file's attributes, permissions, or owner; or starts a program. When a user changes a folder; or views its attributes, permissions, or owner. Audit Execute in high-security networks.
Delete	Deleted folders or files. Tracks copying of files. Audit Delete for all sensitive data and in medium- and high-security networks.
Change Permissions	Changes to folder or file permissions. Audit Change Permissions in medium- and high-security networks.
Take Ownership	Changes to folder or file ownership. Audit Take Ownership in medium- and high-security networks.

Auditing the Everyone Group

Auditing is a good example of when you would use the Everyone group. The Everyone group includes all local and remote users who have connected to the computer, including those who connect as Guest. By auditing the Everyone group, you can track use of a resource by anyone who can connect to the resource, and not just the users that you have created accounts for in the domain.

▸ To audit a file

In this procedure, you audit the Bronte.txt file and any member of the Everyone group who successfully deletes it, changes permission on it, or takes ownership of it.

1. Start Windows NT Explorer and expand the LabFiles\Public\Library folder.
2. Right-click Bronte.txt, and then on the menu that appears, click **Properties**.

   The **Bronte Properties** dialog box appears.

3. Click the **Security** tab.

Note Auditing can only be done on NTFS partitions. If there is no **Security** tab, the selected file is not on an NTFS partition.

---

4. Click **Auditing**.

   The **File Auditing** dialog box appears.

5. Click **Add**.

   The **Add Users and Groups** dialog box appears.

6. Under **Names**, click **Everyone**, and then click **Add**.
7. Click **OK**.

   The **Everyone** group appears under **Name** in the **File Auditing** dialog box.

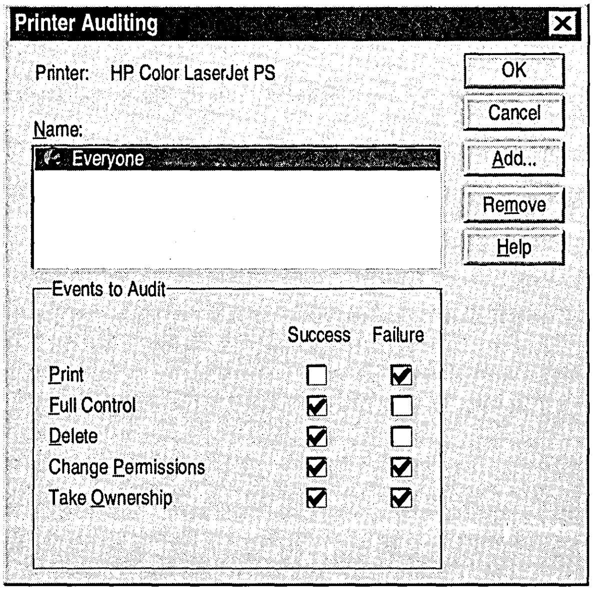
Note You can easily remove a user or group from auditing by selecting its name and then clicking **Remove**.

---

8. Under **Events to Audit**, select the **Success** check box for the following events:
   - **Delete**
   - **Change Permission**
   - **Take Ownership**
9. Click **OK** to apply your changes and return to the **Bronte Properties** dialog box.
10. Click **OK** to return to Windows NT Explorer.
11. Quit Windows NT Explorer.

Auditing a Printer

Setting up auditing on a printer is similar to setting up auditing on folders and files. First you define the Audit policy, and then you specify the printer events to audit, and the users and groups that you want to track using the printer. To gain access to the **Printer Auditing** dialog box, in the Printers window, double-click the printer, on the **Printer** menu, click **Properties**, click the **Security** tab, and then click **Auditing**.



Printer Auditing

Printer: HP Color LaserJet PS

Name:

Everyone

Events to Audit

	Success	Failure
Print	□	☑
Full Control	☑	□
Delete	☑	□
Change Permissions	☑	☑
Take Ownership	☑	☑

The following table explains the options for auditing printers.

Audit this event	To track
Print	Printer usage. This is useful for billing individual departments.
Full Control	Changes to job settings; pausing, restarting, moving, or deleting documents; sharing a printer; or changing printer properties. This is useful in high-security networks.
Delete	Deleted print jobs. This is useful in high-security networks.
Change Permissions	Changes to printer permissions. This is useful in medium- and high-security networks.
Take Ownership	Changes to printer ownership. This is useful in medium- and high-security networks.

▶ To audit a printer

In this procedure, you audit a printer and any member of the Everyone group who successfully prints to it, changes permission on it, or takes ownership of it.

1. Click the **Start** button, point to **Settings**, and then click **Printers**.
2. In the Printers window, double-click any printer.
3. On the **Printer** menu, click **Properties**.

   The *printer_name* **Properties** dialog box appears.
4. Click the **Security** tab, and then click **Auditing**.

   The **Printer Auditing** dialog box appears.
5. Click **Add**.

   The **Add Users and Groups** dialog box appears.
6. Under **Names**, click **Everyone**, and then click **Add**.
7. Click **OK**.

   The **Everyone** group appears under **Name** in the **Printer Auditing** dialog box.
8. Under **Events to Audit**, select the **Success** check box for the following events:
   - **Print**
   - **Change Permissions**
   - **Take Ownership**
9. Click **OK** to apply your changes.
10. Click **OK** to close the *printer_name* **Properties** dialog box.
11. Close the *printer_name* window.
12. Close the Printers window.
13. Log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- When planning the Audit policy, determine what resources and actions are necessary to monitor.
- The Audit policy is set on a computer-by-computer basis. If it is set on the PDC, you can audit events that occur on all domain controllers. If it is set on a computer running Windows NT Workstation or on a member server, you can only audit events on that particular computer.
- To set up auditing, first define the Audit policy for the domain or the computer, specify the folder, file, and printer events to audit, and then specify the users and groups whose use of the resources you want to track.
- Audit the Everyone group to track use of a resource by all users that can connect to it, and not just its use by domain users.

For more information on	See
The procedure for auditing a file or directory	Windows NT Help.
The procedure for changing the printer settings	Windows NT Help.
Setting up auditing	Chapter 9, "Monitoring Events," in Microsoft Windows NT Server *Concepts and Planning.*
Auditing file and folder access	Chapter 37, "Windows NT Workstation Troubleshooting," in the *Microsoft Windows NT Workstation Resource Kit.*
The Everyone group	Chapter 3, "Setting Up Group Accounts," in this book. Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning.*

Lesson 3: Using Event Viewer to View the Security Log

Event Viewer provides information about errors, warnings, and the successes or failures of tasks. This lesson describes the three types of logs created in Event Viewer, but focuses on the security log. The lesson also shows you how to use Event Viewer to view information recorded as a result of an audited event.

This lesson requires that you have completed Lesson 2.

After this lesson, you will be able to:

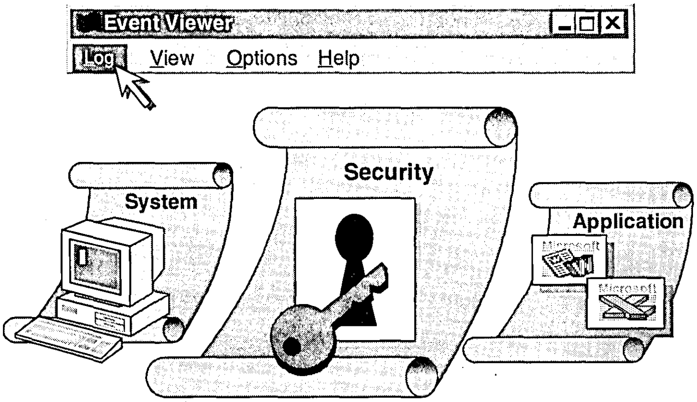
- Use Event Viewer to view the security log of a local and remote computer.
- Use the **Filter Events** menu command to filter and view specific events.
- Use the **Find** menu command to locate events in the security log.

Estimated lesson time: 30 minutes

Event Viewer provides information about errors, warnings, and the successes or failures of tasks. This information is stored in one of three types of logs:

- *System log*. Contains errors, warnings, and information generated by Windows NT and third-party components, such as a network adapter card driver. The selection of events that are recorded is preset by Windows NT and the third-party components.
- *Security log*. Contains information about the success or failure of audited events. The events that are recorded are a result of your Audit policy.

- *Application log*. Contains errors, warnings, or information generated by programs, such as a database or e-mail program. The selection of events that are recorded is preset by the program developer.



Event Viewer provides the ability to view logs on any computer running Windows NT. Event Viewer on computers running Windows NT Workstation is identical to Event Viewer on computers running Windows NT Server.

Administrative Requirements for Viewing the Security Log

The security log resides on the computer where the Audit policy was set. To view a security log, you must be a member of the Administrators or Server Operators groups on the computer where the security log resides.

For example, if the Audit policy was set on a computer running Windows NT Workstation or on a member server, you must have administrative privileges on that computer. If the Audit policy was set on the primary domain controller (PDC), you must have administrative privileges on the PDC.

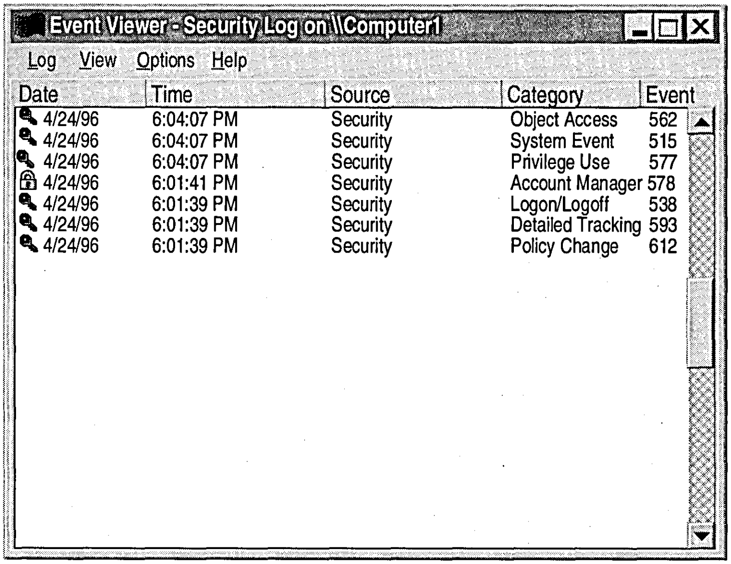
Note To view a security log on a computer in a different domain, the appropriate trust relationship must exist.

Viewing the Security Log

The security log is where audited events are recorded. Successful events appear with a key icon; unsuccessful events appear with a lock icon. Other key information includes the date and time that the event occurred, and the category of the event. The **Category** indicates the type of event that was audited (set in the Audit policy).

The following table lists the Event Viewer categories and specifies which type of event in the Audit policy each category corresponds to.

This Event Viewer category	Corresponds to this type of event
Object Access	File and Object Access
System Event	Restart, Shutdown, and System
Privilege Use	Use of User Rights
Account Management	User and Group Management
Logon/Logoff	Logon and Logoff
Detailed Tracking	Process Tracking
Policy Change	Security Policy Changes



Date	Time	Source	Category	Event
4/24/96	6:04:07 PM	Security	Object Access	562
4/24/96	6:04:07 PM	Security	System Event	515
4/24/96	6:04:07 PM	Security	Privilege Use	577
4/24/96	6:01:41 PM	Security	Account Manager	578
4/24/96	6:01:39 PM	Security	Logon/Logoff	538
4/24/96	6:01:39 PM	Security	Detailed Tracking	593
4/24/96	6:01:39 PM	Security	Policy Change	612

▸ To create log file entries in the security log

In this procedure, you perform tasks that create entries in the security log to see the effects of your Audit policy.

1. Log on as User9.
2. In Windows NT Explorer, expand the LabFiles\Public\Library folder, and then double-click Bronte.txt to open it.
3. Close the file.
4. Log off and then log on as Administrator.
5. Create a user account.
6. Shut down and restart your computer.

To view the security log on the local computer

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer.**

   If this is the first time that you started Event Viewer, the system log for your computer appears. Otherwise, the last log that you viewed appears.
3. On the **Log** menu, click **Security** (if it does not already appear).
4. Scroll through the log and look for the following categories of events.
   - **Logon/Logoff**
   - **Object Access**
   - **Privilege Use**
   - **Account Management**
5. Double-click the different events for a description of them, or select the event and then on the **View** menu, click **Detail.**

To view the security log on a remote computer

If you have two computers, log on as Administrator on the secondary computer and complete this procedure.

Note If your computers are connected to each other by a modem (using connections slower than 28.8), on the **Options** menu click **Low Speed Connection**, or on the **Log** menu, click **Select Computer**, and then click to select the **Low Speed Connection** check box. If this option is selected, Windows NT does not list all the computers in the default domain, thereby minimizing network traffic across the link.

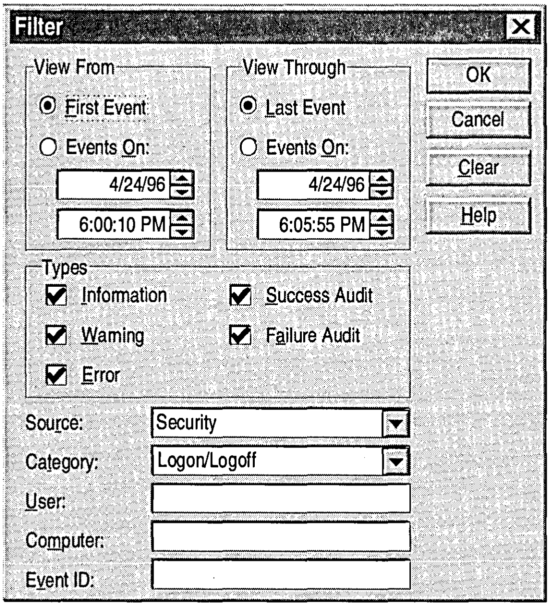
1. On the **Log** menu, click **Select Computer**.

   The **Select Computer** dialog box appears.
2. In the **Computer** box, type the name of the remote computer, or double-click the domain and select the computer from the list.

Filtering Events

By default, Event Viewer lists all events recorded in the selected log. To view a subset of events that have specific characteristics, click **Filter Events** on the **View** menu. When filtering is on, a check mark appears by the **Filter Events** command on the **View** menu and "(Filtered)" appears on the Event Viewer title bar. If **Save Settings On Exit** on the **Options** menu is turned on (you see a check mark next to it), when you quit Event Viewer, the filter remains in effect the next time you start Event Viewer.

Filtering has no effect on the actual content of the log; it changes only the view. All events are logged continuously, whether the filter is active or not.



View From
● First Event
○ Events On: 4/24/96 6:00:10 PM

View Through
● Last Event
○ Events On: 4/24/96 6:05:55 PM

Types
☑ Information ☑ Success Audit
☑ Warning ☑ Failure Audit
☑ Error

Source: Security
Category: Logon/Logoff
User:
Computer:
Event ID:

The following table describes how to use the options in the **Filter** dialog box.

Use this option	To
View From/ View Through	Specify the range of dates for which you want to view events.
Types	Select the types of events that you want to view.
Source	Specify the software or component driver that generated the event.
Category	Select the classification of the event as defined by the source; for example, a security log category is Logon/ Logoff.
User	Specify a user account to locate events resulting from a specific user.
Computer	Specify a computer name to locate events resulting from a specific computer.
Event ID	Look at an event number to identify the event. This number helps product support representatives to track events.

▸ To filter for Logon/Logoff events

1. In Event Viewer, on the **Log** menu, click **Open**.

   The **Open** dialog box appears.

2. In the LabFiles folder, double-click Security.evt.

   The **Open File Type** dialog box appears. The **System** file type is selected by default.

3. Under **Open File of Type**, click **Security**, and then click **OK**.

   The security event log for Security.evt appears.

4. On the **View** menu, click **Filter Events**.

   The **Filter** dialog box appears.

5. In the **Source** box, click **Security**.

6. In the **Category** box, click **Logon/Logoff**, and then click **OK**.

   Notice that the lock icon appears next to each event indicating that the event failed.

7. Double-click each event for a description.

   Under **Description**, notice the reason that the event failed and the user who caused it to fail, possibly attempting to breach security.

▸ **To filter for unauthorized access to folders and files**

1. On the **View** menu, click **Filter Events**.

   The **Filter** dialog box appears.
2. In the **Source** box, click **Security**.
3. In the **Category** box, click **Object Access**.
4. Under **Types**, make sure that only the **Failure Audit** check box is selected (click to clear all of the other check boxes).
5. Click **OK**.
6. Double-click each event to see a description.

   On what file did the failed event occur?

   ____

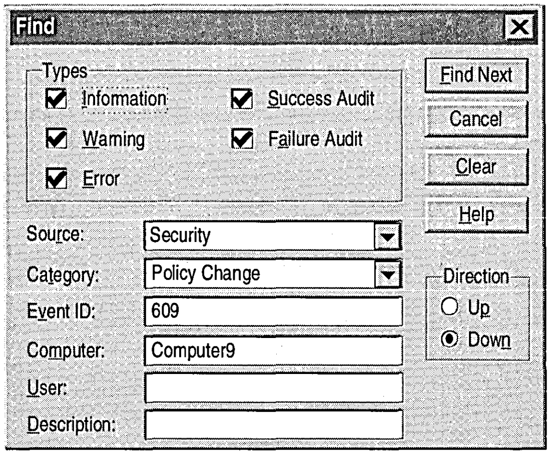
   What action was attempted on the file? (Scroll through the **Description** and look at **Accesses**.)

   ____

Locating Events

To search for events that match a specific type, source, or category, click **Find** on the **View** menu. Searches can be useful when you are viewing large logs. For example, you can search for all Warning events related to a specific program, or you can search for all Error events from all sources.

Unlike the **Filter Events** command, the **Find** command does not enable you to search for events based on dates. You can, however, search on text that would appear in the description of the event.



Find

Types
☑ Information ☑ Success Audit
☑ Warning ☑ Failure Audit
☑ Error

Source: Security
Category: Policy Change
Event ID: 609
Computer: Computer9
User:
Description:

Direction
○ Up
● Down

- **To search for printer usage events**

1. On the **View** menu, click **All Events.**
2. On the **View** menu, click **Find.**

   The **Find** dialog box appears.
3. In the **Description** box, type **printer** and then click **Find Next.**

   The first printer event is highlighted.
4. On the **View** menu, click **Detail.**

   Under **Description**, notice that the action the user performed was to print the file.
5. Click **Close.**

- **To search for server hardware events**

1. On the **View** menu, click **Find.**

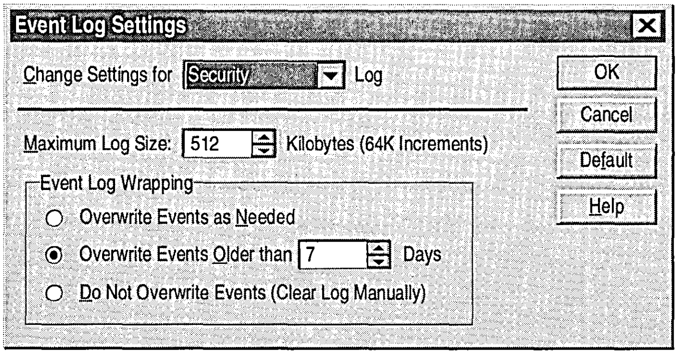
   The **Find** dialog box appears.
2. Click **Clear** to reset the **Find** dialog box options.
3. In the **Description** box, type **shutdown** and then click **Find Next.**

   The first shutdown event is highlighted.
4. On the **View** menu, click **Detail.**

   Notice the last time that the computer was shut down.
5. Click **Close.**

Archiving the Security Log

You can track trends in your system by archiving event logs. Viewing trends helps you to determine resource use and to plan for growth. You can also determine a pattern if unauthorized use of resources is a problem.



Event Log Settings

Change Settings for Security Log

Maximum Log Size: 512 Kilobytes (64K Increments)

Event Log Wrapping

○ Overwrite Events as Needed

● Overwrite Events Older than 7 Days

○ Do Not Overwrite Events (Clear Log Manually)

When you select events to audit, you need to keep in mind that the log can become full, which makes it unable to record any more events; however, you can avoid this problem. In the **Event Log Settings** dialog box, you can control:

- The size of the logs that you choose to archive:
  - Logs can be from 64 kilobytes (KB) to 4,194,240 KB.
  - The default is 512 KB.
- How events are recorded, by selecting any of the following options:
  - **Overwrite Events as Needed.**
  - **Overwrite Events Older than *x* Days**, and then entering the number of days.
  - **Do Not Overwrite Events (Clear Log Manually).**
  - If you select **Do Not Overwrite Events**, you may need to archive the information in the current log before you clear it.

▸ To control the size and content of a log file

1. On the **Log** menu, click **Log Settings.**

   The **Event Log Settings** dialog box appears.

2. Click **Overwrite Events as Needed.**

   Older events will now be overwritten by new events. Note that because some events repeat at frequent intervals, use of this option may result in important events being overwritten.

3. Click **OK** when finished.

▸ To archive the security log

1. On the **Log** menu, make sure that the **Security** command is turned on (that it has a check mark by it), and then click **Save As.**
2. Save the log in the LabFiles folder using a name that easily identifies the file.

Tip If you archive security logs, include the date as part of the file name to help you locate the file quickly.

▸ **To clear the security log**

1. On the **Log** menu, click **Clear All Events.**

   A message appears, asking you if you want to save the event log before closing it.

2. Click **No.**

   Another message appears, warning that this is an irreversible action and requesting verification.

3. Click **Yes.**

   Notice that a system event appears in the security log.

4. Double-click the event to see the description.

   Notice that the description states that the audit log was cleared.

5. Click **Close.**

▸ **To view an archived security log**

1. On the **Log** menu, click **Open.**
2. In the **Open** dialog box, locate and double-click the log that you archived.

   The **Open File Type** dialog box appears.

3. Under **Open File of Type**, click **Security**, and then click **OK.**
4. Quit Event Viewer and log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- Event Viewer is the administrative tool that is used to view a security log on any computer running Windows NT.
- The security log is where Event Viewer records the success or failure (whichever of these you are auditing) of each audited event.
- To view a security log, you must be a member of the Administrators or Server Operators group on the computer where the security log resides. If the computer is in a different domain, the appropriate trust relationship must exist between the domains.
- Use the **Filter Events** menu command to set which events and characteristics appear in the security log when you start Event Viewer.
- Use the **Find** menu command to locate.events in the security log.
- Archive security logs to track trends. This is useful in determining resource use and in planning for growth.

For more information on	See
How to use Event Viewer	Event Viewer Help.
	Chapter 9, "Monitoring Events," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 37, "Monitoring Events," in the *Microsoft Windows NT Workstation Resource Kit.*
Trust relationships	Chapter 1, "Managing Windows NT Server Domains," in Microsoft Windows NT Server *Concepts and Planning*.
Administrative privileges	Chapter 3, "Setting Up Group Accounts," in this book.
	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
Interpreting events	Chapter 9, "Monitoring Events," in Microsoft Windows NT Server *Concepts and Planning*.
	Chapter 37, "Monitoring Events," in the *Microsoft Windows NT Workstation Resource Kit.*

Best Practices

The following checklist provides best practices for auditing resources and events. Use this checklist when planning and maintaining an Audit policy:

□ Define an Audit policy that is useful, but manageable. Audit only those events that will provide you with meaningful information about your network environment. This will minimize use of server resources and make key information easier to locate.

- In minimum-security networks, track successful events if you need to determine resource use. In medium-security networks, track successful events of key resources and of administrative and security policy changes. In high-security networks, track all successful events.
- In medium-security networks, track unsuccessful events to alert you to possible security breaches. In high-security networks, track all unsuccessful events.
- In all networks, audit sensitive and confidential data.

□ Audit the Everyone group instead of the Users group. This ensures that anyone who can connect to the network is audited, not just the users that you create accounts for in the domain.

□ Set up a schedule for viewing audit logs. Make it a regular part of your network administration tasks.

□ Archive audit logs regularly to track trends. Doing so is useful for determining resource use and for planning purposes.

Note If you want to remove the account that was created by running the Chapter9.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter9.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. On which computer would you have to set the Audit policy to audit domain logon attempts?

2. On which computer would you have to set the Audit policy to audit a folder located on a computer running Windows NT Workstation that is part of the domain?

3. Which of the following are true statements about setting up and administering auditing? (Circle all that apply.)

   a. Only members of the Administrators group can set up auditing.

   b. Only members of the Administrators and Server Operators groups can set up auditing.

   c. Users with the user right *Manage auditing and security log* can set up and administer auditing.

   d. Only members of the Administrators and Server Operator groups can administer auditing once it is set up.

   e. Only members of the Server Operators group can administer auditing once it is set up.

4. What event must be set in the **Audit Policy** dialog box before you can audit files, folders, and printers?

   ____

   ____

5. Complete this sentence. Folders and files can be audited on ____________ volumes only.

6. In which event log are audited events recorded?

   a. System log

   b. Security log

   c. Application log

   d. Error log

Answer Key

Procedure Answers

Page 338

▶ **To plan an Audit policy**

Suggested answers:

Logon and Logoff: Failure (for attempts to gain access to the network).

File and Object Access: Success (for printer use) and Failure (for unauthorized access to the database).

Use of User Rights: Success (for Administrator actions and backup procedures).

User and Group Management: Success (for Administrator actions).

Security Policy Changes: Success (for Administrator actions).

Restart, Shutdown, and System: Success and Failure (for attempts to breach the server).

Process Tracking: Success.

Page 352

▶ **To filter for unauthorized access to folders and files**

6. On what file did the failed event occur?

   Wuthering Heights.txt.

   What action was attempted on the file? (Scroll through the **Description** and look at **Accesses**.)

   The Administrator attempted to delete the file.

Page 358

Review Answers

1. On which computer would you have to set the Audit policy to audit domain logon attempts?

   The Audit policy must be set on the primary domain controller.

2. On which computer would you have to set the Audit policy to audit a folder located on a computer running Windows NT Workstation that is part of the domain?

   The Audit policy must be set on the computer where the file is located—in this situation, on the computer running Windows NT Workstation.

3. Which of the following are true statements about setting up and administering auditing? (Circle all that apply.)

   Answers a, c, and d are true.

4. What event must be set in the **Audit Policy** dialog box before you can audit files, folders, and printers?

   File and Object Access.

5. Complete this sentence. Folders and files can be audited on ____________ volumes only.

   "NTFS" is the correct answer.

6. In which event log are audited events recorded?

   Answer b is correct.

CHAPTER 10

Monitoring Resources

About This Chapter

This chapter provides an overview of Server Manager and Windows NT Diagnostics and shows you how to use them to obtain key information about network and computer resources.

The hands-on procedures guide you through viewing computer properties; viewing user sessions, shared resources, and resources in use; setting administrative alerts; sending messages to users; and gathering information about a computer configuration to use for inventory tracking and troubleshooting.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- Knowledge about the Administrators, Server Operators, and Power Users groups and the skills to add user accounts to them.
- Knowledge about shared resources, and about share and NTFS permissions.
- Shared the LabFiles\Public folder as Public. If the Public folder is not shared, see Chapter 5, "Securing Network Resources with Share Permissions" for instructions. Or, click the **Start** button, and then click **Run**. Then, in the **Open** box, type **net share public=***drive***:\LabFiles\Public** and click **OK**.
- A user account named User10. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter10.cmd to create it.

Lesson 1: Introduction to Monitoring Resources

You use Server Manager to assess server usage. You use Windows NT Diagnostics to obtain configuration information about a computer. This lesson describes the information provided by each and the requirements for using them.

After this lesson, you will be able to:

- Describe the function of Server Manager.
- Describe the function of Windows NT Diagnostics.
- Name the built-in group accounts that have the administrative user rights required for gaining access to Server Manager.

Estimated lesson time: 20 minutes

Server Manager

Server Manager is a Windows NT Server tool that you use to assess resource usage on computers running Windows NT. With Server Manager, you can view a list of connected users, view shared and open resources, manage a list of administrative alert recipients, manage services and shared folders, and send messages to connected users.

Note You can install Server Manager on any computer running Windows NT Workstation or Windows 95 by installing the client-based administration tools located in the Clients\Srvtools folder on the Windows NT Server compact disc.

Windows NT Diagnostics

Windows NT Diagnostics (Winmsd.exe) is a Windows NT Workstation and Windows NT Server diagnostic tool that you use to view and print configuration information for a local or remote computer. With Windows NT Diagnostics, you can view the following:

- Operating system information, such as the version number, system boot options, services, system settings, and user environment variables
- Hardware details, such as BIOS information, video resolution, CPU type, and CPU settings
- Physical memory, paging file information, and DMA (Direct Memory Access) usage
- The current state of each driver and service on the computer

- Drives and devices installed on the computer, plus related interrupt request line (IRQ) and port information
- Network information, including transports, configuration settings, and statistics
- Printer settings, fonts settings, and system processes that are running

Requirements

The following list describes the requirements for using Windows NT Diagnostics and Server Manager:

- To use Windows NT Diagnostics, you can be logged on as any user. Because Windows NT Diagnostics does not allow you to make configuration changes, all users can use it. However, a few of the settings are only available to members of the Administrators, Server Operators, and Power Users groups.
- To use Server Manager, you must be a member of the Administrators, Server Operators, or Power Users group on the computer that you are monitoring.

  If you are a member of the Server Operators group on a domain controller, you will have Server Operator privileges on all domain controllers in the domain.

  A few Server Manager functions are accessible only by members of the Administrators group. When Server Operators, Account Operators, or Power Users attempt to perform these functions, a message appears indicating that access is denied.

▸ To add a user to the Server Operators group

In this procedure, you give a user the necessary rights to administer the server by adding his or her account to the Server Operators group.

1. Log on as Administrator.
2. In User Manager for Domains, add User10 to the Server Operators group.

▸ To determine the built-in rights that are assigned to Server Operators

1. In the User Manager for Domains window, on the **Policies** menu, click **User Rights.**
2. In the **Right** box, click each item in the list to determine which rights are automatically assigned to the Server Operators group (that is, which rights cause **Server Operators** to appear in the **Grant To** box). In the following list, mark the check box next to each right that is granted automatically to the Server Operators group:

   □ **Access this computer from network**

   □ **Add workstations to domain**

   □ **Back up files and directories**

   □ **Change the system time**

   □ **Force shutdown from a remote system**

   □ **Load and unload device drivers**

   □ **Log on locally**

   □ **Manage auditing and security log**

   □ **Restore files and directories**

   □ **Shut down the system**

   □ **Take ownership of files or other objects**
3. Quit User Manager for Domains and log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- Server Manager is a Windows NT Server tool that enables you to assess server usage.
- Windows NT Diagnostics (Winmsd.exe) is a Windows NT Workstation and Windows NT Server diagnostic tool that enables all users to view and print configuration information for a local or remote computer.
- To use Server Manager, you must be a member of the Administrators, Server Operators, or Power Users group on the computer that you are monitoring.

For more information on	See
Installing client-based administration tools	Chapter 11, "Managing Client Administration," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 2: Viewing Computer Properties

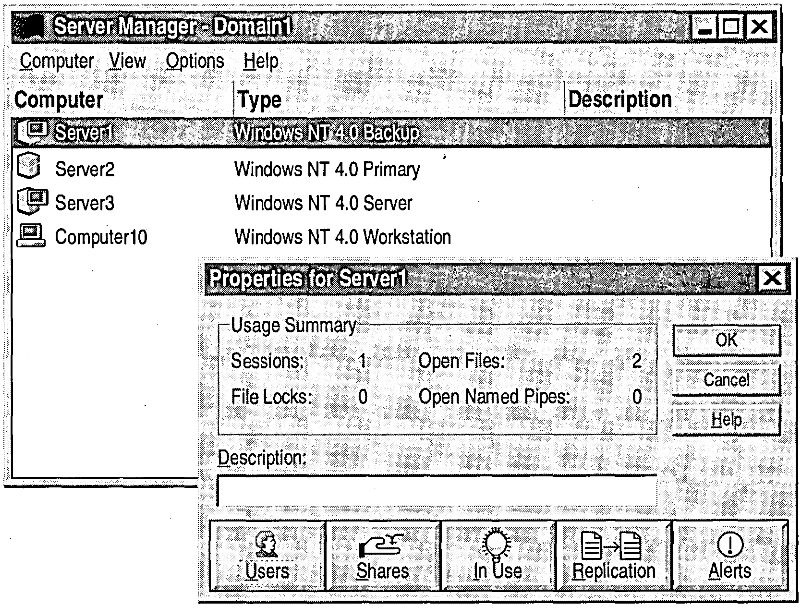
The computer properties that you can view in Server Manager show you information about system resources. This information is useful in determining how many users are connected to the computer and how many shared resources are in use. This lesson guides you through the steps to view the properties on a local or remote computer.

After this lesson, you will be able to:

- Use Server Manager to view server usage.
- Use Server Manager to view server properties.

Estimated lesson time: 20 minutes

Computer properties are viewed using Server Manager.



Computer	Type	Description
Server1	Windows NT 4.0 Backup	
Server2	Windows NT 4.0 Primary	
Server3	Windows NT 4.0 Server	
Computer10	Windows NT 4.0 Workstation	

Usage Summary

Sessions: 1 Open Files: 2

File Locks: 0 Open Named Pipes: 0

Description:

To start Server Manager

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Server Manager**.

   The following information appears in the Server Manager window for the current domain:

   - The computer name, and the operating system and version it is running. (If the computer is inactive, the operating system is displayed without the version.)
   - An icon indicating whether the computer is a primary domain controller, a backup domain controller or member server, or a computer running Windows NT Workstation or another client.

     In the previous illustration, the icon for Server1 and Server3 indicates a backup domain controller or a member server. The icon for Server2 indicates a primary domain controller. The icon for Computer10 indicates a computer running Windows NT Workstation or another client.
   - If a computer is not running, the icon for the computer appears dimmed.
   - A description (configured during installation).

Note To view computers in another domain, on the **Computer** menu, click **Select Domain,** type the domain name, and then click **OK**. To view all computers in the domain that are running Windows NT, view just the servers, or view just the workstations, click the appropriate option on the **View** menu.

To view computer properties

- In the Server Manager window, double-click the name of your computer to view its properties.

  –or–

  Click the computer name, and then on the **Computer** menu, click **Properties**.

  The **Properties for** *computer_name* dialog box appears.

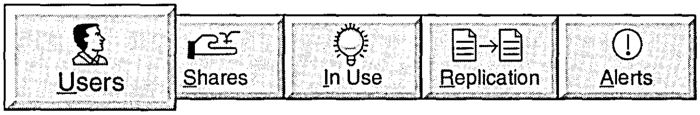
  The following table describes the information for the selected computer.

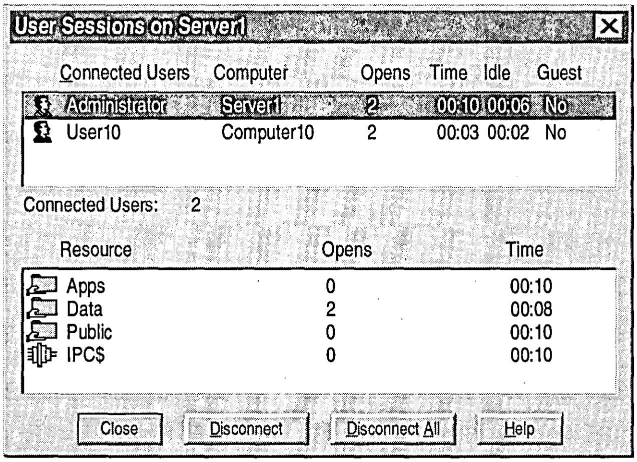
Item	Description
Sessions	The number of users remotely connected to the computer.
Open Files	The number of shared resources opened on the computer.
File Locks	The number of file locks by users on the computer.
Open Named Pipes	The number of named pipes opened on the computer.

Viewing User Sessions

The **Users** button provides information on user sessions. User session information is useful in determining which users you need to contact when you have to shut down the server, and which users you need to contact when another user is trying to access a file that is already in use. Using the **Users** button, you can:

- View users connected to the computer, and view the shared folders that they are connected to.
- View the files opened by each user.
- Disconnect users from the computer to:
    - Force the user to reconnect to a shared folder, so that changes made to a user's group membership for the resource take effect. Windows NT checks a user's group membership when the user connects to a resource. If the user's permissions for the resource change as a result of becoming a member of a new group, those permissions will not take effect until the next time the user connects to the resource.
    - Free idle connections on a computer running Windows NT Workstation. Windows NT Workstation allows only 10 incoming network connections.
    - Shut down a server.





Connected Users	Computer	Opens	Time	Idle	Guest
Administrator	Server1	2	00:10	00:06	No
User10	Computer10	2	00:03	00:02	No

Connected Users: 2

Resource	Opens	Time
Apps	0	00:10
Data	2	00:08
Public	0	00:10
IPC$	0	00:10

When you select a user under **Connected Users**, the shared resources to which the user is connected appear under **Resource**, including the name of the resource, the number of files that the user has open, and the time that has elapsed since the resource was first opened.

The following table describes the information under **Connected Users** at the top of the dialog box.

Item	Description
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 that the user has open 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.

▸ To view user sessions

In this procedure, you view user sessions for your user account. You create a session by connecting to your own computer.

1. In the **Properties for** *computer_name* dialog box, click **Users**.

   The **User Sessions on** *computer_name* dialog box appears.
2. Click the **Start** button, and then click **Run**.
3. In the **Open** box, type \\computer_name\users (where *computer_name* is the name of your computer), and then click **OK**.

   A window that shows the contents of the Users shared folder appears.
4. Switch to Server Manager.
5. Update the contents of the **User Sessions on** *computer_name* dialog box by closing the dialog box and then opening it.
6. Under **Connected Users**, click the user account that you logged on with (if it is not already selected).

   Under **Resource**, notice the connections that have been established to your server. The Users folder appears as a connection.

▸ To disconnect users from shared resources

In this procedure, you disconnect a user who has connected to a shared resource.

1. In the **User Sessions on** *computer_name* dialog box, make sure your user account is selected, and then click **Disconnect**.

   A message appears, prompting you to confirm the operation.
2. Click **Yes** to disconnect the user from the Users folder.

   Notice that all entries for your user account were removed.

Note If you wanted to disconnect all users, you would click **Disconnect All**.

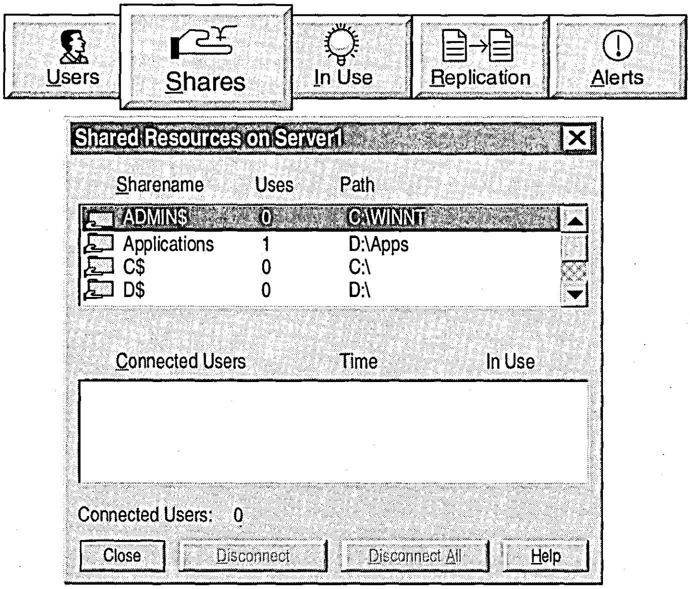
3. Click **Close** to return to the **Properties for** *computer_name* dialog box.
4. Click **OK** to return to the Server Manager window.
5. Quit Server Manager and log off.

Caution Always notify users before you disconnect them or shut down the server so that you give them an opportunity to save their files; otherwise, they may lose data.

Monitoring Shared Resources

The **Shares** button provides a list of shared resources on the computer and the users that are connected to each resource. Use this button to:

- Determine if the maximum number of users that are permitted to gain access to a particular resource has been reached. This may be one reason why a user cannot connect to a shared resource.
- Disconnect users. If users turned off their computers without either logging off or disconnecting from the network resource, their connection may still be active.



Sharename	Uses	Path
ADMIN$	0	C:\WINNT
Applications	1	D:\Apps
C$	0	C:\
D$	0	D:\

Connected Users	Time	In Use

Connected Users: 0

The following table describes the information in the dialog box options.

Item	Description
Sharename	The name of the shared resource. This can be a shared folder, a printer, or a named pipe.
Uses	The number of connections to the shared resource.
Path	The path of the shared resource.
Connected Users	The names of the users connected to the selected shared resource.
Time	The time that has elapsed since the user first connected to this resource.
In Use	Whether the user currently has any files open from this shared resource.

▸ To connect to a shared resource

In this procedure, you connect to your own computer. This procedure mimics what occurs when another user connects to your computer.

1. Log on as User10 (or as Administrator, if you did not complete Lesson 1).
2. Right-click Network Neighborhood or My Computer, and then click **Map Network Drive.**

   The **Map Network Drive** dialog box appears.
3. In the **Drive** box, click **P**, and in the **Path** box type \\*computer_name***public** and then click **OK**.

   A *drive* window appears for the Public shared folder.
4. Minimize, but do not close, the window.

▸ To view a list of resources shared by computers

In this procedure, you use Server Manager to view resources shared by other computers so that you can see which resources are currently in use on the computer.

1. Start Server Manager and double-click your computer name.
2. In the **Properties for** *computer_name* dialog box, click **Shares.**

   The **Shared Resources on** *computer_name* dialog box appears.
3. Under **Sharename**, click **Public.**

   Notice that your user account appears as a user connected to the Public shared folder. If other network users have connected to your Public shared folder, their user accounts will also appear here.

4. Under **Sharename**, click IPC$.

   Notice that your user account appears as a user connected to IPC$.

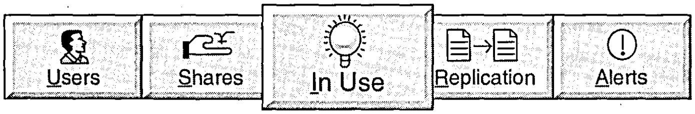
   IPC$ indicates that a resource is sharing the named pipes that are essential for communication between programs. IPC$ is used during remote administration of a computer, and when viewing a computer's shared resources.

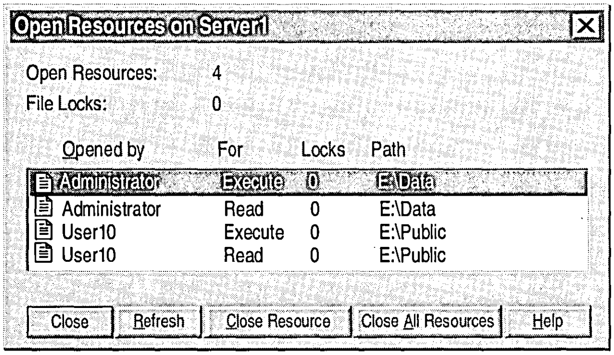
5. Click **Close** to return to the **Properties for** *computer_name* dialog box.

Monitoring Resources in Use

The **In Use** button provides a list of the users that are connected to a shared resource and the files that they have open. Use this button to:

- Determine if a file is in use. For example, if a user cannot access a specific file because another user has the file open, you can notify this user of the file that another user needs to access the file.
- Close a file. For example, if you make changes to NTFS permissions for a file, for those changes to be immediately effective, the file has to be closed and then reopened.




Open Resources on Server1

Open Resources: 4
File Locks: 0

Opened by	For	Locks	Path
Administrator	Execute	0	E:\Data
Administrator	Read	0	E:\Data
User10	Execute	0	E:\Public
User10	Read	0	E:\Public

The following table describes the information in the **Open Resources on** *computer_name* dialog box.

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.
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 view a list of open resources on the server

In this procedure, you open a resource and then use the **In Use** button to view it as being open.

1. Click the **Start** button, point to **Programs**, point to **Accessories**, and then click WordPad.
2. Open P:\Expenses.doc.
3. Minimize WordPad.
4. In the **Properties for** *computer_name* dialog box, click **In Use**.

   Notice the resources in use on your computer.
5. Click the **Start** button, and then click **Run**.
6. In the **Open** box, type **\\***computer_name***\users** (where *computer_name* is your computer), and then click **OK**.

   A window that shows the contents of the Users shared folder appears.
7. Minimize the window for the Users shared folder.
8. In the **Open Resources on** *computer_name* dialog box, click **Refresh** to update the list of open resources. It does not update automatically.

   Notice that an additional open resource appears.

▸ To close a single resource

1. In the **Open Resources on** *computer_name* dialog box, click the Public folder, and then click **Close Resource**.

   A message appears, warning you that disconnecting users may cause loss of data.

2. Click **Yes**.

   Notice that the entry was removed.

   Note To close all resources, you would click **Close All Resources.**

3. Close all windows, quit Server Manager, and then log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- The computer properties that you can view in Server Manager show you information about system resources.
- The **Users** button provides information on user sessions.
- The **Shares** button provides a list of shared resources on the computer and the users that are connected to each resource.
- The **In Use** button provides a list of the users that are connected to a shared resource and the files that they have open.

For more information on	See
Viewing resources in use	Server Manager Help.
Viewing shared resources	Server Manager Help.
Server Manager	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 3: Setting Alerts and Sending Messages

You can set administrative alerts so that Windows NT notifies administrators that operating system problems exist. You can notify users that a server event will occur by sending a Windows NT message. This lesson guides you through the steps to set administrative alerts and to send messages to users.

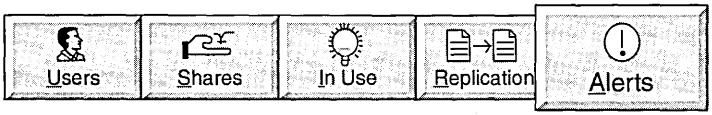
After this lesson, you will be able to:

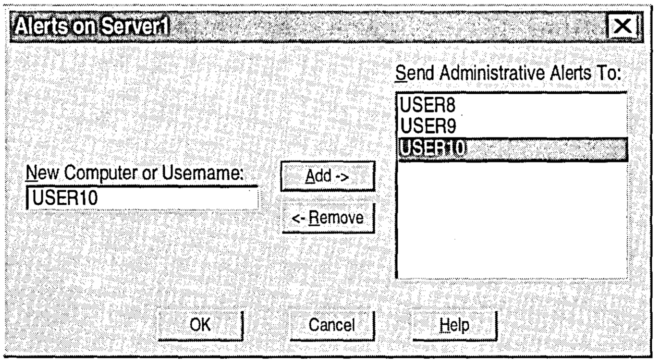
- Set administrative alerts.
- Send messages to users to notify them of disruptions in service.

Estimated lesson time: 20 minutes

Setting Administrative Alerts

The **Alerts** button allows you to create a list of users or computers that need to receive an alert when there are Windows NT operating system problems, such as security and access problems, user session problems, and printer problems. For example, you can notify the Administrators group when a computer is running low on disk space so that appropriate action can be taken.




Alerts on Server1

Send Administrative Alerts To:
USER8
USER9
USER10

New Computer or Username: USER10

Note Administrative alerts are generated *only* by the Windows NT Alerter service. They are not generated by programs, such as Microsoft Word.

▸ To set an administrative alert

1. Log on as Administrator.
2. Start Server Manager, and then double-click your computer name.
3. In the **Properties for** *computer_name* dialog box, click **Alerts**.

   The **Alerts on** *computer_name* dialog box appears.
4. In the **New Computer or Username** box, type **user10** and then click **Add**.

   User10 appears under **Send Administrative Alerts To**.
5. Click **OK** twice to apply your changes and to return to the Server Manager window.

   When an operating system problem occurs, an alert will be sent to User10.

Sending Messages to Users

Always send messages to all users connected to a particular computer when there will be a disruption to the server or the resource availability. This gives users an opportunity to save their files.

Send messages to users before:

- Performing a backup or restore operation on a user's files.
- Disconnecting users from a resource.
- Shutting down the server.

Note The Messenger service must be running to send messages. It is started by default. Computers running Windows 95 must be running WinPopUp.exe to receive messages.

▸ To send a message to all users connected to your computer

1. In the Server Manager window, make sure that your computer is selected.
2. On the **Computer** menu, click **Send Message**.

   The **Send Message** dialog box appears.
3. Under **Message**, type a message notifying users to save and close their files because they will be disconnected within the next few minutes.
4. Click **OK** to send the message.

   The message is sent to all users who are currently connected to your computer and have started the Messenger service. Because you have opened a shared resource on your server, your own computer will also receive the message. Notice that the message includes the name of the computer from which the message was sent, as well as the date and time.
5. Click **OK** to close the message.
6. Quit Server Manager, and then log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- By setting administrative alerts, you can notify administrators when operating system problems occur.
- When there will be a disruption to the server or the resource availability, always send a message to all users connected to a particular computer.

For more information on	**See**
Managing administrative alerts	Server Manager Help.
Starting and stopping services	Server Manager Help.
Configuring service startup	Server Manager Help.
Administrative alerts	Chapter 4, "Managing Shared Resources and Resource Security," in Microsoft Windows NT Server *Concepts and Planning*.
Windows NT services	Windows NT Help.

Lesson 4: Using Windows NT Diagnostics

It is recommended that you have a log book for every computer that contains information about the computer's configuration. Having current information makes it easier to rebuild a computer in the event of a serious system failure. This information also helps product support personnel to troubleshoot problems.

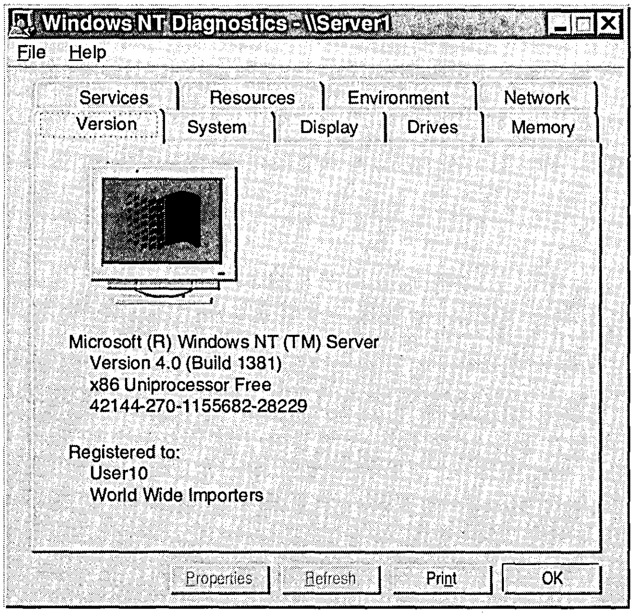
This lesson describes the Windows NT Diagnostics options and guides you through the steps to gather information about a computer's configuration. The lesson also covers how to save and print a report for your log book.

After this lesson, you will be able to:

- Describe the Windows NT Diagnostics options.
- View system configuration information.
- Save or print a report.

Estimated lesson time: 20 minutes

Windows NT Diagnostics is a useful tool for gathering information about a computer's hardware and software configuration and for printing a report containing this information.



Microsoft (R) Windows NT (TM) Server
Version 4.0 (Build 1381)
x86 Uniprocessor Free
42144-270-1155682-28229

Registered to:
User10
World Wide Importers

The following table describes the types of information that you can view in Windows NT Diagnostics.

Tab	Description
Version	Operating system information, including version numbers, build and service pack information, and the identity of the registered owner.
System	ROM BIOS and CPU information, including the CPU type and the number of CPUs in the computer.
Display	Information about the video driver and adapter.
Drives	Available drives and their types, including removable (floppy or optical), non-removable (hard disk), and remote (network connections).
Memory	Information about physical and virtual memory. Specifics about the paging file (Pagefile.sys), total memory, available memory, and a memory load index are displayed.
Services	Services listed in the **CurrentControlSet**, along with the state of the service, either running or stopped.
Resources	Active devices and details about each resource, including direct memory access (DMA), interrupt request line (IRQ) status, memory, and port information.
	Information about IRQ interrupts within the computer and which device has locked a particular interrupt for use.
	Information about DMA channels that are used by devices or drivers.
Environment	Environment variables, such as the path command (which is the same information you see when you type **set** at a command prompt).
Network	Network-related configuration information, including current network statistics.

Note If you view information on a remote computer, the **Drives** and **Memory** tabs do not appear.

Gathering Information

When you call Microsoft Technical Support, the support engineer will ask you a number of questions about the computer for which you are requesting support. You will be asked to provide information about the computer's hardware and software configuration and settings.

Having the answers to these questions ready will speed up the process of creating a customer record and if needed, escalating your call to the secondary response group.

► To gather information about your computer

In this procedure, you locate the configuration information for your computer that is typically requested when you call Microsoft Technical Support.

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Windows NT Diagnostics**.
3. Locate the information in the following table by performing the steps under **Do this**.

For this information	Do this
Version of Windows NT installed	Click the **Version** tab.
Computer BIOS (*x*86-based computers) or firmware revision level (RISC-based computers)	Click the **System** tab, and then look under **BIOS Information**.
Processor and HAL type	Click the **System** tab, and then look at **HAL** and **Processor(s)**.
File systems in use	Click the **Drives** tab, expand Local Hard Drives, double-click a drive, and then click the **File System** tab.
Total memory (RAM)	Click the **Memory** tab, and then look under **Physical Memory**.
Services installed	Click the **Services** tab, and then look under **Service**.
Hardware IRQs, I/O ports, DMA addresses, and similar information	Click the **Resources** tab. For IRQs, click the **IRQ** button. For the I\O ports, click the **I\O Port** button. For DMA addresses, click the **DMA** button.
Folder where Windows NT is installed	Click the **Environment** tab, and then look at **windir**.

(continued)

For this information	Do this
Name of the domain that you are currently logged into	Click the **Network** tab, and then look at **Logon Domain.**
Name of the domain controller that validated your user account	Click the **Network** tab, and then look at **Logon Server**.
Name of the workgroup or domain that your computer is a member of	Click the **Network** tab, and then look at **Workgroup or Domain**.
Protocols installed	Click the **Network** tab, click the **Transports** button, and then look under **Transport**.

Creating and Printing a Report

In addition to providing a support organization with key information about a computer, a Windows NT Diagnostics report is valuable for inventory and record keeping purposes. It can help you keep track of the RAM, hard disks, and devices installed on each computer.

The following table describes the available print options.

Click an option under	To
Scope	Either print the information on the current tab or on all tabs.
Detail Level	Either print a summary or a complete report.
Destination	Either print the information to a file, to the Clipboard, or to the default printer.

▸ To print or save a report

1. On the Windows NT Diagnostics **File** menu, click **Print Report**.

Note To view and print the diagnostics for another computer, on the **File** menu, click **Select Computer**, and then type of the name of the computer. Note, however, that the printout does not necessarily contain the same data as the onscreen report.

The **Create Report** dialog box appears.

2. Under **Scope**, click **All tabs** to include the information provided on all tabs in the saved report.
3. Under **Detail Level**, click **Complete**.

4. If your computer is connected to a printer, under **Destination**, click **Default Printer**, and then click **OK**.

   –or–

   If your computer is not connected to a printer, under **Destination**, click **File**, and then click **OK**. In the **Save in** box, click **C**, and accept the default file name **msdrpt** by clicking **Save**.

   A Generating WinMSD Report message appears.

5. Retrieve the printed report, or start Notepad and open C:\MsdRpt.txt.

   Compare the information in the report to the information displayed in Windows NT Diagnostics.

6. Close C:\MsdRpt.txt when you are done.
7. Quit Windows NT Diagnostics, and then log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- For every computer, create a log book that contains information about the computer's configuration.
- Having current information makes it easier to rebuild a computer in the event of a serious system failure. This information also helps product support personnel to troubleshoot problems.
- Windows NT Diagnostics helps you to gather information about a computer's hardware and software configuration, and to create and print a report for your log book.

For more information on	**See**
Using Windows NT Diagnostics for system diagnosis	Chapter 7, "Protecting Data," in Microsoft Windows NT Server *Concepts and Planning*.
Using Windows NT Diagnostics to view system configuration data	Chapter 7, "Protecting Data," in Microsoft Windows NT Server *Concepts and Planning*.
Using Windows NT Diagnostics for troubleshooting	Chapter 8, "General Troubleshooting," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit*.
Keeping a log book	Chapter 20, "Preparing for and Performing Recovery," in the *Microsoft Windows NT Workstation Resource Kit*.

Best Practices

The following checklist provides best practices for monitoring network resources. Review this checklist before you monitor network resources:

- □ Install the client-based administration tools (available on the Clients\Srvtools folder on the Windows NT Server compact disc) on a computer running Windows NT Workstation or Windows 95. This allows you to administer any computer running Windows NT Server from the client.
- □ To give users an opportunity to save their files, always notify them before disconnecting them from the server or shutting it down.
- □ Set administrative alerts so that they are sent to the computers of users who are responsible for maintaining the server.
- □ For every computer, maintain a log book that contains information about the computer's configuration. Having this information makes it easier to rebuild a computer in the event of a serious system failure. This information also helps product support personnel to troubleshoot problems.

Note If you want to remove the account that was created by running the Chapter10.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter10.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. Scenario: You want to give a user the ability to monitor resource usage on Server1 and Server2 (in the same domain), but you do not want the user to have full administrative capabilities on either server. Server1 is the primary domain controller (PDC) and Server2 is the backup domain controller (BDC). To which group would you add the user, and on which computer or computers?

   ____

   ____

2. Which of the following tasks can you perform using Server Manager? (Circle all that apply.)
   a. View a list of connected users.
   b. View operating system information, such as the version number, services, system settings, and environment variables.
   c. View shared and open resources.
   d. View network-related information, such as the name of the domain, or the logon server.
   e. Set an administrative alert to notify an administrator of an operating system problem.
   f. Send a message to all users.

3. Scenario: So that User10 can update files in the Public shared folder, you have changed User10's permission for the Public folder from Read to Change by adding his user account to a group. User10 said that he tried adding a file to the Public folder, but was denied access. You checked the NTFS permission and determined that the Everyone group has the Full Control permission. What is the problem, and what Server Manager task can you perform to solve it?

   ____

   ____

4. What is the difference between the **Alerts** option and the **Send Message** command?

   ____

   ____

Answer Key

Procedure Answers

Page 367

▸ **To determine the built-in rights that are assigned to Server Operators**

2. In the **Right** box, click each item in the list to determine which rights are automatically assigned to the Server Operators group (that is, which rights cause **Server Operators** to appear in the **Grant To** box). In the following list, mark the check box next to each right that is granted automatically to the Server Operators group:

   The following check boxes should be marked: Back up files and directories, Change the system time, Force shutdown from a remote system, Log on locally, Restore files and directories, and Shut down the system.

Review Answers

Page 390

1. Scenario: You want to give a user the ability to monitor resource usage on Server1 and Server2 (in the same domain), but you do not want the user to have full administrative capabilities on either server. Server1 is the primary domain controller (PDC) and Server2 is the backup domain controller (BDC). To which group would you add the user, and on which computer or computers?

   Add the user to the Server Operators group on Server1. Because Server1 is a PDC, the user will have Server Operator privileges on all domain controllers in the domain.

2. Which of the following tasks can you perform using Server Manager? (Circle all that apply.)

   Answers a, c, e, and f are correct.

3. Scenario: So that User10 can update files in the Public shared folder, you have changed User10's permission for the Public folder from Read to Change by adding his user account to a group. User10 said that he tried adding a file to the Public folder, but was denied access. You checked the NTFS permission and determined that the Everyone group has the Full Control permission. What is the problem, and what Server Manager task can you perform to solve it?

   The problem is that User10 was connected to the Public folder when his permission for the folder was changed. Because Windows NT only checks a user's membership to a group when the user connects to a shared folder, the effective permission for User10 is still Read. In Server Manager, disconnect User10 from the Public folder. When User10 tries to gain access to the folder, he will automatically be reconnected.

4. What is the difference between the **Alerts** option and the **Send Message** command?

   The Alerts option only sends alerts from the Windows NT operating system to the users that have been added to the Send Administrative Alerts To box. The Send Message command gives you the ability to send a message to all users who are connected to the server.

CHAPTER 11

Backing Up and Restoring Files

About This Chapter

This chapter describes planning strategies for backing up and restoring files on your network and provides instruction on how to back up and restore files using the Windows NT Backup program. In the hands-on procedures, you use a Backup Simulation program to back up and restore files. This program simulates Windows NT Backup.

Before You Begin

To complete the lessons in this chapter, you must have:

- Completed the Setup procedures located in "About This Book."
- Knowledge and skills to create local and global groups and add user accounts to them.
- Knowledge and skills to assign user rights to accounts.
- Knowledge about the built-in Administrators, Server Operators, and Backup Operators groups.
- Knowledge about NTFS permissions.
- Two user accounts named User11-A and User11-B. Log on as Administrator. In Windows NT Explorer, expand the LabFiles folder, and then double-click Chapter11.cmd to create these accounts.

Lesson 1: Introduction to the Windows NT Backup Program

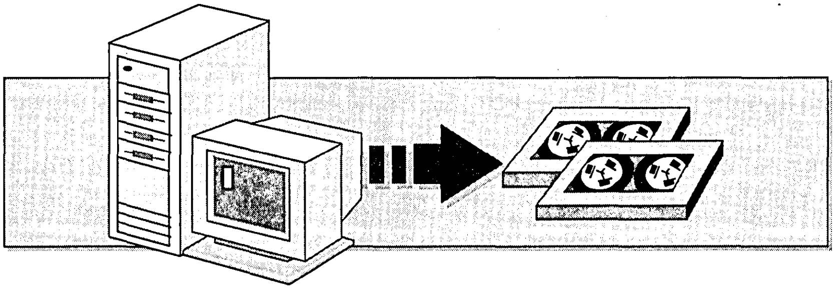
Regular backup of servers and local hard disks prevents data loss and damage caused by disk-drive failures, power outages, virus infections, and other potential disasters. Backup operations based on careful planning and reliable equipment make file recovery a relatively painless process. This lesson explains the underlying concepts of the Windows NT Backup program and the requirements that must be in place to use it.

After this lesson, you will be able to:

- Describe the requirements for backing up and restoring data.

Estimated lesson time: 10 minutes

The Windows NT Backup program is a graphical tool that you can use to back up and restore files to NTFS or FAT volumes, either manually or automatically.



Note Windows NT Backup only supports backing up to tape. To back up information to floppy disks or other non-tape media, use the **xcopy** or **backup** commands.

Requirements

The following requirements must be met to back up and restore files using the Windows NT Backup program:

- A computer running Windows NT Workstation or Windows NT Server with a tape drive that is supported on the hardware compatibility list (HCL).

  To back up the directory database (security and user account information) for the domain, the tape drive must be located on a domain controller.

- The user who performs the backup must have the appropriate user right on the computer where Windows NT Backup is running.
  - All users can back up any files and folders on the network for which they have the Read permission.
  - To back up all files and folders on a network, a user must have the *Back up files and directories* user right.
  - To restore all files and folders on a network, a user must have the *Restore files and directories* user right.
  - By default, the Backup Operators and Server Operators groups have both the Back up files and directories user right and the Restore files and directories user right. If you want to assign the ability to back up files to a user, the easiest way is to add him or her to either the Backup Operators or Server Operators group.

Creating a Backup Operator

You can give a user the right to back up and restore all files on a computer running Windows NT, regardless of the NTFS permissions assigned to those files, by adding the user to the Backup Operators group. In networks where security is an issue, it is recommended that the user who performs the backup not have the right to restore files.

This prevents the user from restoring the files to a FAT volume, which removes NTFS security, or restoring files to a computer where the user has administrator privileges and can assign the NTFS permission Full Control to all files.

To give a user only the backup right, following these guidelines:

❑ Create a local group named Backup Only Operators on the computer where the tape drive is located and assign it the following user rights:

  - Log on locally. This user right is required to back up the registry. The registry is a database where Windows NT stores its configuration information, including the security and user account information in the directory database.
  - Back up files and directories. This user right provides the capability to perform a backup.

□ Create a global group named Backup Only on the primary domain controller. This group will be used to organize all user accounts that you want to give backup rights to.

□ Add the global group Backup Only to the local group Backup Only Operators. Add the user account to the global group Backup Only.

▸ **To create a local group with the appropriate user rights**

1. Log on as Administrator.
2. Start User Manager for Domains, and create a local group named *Backup Only Operators*.
3. Grant the following user rights to the Backup Only Operators group:
   - Back up files and directories
   - Log on locally

▸ **To create a global group to organize users who can back up data**

1. Create a global group named *Backup Only*.
2. Add the global group Backup Only to the local group Backup Only Operators.

▸ **To give a user the rights to back up the computer**

1. Add the user account User11-A to the global group Backup Only.
2. Quit User Manager for Domains.
3. Log off.

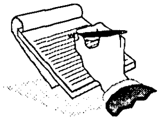
Lesson Summary

The following information summarizes the key points in this lesson:

- To use Windows NT Backup, you must have a computer running Windows NT Workstation or Windows NT Server with a tape drive supported on the hardware compatibility list (HCL).
- To back up the directory database (security and user account information) for the domain, the tape drive must be located on a domain controller.
- All users can back up any folders and files on the network for which they have the Read permission.
- You can give a user the right to back up and restore all files on a computer running Windows NT by adding the user to the Backup Operators group or by assigning the user right Back up files and directories (to back up files) and the user right Restore files and directories (to restore files) to a user account or group of which the user is a member.

For more information on	See
Hardware considerations	Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.
User rights	Chapter 2, "Working With User and Group Accounts," in Microsoft Windows NT Server *Concepts and Planning*.
NTFS permissions	Chapter 6, "Securing Network Resources with NTFS Permissions," in this book.
Groups	Chapter 3, "Setting Up Group Accounts," in this book.

Lesson 2: Planning a Backup Strategy



Before you begin backing up files, you need a backup strategy that meets the needs of your organization, and that guarantees the recovery of lost data. Effective information backup and retrieval are an administrator's most critical functions. It is important to create backup policies. This lesson describes important issues to consider for planning an effective backup strategy.

After this lesson, you will be able to:

- Describe the considerations for backing up files.
- Determine which folders and files to back up.
- Determine the backup type to use.
- Determine whether to rotate or archive tapes.
- Describe the difference between a backup set, catalog, and backup log.

Estimated lesson time: 30 minutes

A good backup strategy ensures that you can quickly recover your data if it is lost. Consider the following points to create an effective backup strategy that is best suited to your network:

- To determine which files to back up, use the following general backup rule: if you cannot get along without it, back it up.
- Deciding whether to perform a network backup or multiple local backups depends on which computers your organization uses for storing critical data.
  - Do a network backup when the critical data is on multiple servers or you want to perform a backup over the network. The following table describes the advantages and disadvantages of performing a network backup.

Advantages	Disadvantages
Backs up the entire network.	Users must copy their important files to the servers.
Requires fewer tape drives.	Cannot back up the registry on remote computers.
Less media to manage.	Increases network traffic.
One user can do the backup.	Requires greater planning and preparation.

  - Do multiple local backups when the critical data is on client computers. The following table describes the advantages and disadvantages of performing a local backup.

Advantages	Disadvantages
Fewer network resources committed.	Requires more tape drives and tapes. Users are responsible for backing up the data on their computers. The users may not be reliable.

  - Do both network and local backups when the critical data is on servers and workstations.
- How frequently to back up the data depends on the following:
  - How critical the data is to your company. You would want to back up critical data more often.
  - How frequently the data changes. For example, if users create or modify reports only on Fridays, a weekly backup for the report files would be sufficient.

Tip Plan to perform backups when network usage is low. If files are in use, Windows NT only backs up the last saved version of the file.

Determining Which Files to Back Up

There are folders and files that you need to always back up, some that you need to back up intermittently, and some that you never need to back up.

Use the following guidelines to help you determine which files to back up.

- Always back up:
  - Critical files that your organization needs to operate.
  - The registry on any domain controller—a BDC or PDC. Each domain controller maintains a copy of the directory database. Backing up the registry on a domain controller prevents loss of all user accounts and security information.

Important Windows NT Backup can only back up the registry on the computer where the tape drive is installed. If possible, you should have your tape drive installed on a domain controller.

- Periodically back up files that seldom change or are not critical to your organization.
- Do not back up temporary files, as they change constantly and are rarely used to recover data. Backing up temporary files not only uses extra tapes, it results in the creation of unnecessary files that take additional time to sort through when you need to look for key files to restore.

Note Windows NT Backup is not intended for volume recovery; it does not back up data at the sector level and cannot restore the boot partition. This means that to restore the operating system volume, you must format a volume, reinstall Windows NT, and then use Windows NT Backup to restore the registry and any additional files from the latest backup tape.

Determining the Backup Type to Use

Windows NT Backup provides five backup types—normal, copy, incremental, differential, and daily copy. Some backup types use *backup markers*, also known as archive attributes, to track when a file has been backed up. An effective backup strategy may combine different backup types, depending on the amount of time available to perform the backup and how quickly you would need to locate and restore files.

The following table describes the backup types.

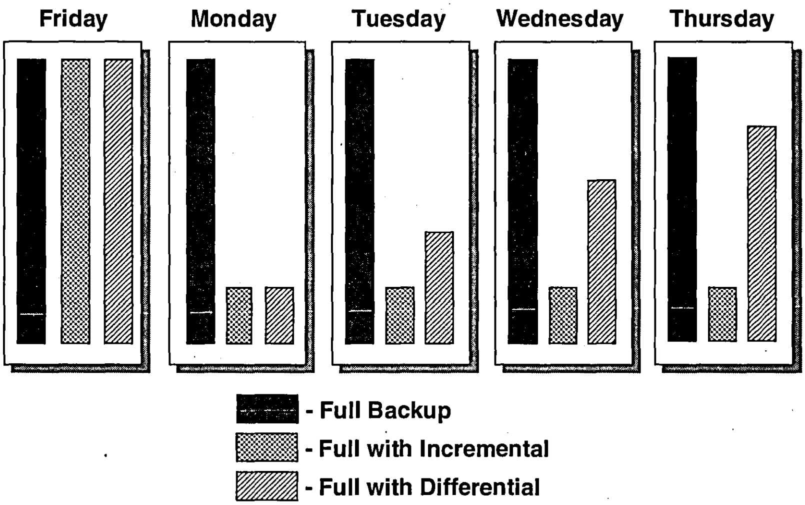
This backup type	Backs up
Normal (also called full)	Selected files and marks each as having been backed up. With normal backups, you can restore files quickly because files on the last tape are the most current. Always perform a normal backup of all files as the initial backup.
Incremental	Only those files created or changed since the last normal or incremental backup. It marks files as having been backed up. If you use a combination of normal and incremental backups, restoring requires starting with your last normal backup and then working through all the incremental tapes.
Differential	Those files created or changed since the last normal (or incremental) backup. It does not mark files as having been backed up. If you are doing normal and differential backups, restoring requires only the last normal and last differential backup tape.

(continued)

This backup type	Backs up
Copy	Selected files, but does not mark each file as having been backed up. Copying is useful if you want to back up files between normal and incremental backups, because copying does not invalidate these other backup operations.
Daily copy	Selected files that have been modified the day the daily backup is performed. The backed up files are not marked as having been backed up. (This can be useful if you want to take work home and need a quick way to select the files that you worked on that day.)

Examples of Using Different Backup Types

You can combine backup types to create a backup strategy to fit your particular needs. Some backup types require more time to back up data, but less time to restore. Others require less time to back up, but more time to restore. You need to consider which task you want to spend your time on, and how quickly you need access to lost data.



The time necessary for backup and restore operations varies depending on the backup strategy used. Each strategy has advantages and disadvantages.

Normal Backup

Using this strategy (as shown in the previous illustration), a full backup is performed every day. The disadvantage of this strategy is that this type of backup takes the longest amount of time each day and requires the most tapes. The advantage of this strategy is that if there is a catastrophic system failure on Thursday, only one tape will be required to perform a full restore.

Normal with Incremental

Using this strategy (as shown in the previous illustration), a full backup is performed each Friday. On Monday, everything that has changed since Friday is backed up. On Tuesday, everything that has changed since Monday is backed up, on Wednesday, everything that has changed since Tuesday is backed up, and so on. The advantage with this strategy is that the amount of time to do daily backup is minimal. The disadvantage is that if there is a catastrophic system failure on Thursday, it is possible that five tapes will be required to perform a full restore.

Normal with Differential

Using this strategy (as shown in the previous illustration), a full backup is performed on Friday. On Monday, everything that has changed since Friday is backed up. On Tuesday, everything that has changed since Friday is backed up, on Wednesday, everything that has changed since Friday is backed up, and so on. The disadvantage with this strategy is that backing up files takes progressively longer each day. The advantage is that if there is a catastrophic system failure on Thursday, only two tapes will be required to perform a full restore, the Friday tape and the Wednesday tape.

Tip Because the copy backup type does not set a backup marker, use it to make tape copies that will not interfere with ongoing backups—for example, an archive tape.

Rotating and Archiving Tapes

Rotating tapes ensures that you can always go to a previous tape for a lost file, even though it may not be the most current version of the file. If you perform a backup using the same tape, you run the risk of not being able to recover lost files in the event that the tape becomes damaged.

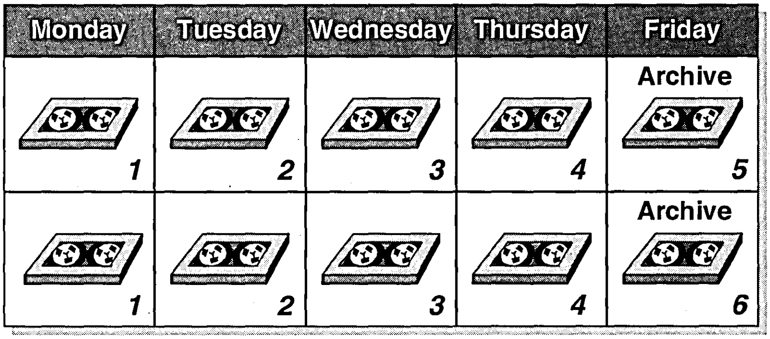
You may want to archive some tapes. Archived tapes are useful for maintaining a record of data for a specific date and time—for example, a quarterly record of financial data in case of an IRS audit. When you archive a tape, you remove it from the tape rotation.

The following are two examples of tape rotation.

Example 1

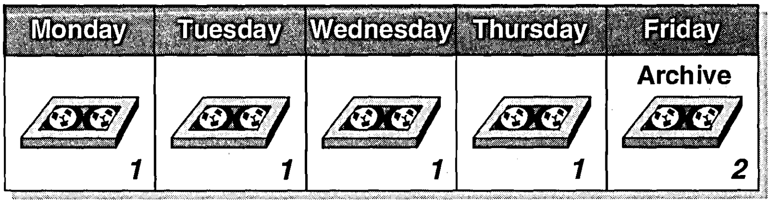
Each day of the week is on a different tape. The tape for one day of the week is archived and removed from rotation. In this example, six tapes are used. The tape for each Friday is archived.

For the following weeks, use the Monday through Thursday tapes for the same day of the week; for example, put the Monday backup on the Monday tape. These backups can either replace or append the previous backup on the tape.



Example 2

The Monday through Thursday backups use the same tape with each new backup appended to the previous one. The Friday backup is on a different tape that is archived. The next week you would start all over again with tape 1.



Note The number of tapes you need is determined not only by tape rotation, but also by the size of the files that you back up and by the life cycle of the tape.

The life cycle of a tape depends on the manufacturer and on storage conditions. If your company does not have a suitable storage facility, consider using a third-party company that specializes in off-site storage for backup media.

Backup Sets, Catalogs, and Backup Logs

Before you do a backup, it is helpful for you to know the differences between backup sets, catalogs, and backup logs.

- A *backup set* is the term used to describe a group of files or folders on a single volume from a single backup operation. One tape can contain many backup sets.

  If a single backup operation requires multiple tapes, the group of tapes is called a family set.

- The *catalog* is a graphical representation of the backup. Windows NT automatically creates catalogs during a backup and stores them on the tape. There are two different catalogs:

  - The *tape catalog* shows all the backup sets on a tape.
  - The *backup set catalog* shows all of the files and folders in the backup set.

  Before you restore files, you must load the catalogs. Then, you can select the backup sets, files, and folders that you want to restore.

- A *backup log* is a text file that records backup operations. The backup log is helpful when restoring data, in that you can print it or read it using any text editor. The backup log is stored on disk, so if the tape containing the backup set catalog is corrupted, the backup log will help you locate a file.

  A backup log may contain some or all of the following information, depending on which log options you select:

  - Date of backup
  - Tape-set number
  - Type of backup
  - Who performed the backup
  - Files backed up
  - Computers backed up
  - Location of the tape drive

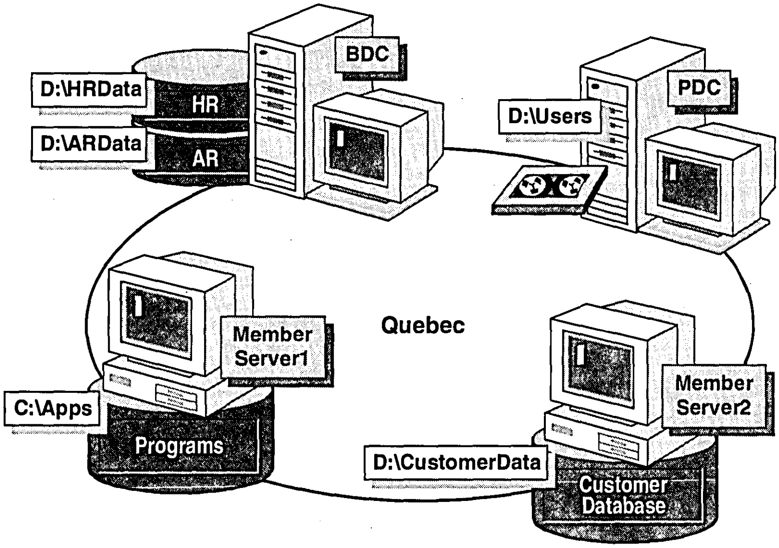
▶ **To plan a backup schedule**

In this exercise, you plan a backup schedule for the Quebec domain. The Quebec domain has four servers—two servers are configured as domain controllers, and two are configured as member servers. The tape drive is installed on the primary domain controller (PDC).

You need to determine:

- Whether files need to be backed up daily or weekly.
- A weekly backup schedule that includes a backup type for each day, which tape to use, and whether that tape will be archived or reused.

Record your decisions on the "Backup Planning Worksheet," located at the end of this lesson.



Use the following criteria to make your decisions:

- Programs are upgraded approximately every three months. Minor updates are applied as necessary.
- The Accounts Receivable (AR) database is updated each day with full and partial payments received from customers.
- The Human Resources (HR) database is updated every time a new employee is hired or an existing employee goes on vacation.
- Users store letters, memos, and archived e-mail in their home folders. Most data does not change frequently.
- Critical customer files are stored in the Customer database.
- Lost data must be restorable in a quick and easy manner.
- All backups should be well documented.

To complete the "Backup Planning Worksheet," you need to:

1. Provide the path to the folders and files that will be backed up. Record it under Folders and Files to Backup.
2. Specify whether the backup is daily (record it under Daily) or, if weekly, the day of the backup (record it under Weekly).
3. Fill in the weekly backup schedule with the backup type, tape number (record this information under Weekly Backup Schedule), and type of backup log (record it under Type of Backup Log).
4. When you are done, compare your answers to the answers on the "Backup Planning Worksheet" in Appendix A of this book.

Lesson Summary

The following information summarizes the key points in this lesson:

- Plan an effective backup strategy to ensure that you can quickly recover lost or corrupted files.
- Always back up critical files and the registry.
- Use backup types to create a backup strategy to fit your needs. Always do a normal backup of all files as your initial backup.
- Rotate your tapes so that you can always go back to a previous tape for a file. If you always back up to the same tape and that tape becomes damaged, you will not be able to recover files.
- Always create and print your backup logs. This will help you to locate lost files quickly.

For more information on	See
Planning a backup	Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.
Backup strategies	Chapter 4, "Planning a Reliable Configuration," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*

Backup Planning Worksheet

Tape Drive Location____________________ **Tape Storage Location**_____________________________________

Folders and Files to Back Up (Provide Path)	Daily	Weekly (Provide Day)

Weekly Backup Schedule

Monday	Tuesday	Wednesday	Thursday	Friday
Backup Type___________ Tape____________ Archive Y__N__	Backup Type___________ Tape____________ Archive Y__N__	Backup Type___________ Tape____________ Archive Y__N__	Backup Type___________ Tape____________ Archive Y__N__	Backup Type___________ Tape____________ Archive Y__N__

Backup Types

N = Normal	D = Differential	I = Incremental	C = Copy	DC = Daily Copy

Type of Backup Log

❑ Full Detail ❑ Summary Only ❑ Don't Log

Lesson 3: Backing Up Files

This lesson guides you through the steps required to back up data. When you create a backup, you need to conduct several preliminary tasks, and then you perform a number of tasks using the Windows NT Backup program.

After this lesson, you will be able to:

- Prepare for a backup.
- Perform a backup to tape.

Estimated lesson time: 20 minutes

Preparing to Back Up Files

Before you begin backing up files, you need to do the following tasks:

□ Prepare your tapes. If you are beginning your backups with tapes that contain obsolete files, it is recommended that you erase the tapes first by clicking **Erase Tape** on the Windows NT Backup **Operations** menu. You can do either a **Quick Erase**, during which the tape header is simply rewritten, or a **Secure Erase**, during which the entire tape is overwritten. The secure erase method may take several hours to complete, depending on the drive technology and tape length.

If you are using a new tape that is not pre-formatted, you must format the tape by clicking **Format Tape** on the Windows NT Backup **Operations** menu. Formatting a tape may take a while, so plan ahead.

□ Connect to all shared folders on other computers that need to be backed up.

Note Windows NT Backup can only back up the registry or event logs on the computer where the tape drive is located.

□ Notify users to close their files before you begin the backup. If backups are performed at night, have users log off their computers before they go home. This will ensure that all files are closed.

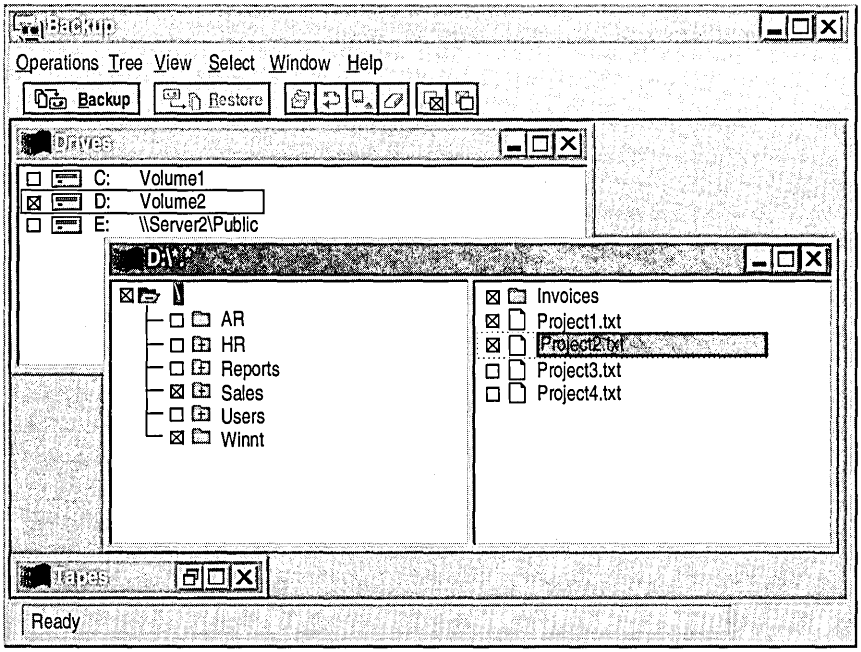
Windows NT Backup does not back up files that are locked open by programs; for example, it would not back up a Microsoft Word document that is currently being edited. Windows NT operating system files are the exception; they can be backed up while they are in use.

You can send a message to users to notify them of the backup. To send a message to users, follow these steps:

1. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Server Manager**.
2. On the **Computer** menu, click **Send Message**.
3. Type the message to your users, and then click **OK**.

Selecting Drives, Folders, and Files

After you have connected to remote drives and notified users, the next step is to start Windows NT Backup (in Administrative Tools) and select the drives, folders, and files that you want to back up, as shown in the following illustration.



□ C: Volume1
☒ D: Volume2
□ E: \\Server2\Public

☒ D:
- □ AR
- □ HR
- □ Reports
- ☒ Sales
- □ Users
- ☒ Winnt

☒ Invoices
☒ Project1.txt
☒ Project2.txt
□ Project3.txt
□ Project4.txt

To back up all folders and files on a drive, in the Drives window, select the check box next to the drive icon.

To select specific folders and files on a drive, in the Drives window, double-click the drive icon. The window for the drive appears. This window shows a graphical view of the drive, which is similar to Windows NT Explorer. You can use one of the following methods to select folders and files:

- Select the check box next to each folder or file.

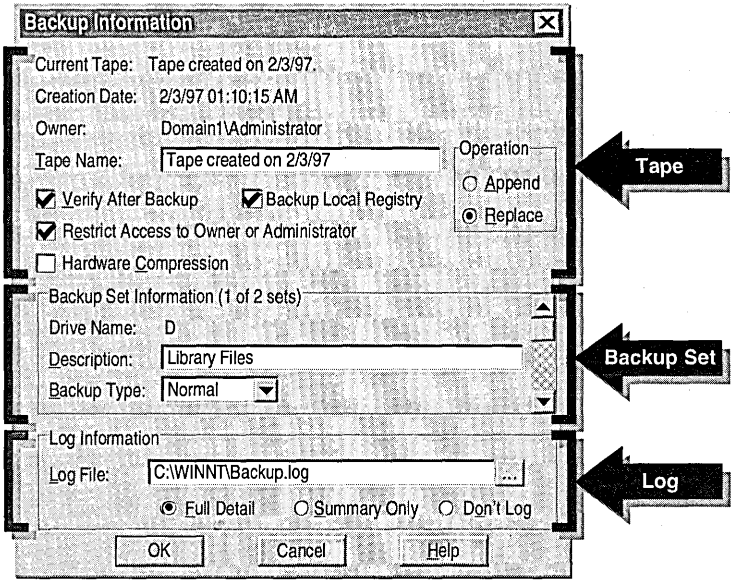
  –or–

- Select the folder or file that you want to back up, and then, on the **Select** menu, click **Check**.

Note If you do not select all the folders and files on a drive or parent folder, the selected check box appears shaded. This indicates a partial selection.

Setting Tape, Backup Set, and Log Options

After you select the drives, folders, or files to back up, the next step is to set the tape, backup set, and log options. Click **Backup** to gain access to the **Backup Information** dialog box. At the top of the dialog box is tape information, which includes the current tape name, creation date, and the owner of the tape.



Backup Information

Current Tape: Tape created on 2/3/97.

Creation Date: 2/3/97 01:10:15 AM

Owner: Domain1\Administrator

Tape Name: Tape created on 2/3/97

Operation: ○ Append ● Replace

☑ Verify After Backup ☑ Backup Local Registry

☑ Restrict Access to Owner or Administrator

□ Hardware Compression

Backup Set Information (1 of 2 sets)

Drive Name: D

Description: Library Files

Backup Type: Normal

Log Information

Log File: C:\WINNT\Backup.log

● Full Detail ○ Summary Only ○ Don't Log

The following table describes the **Backup Information** dialog box options.

Option	Description
Tape Name	A name that you assign to identify where the tape fits into your backup strategy—for example, the name of the server you are backing up. This name can have up to 32 characters. If you select the **Append** option, the **Tape Name** box is not available.
Append	Adds a new backup set after the last backup set on the tape.
Replace	Overwrites all of the data on the tape with the new backup set.
Verify After Backup	Confirms that files are backed up accurately.
Backup Local Registry	Adds a copy of the registry to the backup set. Because you are unable to back up the registry alone, this option is available only if you select at least one other file on the local volume containing the registry file.
Restrict Access to Owner or Administrator	Limits access to the tape to Administrators, Backup Operators, or the user who performed the backup. If you back up the registry, you should select this option.
Hardware Compression	Select this option if you are using a tape drive that supports data compression. This option is available only if the tape drive supports it.
Backup Set Information	**Description**: Describes the backup set. This description should be intuitive, for example—**Server1Drive C** If there are multiple backup sets, you can type a description for each one. Use the scroll bar on the right side of the **Backup Set Information** box to move between backup sets. **Backup Type**: Specifies the type of backup, either Normal, Copy, Incremental, Differential, or Daily Copy.
Log Information	**Log File**: Specifies the name of the text file used to store the log. The default name is Backup.log. It is stored in the *systemroot* folder. (In most installations, *systemroot* is Winnt.) **Full Detail**: Logs all backup information, including the names of all the files and folders that are backed up, skipped, and corrupted. **Summary Only**: Logs only the major backup operations, such as loading a tape, starting backup, and failing to open a file. **Don't Log**: No information is logged.

Tip Print each backup log. Keep the printed copy in a log book.

Implementing a Backup

In this exercise, you use a Backup Simulation program to simulate backing up files to tape. The Backup Simulation is a Visual Basic® program that was developed so that you can practice backing up files without a tape drive in your computer.

With this simulation, you can:

- Erase the tape.
- Select drives, folders, and files to back up.
- Select the backup type.
- Select backup and log options.

▸ To start the Backup Simulation program

1. Log on as Administrator.
2. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Backup Simulation.**

   The Backup Simulation window appears.

   Note If you were using the actual Windows NT Backup program, you would start it by clicking the **Start** button, pointing to **Programs**, pointing to **Administrative Tools**, and then clicking **Backup**.

▸ To erase a tape

In this procedure, you perform a secure erase to ensure that all old files are removed from the tape.

1. In the Backup Simulation window, on the **Operations** menu, click **Erase Tape**.

   The **Erase Tape** dialog box appears with a warning message that all information on the tape will be destroyed.
2. Click **Secure Erase**, and then click **Continue**.

   The Erase Status window appears and shows you a summary of the process.
3. When the operation is finished, click **OK**.

▸ To select folders and files to be backed up

In this procedure, you specify folders and files on drive D to be backed up.

1. Click to clear the check box next to drive D.
2. Double-click the disk icon for drive D.

   The D:\*.* window appears.
3. Expand the folder hierarchy for drive D.

   Notice that on drive D there are two folders—the Data folder and the Public folder.
4. Expand the Data folder, and then select the check box next to the Managers folder.

   Notice that when you selected Managers, the file in Managers was automatically selected.
5. Expand the Public\Library folder, and then select the check box next to the Bronte folder.

   Notice that when you selected Bronte, the file in Bronte was automatically selected.
6. Click the Public\Templates folder (do not select the check box next to it), and then select the check boxes next to the following files:
   - Timesheet.dot
   - Timerecord.doc
   - Timesheet.doc

▸ To begin the backup process

1. In the Backup Simulation window, click **Backup**.

   –or–

   On the **Operations** menu, click **Backup**.

   The **Backup Information** dialog box appears. Notice that the current tape is blank and the creation date is the date that the tape was erased.
2. If you want a tape name other than the default, in the **Tape Name** box, type a descriptive name for your tape. For example, **Archive data** *today's date*
3. Select the following options:
   - **Verify After Backup** to confirm that the files were backed up correctly.
   - **Restrict Access to Owner or Administrator** so that only members of the Administrators and Backup Operators groups can restore files from this tape.

   Notice under **Operation**, that **Replace** is selected and **Append** appears dimmed. This is because no data is on the tape to append to.

▶ To specify a backup set description and the type of log information

1. In the **Description** box, type a descriptive name for your backup. For example, type **classics**
2. In the **Backup Type** box, click **Normal** (if it is not already selected).
3. Accept the default path of *drive*:\systemroot\\Backup.log for the log file.
4. Under **Log Information**, make sure that **Full Detail** is selected, and then click **OK**.

   Note The Backup Simulation program will only create a Full Detail log.

   The Backup Status window appears and shows you a summary of the operation.
5. When the backup process is finished, click **OK**.

   A Tapes window appears in the Backup Simulation window. Notice that it shows the date the tape was created, the drive that contained the files that were backed up, and the type of backup (normal).

▶ To prepare the Backup Simulation for Lesson 5, "Restoring Files"

- Minimize the Backup Simulation window.

Important The Backup Simulation program is designed to back up and restore files in a single operation. This means that if you close the program, you will need to perform another backup before you are able to restore files in Lesson 5 of this chapter, "Restoring Files."

▶ To view the backup log

In this procedure, you view the backup log to see the files that were backed up.

1. Start Windows NT Explorer.
2. In the *drive*:\systemroot folder, double-click Backup.log. (Backup.log may appear in Windows NT Explorer as Backup.)

   The Backup.log file appears in Notepad. Notice that the files in Backup.log are those that you backed up. Each file includes the date and time that the file was created, and the size of the file in bytes.
3. Quit Notepad.
4. Quit Windows NT Explorer.

Lesson Summary

The following information summarizes the key points in this lesson:

- Before you begin to back up files, you need to prepare your tapes, connect to shared folders on remote computers that need to be backed up, and then notify users to close their files.
- Select the drives, folders, and files to be backed up based on your backup strategy.
- Assign descriptive names to your tapes and backup sets. This makes it easier to identify their contents.
- When you back up the registry, always restrict tape access to members of the Administrators or the Backup Operators group.

For more information on	See
Backing up files	Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.

Lesson 4: Scheduling a Backup Using a Batch File

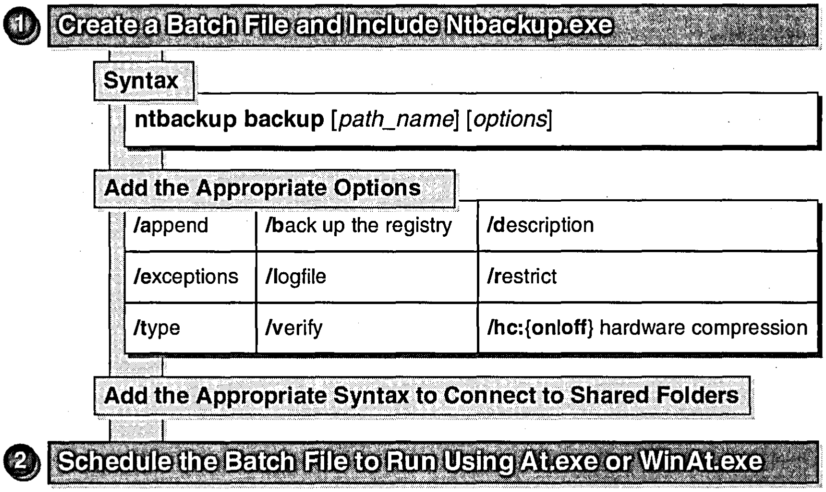
This lesson shows you how to automate the backup process by using a batch file and a Windows NT command scheduling program.

After this lesson, you will be able to:

- Write a batch file to back up your data.
- Use the Microsoft Windows NT **at** command (At.exe) to schedule backups.
- Use the Microsoft Windows NT Command Scheduler (WinAt.exe) to schedule backups.

Estimated lesson time: 20 minutes

There are two steps to scheduling an automatic backup. In the first step, you create a batch file with the **ntbackup** command and the details of the backup. In the second step, you schedule the batch file to run using either the Windows NT **at** command (which is included with Windows NT), or the Windows NT Command Scheduler (which is included in the *Microsoft Windows NT Server Resource Kit* version 4.0). The following illustration provides an overview of the required steps.



1 Create a Batch File and Include Ntbackup.exe

Syntax

ntbackup backup [*path_name*] [*options*]

Add the Appropriate Options

/append	**/b**ack up the registry	**/d**escription
/exceptions	**/l**ogfile	**/r**estrict
/type	**/v**erify	**/hc:**{**onloff**} hardware compression

Add the Appropriate Syntax to Connect to Shared Folders

2 Schedule the Batch File to Run Using At.exe or WinAt.exe

The following table describes options that you can use when you create the batch file.

Option	Description
/a	Appends the backup set after any existing backup sets, rather than replacing it. This is not available for a blank tape.
/b	Backs up the local registry, but only if you back up another file from the same volume.
/d "*text*"	Describes the backup set. This description appears when you view the tape catalog.
/e	Logs exceptions, such as summary log. If this option is not used, a full detail log is created.
/l *file_name*	Assigns a file name to the log file. The default is Backup.log in the *systemroot* folder.
/r	Limits access to the tape to Administrators, Backup Operators, or the user who performed the backup. If not used, anyone with the restore right can restore the backup set.
/t {**Normal | Copy | Incremental | Differential | Daily**}	Specifies the backup type. The default backup type is normal.
/v	Confirms that the files were backed up accurately.
/hc: {**on | off**}	Enables or disables hardware compression for tape drives that support it. The default is hardware compression off.
net use *x***:**	Connects to a shared folder. Use this command at the beginning of the batch file if you are backing up files on a remote computer, and if you need to connect to a shared folder as a different user—for example: **net use x: \\Server1\Data /u:Domain1\User11**
net use *x***: /delete**	Disconnects from a shared folder. Use this command at the end of the batch file to disconnect from any remote shares.
\server_name\share_name	Connects to a shared folder. If you do not need to connect to a shared folder as a different user, you can use the UNC path of the shared folder with the **ntbackup backup** command. By using the UNC name, you do not need to disconnect from the shared folder.

Example of a Scheduled Backup

This example shows a batch file with the **ntbackup** command.

Batch File

```
net use x: \\computer1\public /u:domain1\user11
ntbackup backup c: d: x: \\server1\public
/t incremental /b /hc:on /v /l “c:\weekly.log”
net use x: /delete
```

Examine the example to determine the answers to the following questions.

1. What tasks will this batch file perform?

2. What would you add to this batch file to make it easier to identify the contents of the tape that this batch file creates?

3. What command would you add to the batch file to back up files (owned by the Administrators group) in the Data folder on a computer named Server2?

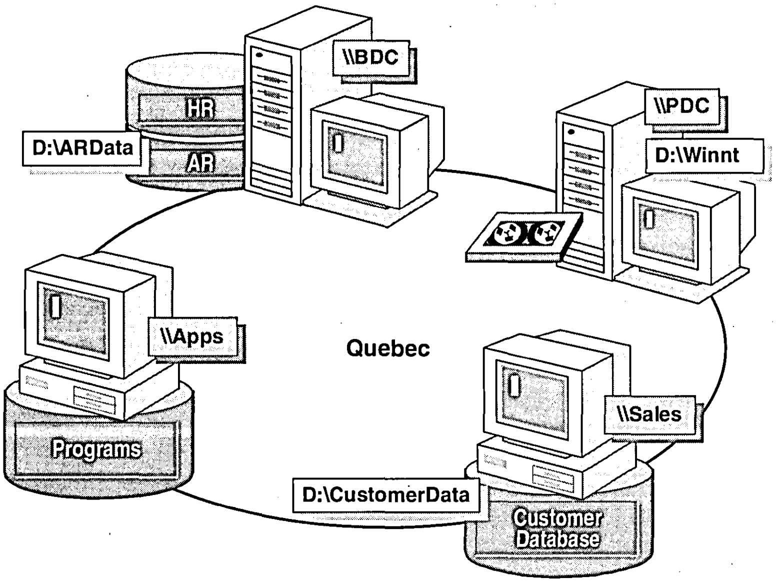
▶ **To write a batch file to back up data**

In this exercise, you write a batch file to schedule a backup for servers in the Quebec domain of World Wide Importers.

You need to create a batch file that does the following:

- Performs a differential backup of the shared CustomerData and ARData folders.
- Provides the description “Customer Data” on the backup tape.
- Create a log named “Tuesday.log.”
- Verifies the backup.
- Adds the backup to the Tuesday backup tape.
- Does not implement hardware compression.

The following illustration shows the network servers and the data that they contain.



Write down the commands that need to appear in the batch file.

____

____

____

____

____

____

▸ To get help on Ntbackup command syntax

1. At a command prompt, type **ntbackup /?** and then press ENTER.
2. Read through the information in Backup Help, and then close it.

Using the AT Command

Once you have a batch file that includes Ntbackup.exe, you can use At.exe to schedule the batch file to run at a specific time. The **at** command schedules commands from a command line.

Example: AT Command

```
at \\computer1 00:00 /every: 5,10,15,20,25,30
"backup.bat"
```

Starting the Schedule Service

To use the **at** command, the Schedule service must be started on the computer that will run the scheduled backup. The Schedule service is a Windows NT service used to schedule tasks, such as backing up files. If you use the **at** command to perform a backup on a regular basis, you should configure the Schedule service to start automatically when Windows NT is started. You can start the Schedule service using Server Manager or the Services program in Control Panel.

▸ **To configure the Schedule service to start automatically using Server Manager**

1. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click Server Manager.
2. Under **Computer**, click your computer name, and then on the **Computer** menu, click **Services**.

   The Services on *computer_name* window appears.
3. Under **Service**, click **Schedule**, and then click **Startup**.

   The Service on *computer_name* window appears.
4. Under **Startup Type**, click **Automatic**, and then click **OK**. The Services on *computer_name* window appears.

   The Schedule service will now automatically start the next time the computer is shut down and restarted.
5. Under **Service**, click **Schedule**, and then click **Start**.

   The Service Control message window appears with the following message: `Attempting to Start the Schedule service on` *`computer_name`*.
6. Click **Close**, and then quit Server Manager.

Scheduling the Batch File

The **at** command uses the following syntax. Become familiar with the syntax and the command options before you schedule the batch file.

at [\\computer_name] [*id*] [**/delete**] *time* [**/interactive**][**/every**: *date*[,...] | **/next**: *date*[,...] "*command*"

The following table describes the **at** command options.

Option	Description
\\computer_name	Specifies a remote computer. If omitted, the commands are scheduled on the local computer.
id	Assigns an identification number to a scheduled command.
/delete	Cancels a scheduled command. If it is omitted, all of the scheduled commands on the computer are canceled.
time	Specifies the time that the command is to run. Time is expressed as hour:minutes in 24-hour notation. It runs 00:00 (midnight) through 23:59.
/interactive	Allows the job to interact with the desktop of the user who is logged on at the time that the job runs. You only use this option if Windows NT Backup is running on your computer and you want to observe it. If any errors occur, you will be able to correct them.
/every: *date*[,...]	Specifies the weekdays or days of the month that a command is to run. If omitted, the default is the current day of the month.
/next: *date*[,...]	Specifies the next weekdays or days of the month that a command is to run. If omitted, the default is the current day of the month.
"*command*"	Specifies the program or batch file to run, such as Ntbackup.exe.

▶ To schedule a task using the AT command

In this procedure, you schedule the game FreeCell to run at a specified time. Using FreeCell will show you how the **at** command works. If you were scheduling an actual backup, you would substitute NtBackup.exe for Freecell.exe.

1. Start a command prompt.
2. View the **at** command syntax by typing **at /?** and then pressing ENTER.

   Read the information about the **at** command.

3. Check the current system time and write it down here. You will need it to complete the next step.

   ____

4. Add two minutes to the system time, type the following command, and then press ENTER. Substitute the future time for *hh:mm* using the 24-hour format.

   at *hh:mm* **/interactive "***drive***:\***systemroot***\\system32\\freecell.exe"**

   FreeCell should run on your computer within the next couple of minutes.

> **Note** If FreeCell fails to run, use the taskbar clock to verify that the time that you entered is correct for A.M. or P.M.

Using the Command Scheduler

The Command Scheduler is a utility included in the *Microsoft Windows NT Server Resource Kit* version 4.0 that provides a graphical way to schedule tasks.

This utility is included on the Supplemental Material compact disc that accompanies this book. If you completed the Setup procedures located in "About This Book," a shortcut to this tool was added to your **Network Administration Training** menu.

▶ To schedule a task using the Command Scheduler

In this procedure, you configure the Schedule service to start the game FreeCell to run at a specified time. If you do not have FreeCell on your computer, substitute Notepad.exe.

1. Click the **Start** button, point to **Programs**, point to **Network Administration Training**, and then click **Command Scheduler**.

   The Command Scheduler window appears.

> **Note** If the Schedule service is not running on your server, Command Scheduler will prompt you to start it.

2. Click **Add**.

   The **Add Command** dialog box appears.

3. In the **Command** box, type *drive*:\systemroot\system32\\freecell.exe

4. Under **This Occurs**, click **Today**.

   Under **Days**, notice that the current day is selected.

5. Under **Time**, add two minutes to the system time to specify a future time.
6. Click **Interactive**, and then click **OK**.

   Notice that the configured command appears in the Command Scheduler window.

7. Quit Command Scheduler and wait until the entered time arrives. FreeCell should run on your computer within the next couple of minutes.
8. Quit FreeCell.

Lesson Summary

The following information summarizes the key points in this lesson:

- You can automate the backup process using a batch file and the Windows NT **at** command (At.exe) or the Windows NT Command Scheduler (WinAt.exe).
- To schedule an automatic backup, first create a batch file with the details of the backup, and second, schedule the batch file to run using either the At.exe (included with Windows NT) or WinAt.exe (included in the *Microsoft Windows NT Server Resource Kit* version 4.0).
- The Schedule service must be started on the computer where the tape drive is installed before you can run the scheduled backup. You can start the Schedule service using Server Manager or the Services program in Control Panel.

For more information on	See
Windows NT Backup command prompt parameters	Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.
Using the **at** command scheduler	The Microsoft Knowledge Base at http://www.microsoft.com/kb/
	Chapter 22, "Disk, File System, and Backup Utilities," in the *Microsoft Windows NT Workstation Resource Kit.*
	Chapter 7, "Disk, File System, and Backup Utilities," in the *Resource Guide* of the *Microsoft Windows NT Server Resource Kit.*

Lesson 5: Restoring Files

This lesson describes the key principles that contribute to an effective data restoration strategy.

This lesson requires that you have completed Lesson 3.

After this lesson, you will be able to:

- Implement a restoration strategy.
- Create a restore operator.
- Restore files.

Estimated lesson time: 30 minutes

Implementing a Restoration Strategy

A good restoration strategy means that you can quickly locate and restore lost files. Having a good restoration strategy depends on the following:

- A good backup strategy. For example, if you always do a full backup of a volume, then in the unlikely event of a disk failure, you can restore the volume in a single operation. Rotating tapes over a period of a week ensures that you can restore an earlier version of a file.
- Keep documentation for each backup. By creating and printing a backup log of each backup, you will be able to quickly locate files that need to be restored without having to load the catalogs from all current backup sets.

  Depending upon the log that you create, the log can include information about the backup type, which folders and files are backed up, and on which tape they are located.
- Keep a record of multiple backups in a calendar format showing the days that you do backups. By each backup, note the type of backup and a tape identifier, such as a number. Then, if there is a problem, you have a quick glimpse of backups over several weeks and which tape was used for each.
- Store a set of backup tapes off-site in case of fire or other disaster. Consider using a third-party company that provides storage of magnetic media. You can even restore tapes to the offline servers at the alternate facility every time you do a backup.
- Perform a trial restoration periodically to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up with software verifications.

  Restore the tape to a drive other than the original drive, and then compare the restored files to the files on the original drive.

Creating a Restore Operator

In networks where security is an issue, it is recommended that the user who restores files is different from the user who backs up files. You can create a restore operator by assigning a user account the Restore files and directories user right.

The following checklist outlines the recommended method for creating a restore operator:

□ Create a local group named Restore Operators on the computer where the tape drive is located and assign it the following three user rights:

- Log on locally. This user right is required to back up the registry.
- Restore files and directories. This user right provides the capability to do a restoration.
- Shut down the system. This user right is required so that the server can be restarted to implemented changes made to Windows NT files, such as the registry.

□ Create a global group named Restore Only on the primary domain controller. This group will be used to organize all user accounts that you want to give restore rights to.

□ Add the global group Restore Only to the local group Restore Operators. Add the user account to the global group Restore Only.

▸ **To create a local group with the appropriate user rights**

1. Start User Manager for Domains.
2. Create a local group named *Restore Operators*.
3. Grant the following user rights to the Restore Operators group:
   - Log on locally
   - Restore files and directories
   - Shut down the system

▸ **To give a user the rights to restore to the computer**

1. Create a global group named *Restore Only*.
2. Add the Restore Only group to the Restore Operators group.
3. Add the user account User11-B to the Restore Only group.
4. Quit User Manager for Domains.

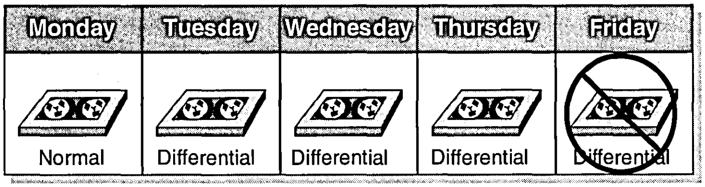
Examples of Restoration Strategies

Each of the following restoration strategies uses a different combination of backup types to back up files. As a general rule, review your backup logs to identify the appropriate tapes to use to restore files for any restoration strategy.

Note If only one file is corrupted, you need to find only the last backup of that file and restore it.

Example 1: Restoring Normal and Differential Backups

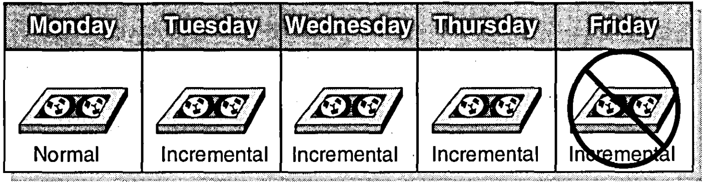
On Friday an entire volume became corrupted. Based on the backup schedule, restore the normal backup from Monday. Then, because the remaining backups are differential, the only additional restoration that is necessary is the backup from Thursday.



Monday	Tuesday	Wednesday	Thursday	Friday
Normal	Differential	Differential	Differential	Differential

Example 2: Restoring Normal and Incremental Backups

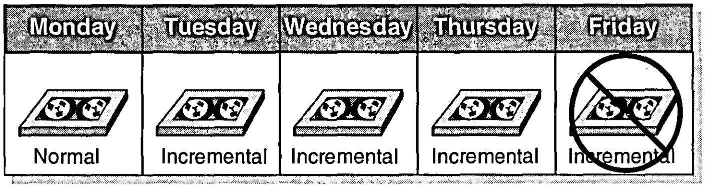
On Friday an entire volume became corrupted. Based on the backup schedule, restore the normal backup from Monday. Because the remaining backups are incremental backups, you also need to restore the backups from Tuesday through Thursday, in that order.



Monday	Tuesday	Wednesday	Thursday	Friday
Normal	Incremental	Incremental	Incremental	Incremental

Example 3: Restoring a Single File

On Friday, one file became corrupted. Because after Monday the backups are incremental backups, you cannot be sure which tape has the most recent copy of the file. Use the backup log to determine when the file was last backed up and which tape contains the backup. Then, restore the file from that tape.



Caution Make sure that the date on your computer is correct. Windows NT Backup uses the date attribute of the file to determine which file version is most current. If you change the date, you may overwrite a file with an older version.

Preparing to Restore Files

Before you begin restoring files, you need to connect to all shared folders on other computers where files will be restored.

Note Windows NT Backup can only restore the registry or event logs on computers where the tape drive is installed.

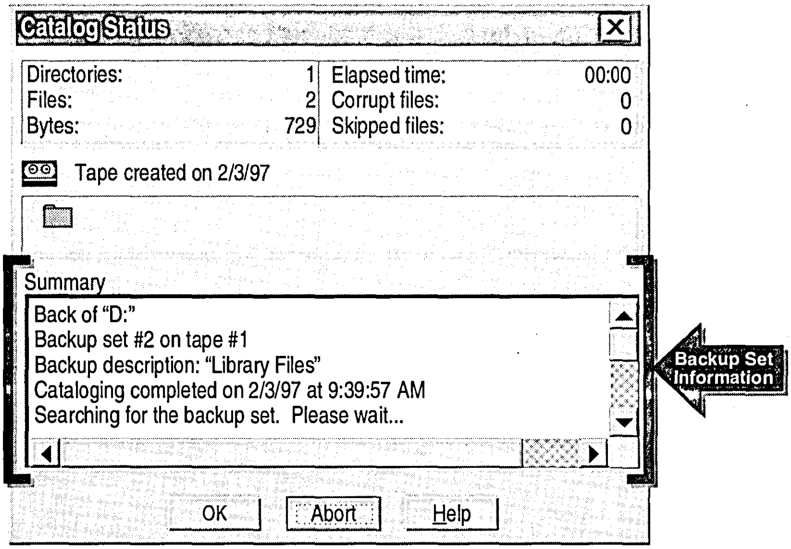
Loading the Tape and Backup Set Catalogs

The first step in restoring data is to start Windows NT Backup (in Administrative Tools) and load the tape and backup set catalogs. The tape catalog shows all the backup sets on a tape. The backup set catalog shows all of the folders and files in the backup set. You use both catalogs to verify the data you have, and to select data to restore. If a tape has only one backup set, loading the tape catalog will automatically load the backup set catalog.

The following table describes the steps that you use in Windows NT Backup to load a tape and backup catalog.

To	Do this
Load a tape catalog	On the **Operations** menu, click **Catalog**.
Load a backup catalog	Double-click the appropriate backup set folder.

After each task, the **Catalog Status** dialog box shows a summary of the backup set information. When the catalog finishes loading, click **OK**.



Directories: 1 Elapsed time: 00:00
Files: 2 Corrupt files: 0
Bytes: 729 Skipped files: 0

Tape created on 2/3/97

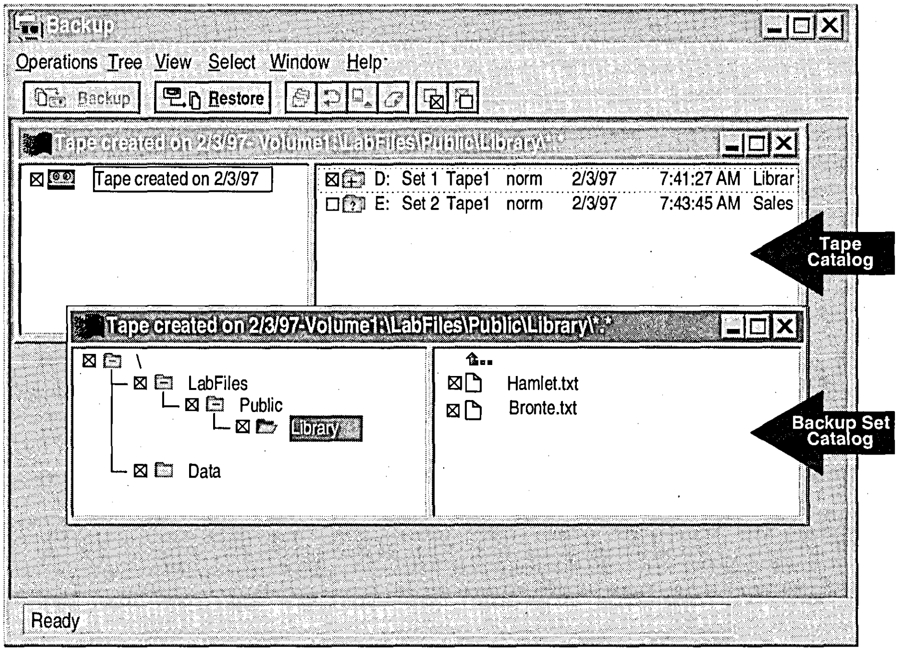
Summary

Back of "D:"
Backup set #2 on tape #1
Backup description: "Library Files"
Cataloging completed on 2/3/97 at 9:39:57 AM
Searching for the backup set. Please wait...

Important If the last tape in a family set is missing or damaged, you can force Windows NT Backup to treat the data on each remaining tape as a single unit, by starting Windows NT Backup at the command prompt with the **/missingtape** option.

Selecting Backup Sets, Files, and Folders

After a backup set catalog is loaded, the *tape_name* window appears with the folder tree for the backup set. The question mark (?) on the folder changes to a plus sign (+). To see this, you have to maximize the *tape_name* window. If there are corrupted files on the tape, the files' corresponding folders are marked with a red X.


Backup
Operations Tree View Select Window Help
Backup
Restore
Tape created on 2/3/97-Volume1:\LabFiles\Public\Library\*.*
☒ Tape created on 2/3/97
☒ D: Set 1 Tape1 norm 2/3/97 7:41:27 AM Librar
□ E: Set 2 Tape1 norm 2/3/97 7:43:45 AM Sales
Tape created on 2/3/97-Volume1:\LabFiles\Public\Library\*.*
☒ \
☒ LabFiles
☒ Public
☒ Library
☒ Data
☒ Hamlet.txt
☒ Bronte.txt
Ready

Tape Catalog

Backup Set Catalog

Once you have loaded the tape catalog, you can select a backup set by clicking the check boxes for the set.

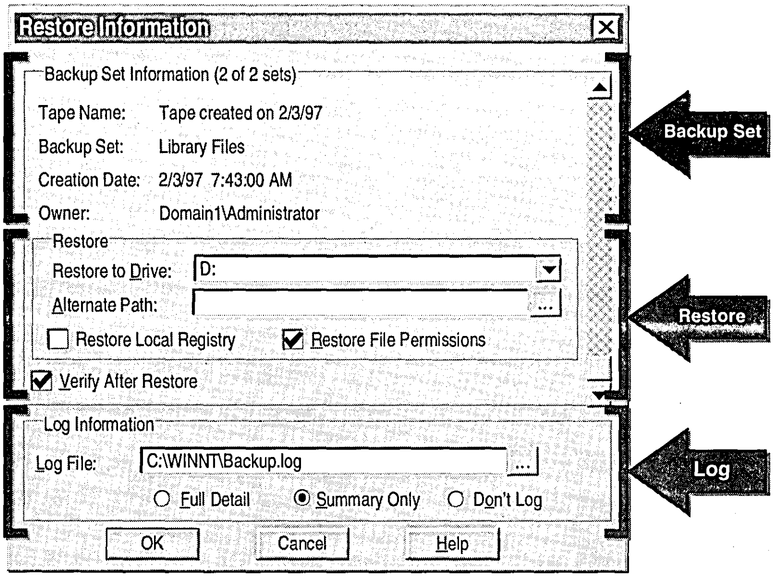
To select individual folders and files in a backup set, double-click the appropriate folder to expand it and then select the check boxes for the appropriate folders and files.

An X appears in the check box of the folder or file that you select, and in the boxes of the parent folder and disk drive. If you select only some of the folders and files on a disk drive or within a parent folder, then the check box appears dimmed.

Note You can select multiple folders or files by holding down the CTRL key and clicking the folders or files.

Setting Restore and Log Options

Once you have selected the folders and files to restore, the next step is to set the restore and log options. You can access the **Restore Information** dialog box by clicking **Restore** in the Backup window.



Restore Information

Backup Set Information (2 of 2 sets)

Tape Name: Tape created on 2/3/97

Backup Set: Library Files

Creation Date: 2/3/97 7:43:00 AM

Owner: Domain1\Administrator

Restore

Restore to Drive: D:

Alternate Path:

□ Restore Local Registry ☑ Restore File Permissions

☑ Verify After Restore

Log Information

Log File: C:\WINNT\Backup.log

○ Full Detail ● Summary Only ○ Don't Log

The following table describes the options under **Restore** and **Log Information** in the **Restore Information** dialog box.

Option	Description
Restore Local Registry	Restores the registry file. For the changes to the registry files to take effect, shut down and restart the computer.
Restore File Permissions	Restores the NTFS permissions. If not selected, files inherit the permissions of the folder to which they are restored. Do not restore file permissions if you restore to a computer that does not have the same user and group accounts.
Verify After Restore	Verifies the content of the files restored to disk against the files on the tape. Windows NT Backup logs exceptions.
Log File	The location of the text file for logging all tape operations. You can browse to find the correct name.
Full Detail	Logs all information on all restore operations including the names of all folders and files that were restored.
Summary Only	Logs only information about the major operations, such as loading a tape, starting to restore a file, and failing to restore a file.
Don't Log	Logs nothing.

Implementing the Restoration of Files

In this exercise, you use the Backup Simulation program to restore files from tape based on specific criteria. The Backup Simulation allows you to perform the following Windows NT Backup functions:

- Select a backup set and create a catalog
- Select a file to restore
- Set restore and log options

▶ To use the Backup.log file to locate the file to restore

In this procedure, you use the Backup.log file to determine the path to the Sven.doc file.

1. In Windows NT Explorer, expand the *systemroot* folder, and then double-click Backup.log to open it. (Backup.log may appear in Windows NT Explorer as Backup.)
2. Search Backup.log for Sven.doc, and write down its path. You will need it to restore the file.

   ____

3. Quit Notepad.

▸ To load the backup set catalog

This procedure requires that you have performed a backup using the Backup Simulation program and that the Backup Simulation program is still running. If you do not meet these requirements, complete all the procedures in Lesson 3 of this chapter, "Backing Up Files."

1. Click **Backup Simulation** on the taskbar to maximize the Backup Simulation window.

   The Tapes window is the active window.

   Note If you were using the actual Windows NT Backup program, you would start it by clicking the **Start** button, pointing to **Programs**, pointing to **Administrative Tools**, and then clicking **Backup**.

   ---

2. In the right pane of the Tapes window, double-click the backup set (the folder icon with the question mark [?] on it) to load the backup set catalog.

   A **Tape Created on** *date* dialog box appears. Notice that the catalog status information appears under **Summary**.

   Note The Backup Simulation creates only one backup set. Because of this fact, you need to load only a backup set catalog, and not a tape catalog.

   ---

3. When the cataloging operation is finished, click **OK**.

   The window for your backup set appears. Notice that the window name is the same as the name that you assigned to the tape.

▸ To select a file to restore

In this procedure, you restore the Sven.doc file to its original folder.

1. In the *tape_name* window, expand the folders to see the files on the tape. Notice that they are the same files that you selected to back up.
2. Locate Sven.doc and select its check box.
3. Click **Restore**.

   The **Restore Information** dialog box appears. Notice that Administrator is the owner of the tape. Only the owner of the tape, or a member of the Administrators or Backup Operators groups can restore files contained on the tape. This is because the Restrict Access to Owner or Administrator check box was selected when this tape was created.

▸ To set restore and log options

1. In the **Restore to Drive** box, type **d:** (if it does not already appear) to specify the location where Sven.doc will be restored.

   If you wanted to restore a file to a different drive and folder, you would specify the location in the **Alternative Path** box.

2. Select the **Verify After Restore** and **Restore File Permissions** check boxes to ensure that all files are restored without errors, and to guarantee that NTFS permissions assigned to the original backup files are correctly applied.
3. Under **Log Information**, make sure that **Full Detail** is selected so that the restored file and restore operation are added to the log.

▸ To start the restoration process

1. In the **Restore Information** dialog box, click **OK**.

   The Restore Status window appears with a summary of the restoration process, and then changes to a Verify Status window.

   If any files did not restore properly, information describing any problems would be described here.

2. When the restoration process is finished, click **OK**.

   The Backup Simulation window appears.

3. Quit the Backup Simulation program.
4. Log off.

Lesson Summary

The following information summarizes the key points in this lesson:

- A good data restoration strategy depends on creating a good backup strategy, keeping documentation of your backup, maintaining a regular backup schedule, storing tapes in a safe location, and performing trial restorations periodically.
- In networks where security is an issue, it is recommended that the user who restores files be different from the user who backs up files. You can give a user the ability to only restore files by assigning a user account to the Restore files and directories user right.
- Before you begin to restore files, connect to shared folders on remote computers where files will be restored.
- Load the tape and backup set catalogs for a list of all the files in a backup set. Use both of these catalogs to locate files to restore.
- If you restore files to a computer that does not have the same user and group accounts as the computer where the files originated, do not restore file permissions. The files will inherit the permissions of the folder to which they are restored.

For more information on	**See**
Restoring files	Chapter 6, "Backing Up and Restoring Network Files," in Microsoft Windows NT Server *Concepts and Planning*.
Comparing the restored files with the original files	The Windiff utility on the *Microsoft Windows NT Server Resource Kit CD-ROM*.

Best Practices

The following checklist provides best practices for backing up and restoring files. Review this checklist before you back up and restore files:

□ In minimum-security and medium-security networks, grant one user backup rights and a different user restore rights.

- Grant backup only rights by creating a local group named Backup Operators and then assigning the *Back up files and directories* user right to the group. Then, create a global group named Backup Only and add it to the local group.
- Grant restore only rights by creating a local group named Restore Operators and then assigning the *Restore files and directories* user right to the group. Then, create a global group named Restore Only and add it to the local group.
- Train personnel with restore rights to perform all of the restore tasks in the event that the administrator is unavailable.

Note In a high-security network, only administrators should restore files.

□ Back up an entire volume to prepare for the unlikely event of a disk failure. It is more efficient to restore the entire volume in one operation.

□ Always back up the registry on a domain controller to prevent the loss of user account and security information.

□ Always create and print a backup log for each backup. Keep a book of logs to make it easier to locate specific files.

□ Keep three copies of tapes. Keep at least one copy off-site in a properly controlled environment.

□ Perform a trial restoration periodically to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up with software verifications.

□ Secure both the tape drive and the backup tapes. Someone can access the data from a stolen tape by restoring the data to another server for which they are an administrator.

Note If you want to remove the accounts that were created by running the Chapter11.cmd file at the beginning of this chapter, log on as Administrator, and then double-click DeleteChapter11.cmd in the Cleanup folder on the Supplemental Material compact disc.

Review

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

1. Which of the following should you always back up?
   a. Temporary files
   b. Files critical to your organization
   c. Registry files
   d. Program files

2. Scenario: As administrator of the World Wide Importers network, you have been assigned the task of implementing a backup strategy for the Accounts Receivable server. Because there are only a few hours in the evening when the server is not in use, you need to be able to back up all files in the least amount of time possible. If files are lost, you need to be able to restore them from only two tapes. Which of the following is the best backup strategy for World Wide Importers?
   a. Do a normal backup Monday through Friday.
   b. Do a normal backup on Monday, and incremental backups Tuesday through Friday.
   c. Do a normal backup on Monday, and differential backups Tuesday through Friday.
   d. Do a daily copy Monday through Friday.
   e. Do a normal backup on Monday, and copy backups Tuesday through Friday.

3. Which of the following would ensure that your backup and restoration procedures are successful? (Circle all that apply.)
   a. Select the **Verify After Backup** check box when backing up files.
   b. Select the **Verify After Restore** check box when restoring files.
   c. Perform a trial restoration periodically, by restoring a recent backup to a drive other than the original drive, and then comparing the restored files to the files on the original drive.
   d. Select the **Restrict Access to Owner or Administrator** check box when backing up files.

4. Scenario: You want to create a local Backup Only Operators group. Which of the following user rights do you need to assigned to that group? (Circle all that apply.)

   a. Load and unload device drivers.

   b. Log on locally.

   c. Back up files and directories.

   d. Restore files and directories.

   e. Shutdown the system.

5. Scenario: You want to create a local restore operators groups. Which of the following user rights do you need to assign to that group? (Circle all that apply.)

   a. Load and unload device drivers.

   b. Log on locally.

   c. Back up files and directories.

   d. Restore files and directories.

   e. Shut down the system.

6. Scenario: You need to restore a particular file. You did a normal backup yesterday, but you forgot to create a backup log. How do you find the file?

   ____

   ____

7. Scenario: You need to restore the server data. The backup for the data consists of multiple tapes of which the last tape is damaged. What can you do?

   ____

   ____

Answer Key

Procedure Answers

Page 405

▸ **To plan a backup schedule**

Strategy used in planning worksheet (see Appendix A, "Backup Planning Worksheet"):

The tape drive is at the PDC to back up the registry. Tape storage can be two tapes on-site and one tape off-site.

All folders, except for Apps, are backed up daily because they contain files that change frequently or are critical.

The Apps folder is backed up weekly because it contains program files that change infrequently.

A normal backup is done on Monday and then a differential backup is done Tuesday through Friday so that if there is a catastrophic system failure, a minimal number of tapes will be required to perform a full restore. Monday's backup is archived because it contains a copy of all files. The backups done on Tuesday through Friday are on the same tape.

A Full Detail backup log is created so that all backup events are recorded.

Page 420

Example of a Scheduled Backup

1. What tasks will this batch file perform?

   The batch file connects to \\Computer1\Public as User11 (from Domain1), and then performs an incremental backup of drives C, D, and X; of the shared folder Public on Server1; and of the local registry.

   It also verifies that the files were backed up correctly, uses hardware compression, and then records the results in the log file named C:\Weekly.log. It also disconnects from the two remote shared folders.

2. What would you add to this batch file to make it easier to identify the contents of the tape that this batch file creates?

   Add the /d option with a complete description of the backup set. For example: /d "Incremental backup of drives C, D, X, \\Server1\Public, and the registry"

3. What command would you add to the batch file to back up files (owned by the Administrators group) in the Data folder on a computer named Server2?

   Add the UNC path \\Server2\Data after the command ntbackup backup—for example, type: ntbackup backup \\server2\data

Page 420

▸ **To write a batch file to back up data**

Possible answer 1:

```
net use e: \\sales\customerdata

net use f: \\bdc\ardata

ntbackup backup e: f: /t differential /a /HC:off /v /d "Customer Data" /l
"Tuesday.log"

net use e: /delete

net use f: /delete
```

Possible answer 2:

```
ntbackup backup \\sales\customerdata \\bdc\ardata /t differential /a
/HC:off /v /d "Customer Data"
/l "Tuesday.log"
```

Page 434

▸ **To use the Backup.log file to locate the file to restore**

2. Search Backup.log for Sven.doc, and write down its path. You will need it to restore the file.

   D:\Data\Managers\Sven.doc

Page 439

Review Answers

1. Which of the following should you always back up?

   Answers b and c are correct.

2. Scenario: As administrator of the World Wide Importers network, you have been assigned the task of implementing a backup strategy for the Accounts Receivable server. Because there are only a few hours in the evening when the server is not in use, you need to be able to back up all files in the least amount of time possible. If files are lost, you need to be able to restore them from only two tapes. Which of the following is the best backup strategy for World Wide Importers?

   Answer c would be the best strategy.

3. Which of the following would ensure that your backup and restoration procedures are successful? (Circle all that apply.)

   Answers a, b, and c are correct.

4. Scenario: You want to create a local Backup Only Operators group. Which of the following user rights do you need to assigned to that group? (Circle all that apply.)

   Answers b and c are correct.

5. Scenario: You want to create a local restore operators groups. Which of the following user rights do you need to assign to that group? (Circle all that apply.)

   Answers b, d, and e are correct.

6. Scenario: You need to restore a particular file. You did a normal backup yesterday, but you forgot to create a backup log. How do you find the file?

   First load the tape catalog to determine the appropriate backup set. Then, load the backup set catalog, which shows all the folders and files in the backup set.

7. Scenario: You need to restore the server data. The backup for the data consists of multiple tapes of which the last tape is damaged. What can you do?

   You can force Windows NT Backup to treat the data on the remaining tapes as a single unit by starting Windows NT Backup at the command prompt and including the /missingtape option.

APPENDIX A

Planning Worksheets

User Accounts Planning Worksheet

Naming Convention: First name + Last Initial + Additional Characters

Full Name	User Account	Description	Password Requirements	Home Folder Location	Logon Hours	Workstation Restrictions
Linda Mitchell	VicePresident	Vice president	User Must Change Password at Next Logon	Server	All	N
	Director	Director of human resources	User Must Change Password at Next Logon	Server	All	N
	SalesMgr	Sales manager	User Must Change Password at Next Logon	Server	All	N
	SalesRep	Sales representative	User Must Change Password at Next Logon	Server	All	N
Linda Mitchell	CustomerService1	Customer service representative (night shift)	User Must Change Password at Next Logon	Server	6 P.M.–6 A.M. (7 days)	N
	CustomerService2	Customer service representative (day shift)	User Must Change Password at Next Logon	Server	All	N
	AccountingMgr	Accounting manager	User Must Change Password at Next Logon	Server	All	N
	Accountant	Accountant	User Must Change Password at Next Logon	Server	All	N
	Temp	Temporary employee	User Cannot Change Password	Server	8 A.M.–5 P.M. (7 days)	Y

Group Accounts Planning Worksheet

Group Account	Local or Global	Members	Location
Executives	Global	VicePresident3, Director3	PDC (in both domains)
Managers	Global	SalesMgr3, AccountingMgr3	PDC (in both domains)
Customer Service	Global	CustomerService3-A, CustomerService3-B	PDC (in both domains)
Sales	Global	SalesMgr3, SalesRep3	PDC (in both domains)
Accountants	Global	AccountingMgr3, Accountant3	PDC (in both domains)
Istanbul\Domain Users*	Global	VicePresident3, Director3, SalesMgr3, SalesRep3, CustomerService3-A, CustomerService3-B, AccountingMgr3, Accountant3, and Temp3 (all user accounts)	PDC (in the Istanbul domain)
Quebec\Domain Users*	Global	VicePresident3, Director3, SalesMgr3, SalesRep3, CustomerService3-A, CustomerService3-B, AccountingMgr3, Accountant3, and Temp3 (all user accounts)	PDC (in the Quebec domain)
Programs	Local	Istanbul\Domain Users*	Member Server1 (in the Istanbul domain)
Programs	Local	Quebec\Domain Users*	Member Server1 (in the Quebec domain)
Printer	Local	Istanbul \Domain Users* and Quebec\Domain Users*	PDC (in the Istanbul domain)
HR	Local	Global groups: Executives3 and Managers3 (from both domains)	BDC (in the Quebec domain)
Customer Files	Local	Global groups: Executives3, Managers3, Customer Service3, and Sales3 (from both domains)	Member Server2 (in the Quebec domain)
AR	Local	Global group: Accountants3 (from both domains)	PDC (in the Quebec domain)
Employee Files	Local	Global group: Managers3 (from both domains)	Windows NT Workstation (in the Istanbul domain)

*Domain Users is a built-in global group that contains all domain user accounts by default. You can either create a global group and add all domain user accounts or you can use the built-in group Domain Users.

Shared Folders Planning Worksheet

Folder Name	UNC Name	Local Group	Members	Share Permissions
Apps	\\Server3\Apps	Users Administrators	Default members Default members	Read Full Control
ProjMan	\\Server3\ProjMan	Project Managers Administrators	Managers global group Default members	Change Full Control
Data	\\Server2\Data	Data Access	Executives global group	Read
Acctng	\\Server2\Account	Accounting Access	Accountants global group	Full Control
HR	\\Server2\HR	HR Access	HR global group	Full Control
Reviews	\\Server2\Reviews	Reviews Users Administrators	Managers and Executives global groups Default members Default members	Change Read Full Control
Users	\\Server1\Users	Administrators	Default members	Full Control
User1 User2 User3	\\Server1\User1 \\Server1\User2 \\Server1\User3	None None None		User1: Full Control User2: Full Control User3: Full Control

NTFS Permissions Planning Worksheet

Folder or File	Local Group	Members	NTFS Permissions
Apps	Administrators Users	Default members Default members	Full Control Read
Apps\Wordproc	Administrators Users	Default members Default members	Full Control Read
Apps\Spreadsh	Administrators Spreadsheet6	Default members Global groups: Accountants6, Managers6, and Executives6	Full Control Read
Apps\Database	Administrators Database6	Default members Global groups: Accountants6, Managers6, and Executives6	Full Control Read
Public	Administrators Users Creator Owner (system group)	Default members Default members Users who copy or create a file in the Public folder	Full Control Add & Read Full Control
Public\Library	Administrators Users Library6	Default members Default members Global group: Managers6	Full Control Read Change
Public\Library\Archive.txt			User6: Add & Read
Public\Manuals	Administrators Users	Default members Default members	Full Control Read User 6: Full Control

Backup Planning Worksheet

Tape Drive Location: Primary domain controller **Tape Storage Location**: Two tapes on-site, one tape off-site

Folders and Files to Back Up (Provide Path)	Daily	Weekly (Provide Day)
(PDC) D:\Users\*.*	X	
(PDC) Registry	X	
(BDC) D:\ARData\*.*	X	
(BDC) D:\HRData\*.*	X	
(Member Server1) C:\Apps\*.*		Every Monday
(Member Server2) D:\CustomerData\*.*	X	

Weekly Backup Schedule

Monday	Tuesday	Wednesday	Thursday	Friday
Backup Type: **N** Tape: **1** Archive Y_✓_N__	Backup Type: **D** Tape: **2** Archive Y__N_✓_	Backup Type: **D** Tape: **2** Archive Y__N_✓_	Backup Type: **D** Tape: **2** Archive Y__N_✓_	Backup Type: **D** Tape: **2** Archive Y__N_✓_

Backup Types

N = Normal D = Differential I = Incremental C = Copy DC = Daily Copy

Type of Backup Log

☑ Full Detail ☐ Summary Only ☐ Don't Log

Glossary

A

access 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* user rights.

access privileges Permissions set by Macintosh users that allow them to view and make changes to folders on a server. By setting access privileges (called *permissions* when set on the computer running Windows NT Server), you control which Macintosh can use folders in a volume. Services for Macintosh (SFM) translates access privileges set by Macintosh users to the equivalent Windows NT permissions.

access token (or security token) An object that uniquely identifies a user who has logged on. An access token is attached to all the user's processes and contains the user's security ID (SID), the SIDs of any groups to which the user belongs, any permissions that the user owns, the default owner of any objects that the user's processes create, and the default access control list (ACL) to be applied to any objects that the user's processes create. *See also* permissions.

account *See* group account; user account.

account lockout A Windows NT Server security feature that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on account policy lockout settings. (Locked accounts cannot log on.)

account policy Controls the way passwords must be used by all user accounts of a domain or of an individual computer. Specifics include minimum password length, how often a user must change his or her password, and how often users can reuse old passwords. Account policy can be set for all user accounts in a domain when administering a domain, and for all user accounts of a single workstation or member server when administering a computer.

active Refers to the window or icon that you are currently using or that is currently selected. Windows NT always applies the next keystroke or command you choose to the active window. If a window is active, its title bar changes color to differentiate it from other windows. If an icon is active, its label changes color. Windows or icons on the desktop that are not selected are inactive.

adapter card *See* network adapter.

administrative account An account that is a member of the Administrators local group of a computer or domain.

administrative alerts Administrative alerts relate to server and resource use and warn about problems in areas such as security and access, user sessions, server shutdown due to 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; uninterruptible power supply (UPS).

administrator A person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking issues. To use administrative tools such as User Manager or User Manager for Domains, an administrator must be logged on as a member of the Administrators local group for the computer or domain, respectively.

Administrator privilege One of three privilege levels you can assign to a Windows NT user account. Every user account has one of the three privilege levels (Administrator, Guest, and User). *See also* administrator; Guest privilege; User privilege.

Alerter service Notifies selected users and computers of administrative alerts that occur on a computer. Used by the Server service and other services. Requires the Messenger service. *See also* administrative alerts; Messenger service.

API *See* application programming interface.

application A computer program used for a particular kind of work, such as word processing. This term is often used interchangeably with "program."

application log The application log contains specific events logged by programs. Programs developers decide which events to monitor (for example, a database program might record a file error in the application log). Use Event Viewer to view the application log.

application programming interface (API) A set of routines that a program uses to request and carry out lower-level services performed by another component, such as the computer's operating system or a service running on a network computer. These maintenance chores are performed by the computer's operating system, and an API provides the program with a means of communicating with the system, telling it which system-level task to perform and when.

application window The main window for a program, which contains the program's menu bar and work area. A program window may contain multiple document windows.

archive bit Backup programs use the archive bit to mark the files after backing them up, if a normal or incremental backup is performed. *See also* backup types.

ASCII file Also called a text file, a text-only file, or an ASCII text file, refers to a file in the universally recognized text format called ASCII (American Standard Code for Information Interchange). An ASCII file contains characters, spaces, punctuation, carriage returns, and sometimes tabs and an end-of-file marker, but it contains no formatting information. This generic format is useful for transferring files between programs that could not otherwise understand each other's documents. *See also* text file.

associate To identify a file name extension as "belonging" to a certain program so that when you open any file with that extension, the program starts automatically.

attributes Information that indicates whether a file is a read-only, hidden, system, or compressed file, and whether the file has been changed since a backup copy of it was made.

auditing Tracking activities of users by recording selected types of events in the security log of a server or a workstation.

Audit policy For the servers of a domain or for an individual computer, defines the type of security events that will be logged.

authentication Validation of a user's logon information. When a user logs on to an account on a computer running Windows NT Workstation, the authentication is performed by that workstation. When a user logs on to an account on a Windows NT Server domain, authentication may be performed by any server of that domain. *See also* server; trust relationship.

B

backup domain controller (BDC) In a Windows NT Server domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). BDCs also authenticate user logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist on a domain. *See also* member server; primary domain controller (PDC).

backup set A collection of files from one drive that is backed up during a single backup operation.

backup set catalog At the end of each backup set, Windows NT Backup stores a summary of file and/or directory information in a backup set catalog. Catalog information includes the number of tapes in a set of tapes as well as the date they were created and the dates of each file in the catalog. Catalogs are created for each backup set and are stored on the last tape in the set. *See also* backup set.

backup set map At the end of each tape used for backup, a backup set map maintains the exact tape location of the backup set's data and catalog.

backup types:

copy backup Copies all selected files, but does not mark each file as having been backed up. Copying is useful if you want to back up files between normal and incremental backups, because copying will not invalidate these other backup operations.

daily backup Copies all selected files that have been modified the day that the daily backup is performed.

differential backup Copies those files created or changed since the last normal (or incremental) backup. It does not mark files as having been backed up.

incremental backup Backs up only those files created or changed since the last normal (or incremental) backup. It marks files as having been backed up.

normal backup Copies all selected files and marks each as having been backed up. Normal backups give you the ability to restore files quickly because files on the last tape are the most current.

batch program An ASCII file (unformatted text file) that contains one or more Windows NT commands. A batch program's file name has a .cmd or .bat extension. When you type the file name at the command prompt, the commands are processed sequentially.

BDC *See* backup domain controller.

bits per second (bps) A measure of the speed at which a device, such as a modem, can transfer data.

blue screen The screen displayed when Windows NT encounters a serious error.

boot partition The volume, formatted for either an NTFS or FAT file system, that contains the Windows NT operating system and its support files. The boot partition can be (but does not have to be) the same as the system partition. *See also* file allocation table (FAT); partition; Windows NT file system (NTFS).

bps *See* bits per second.

browse To view available network resources by looking through lists of folders, files, user accounts, groups, domains, or computers. Browsing allows users on a Windows NT network to see what domains and computers are accessible from their local computer.

browse list A list kept by the master browser of all of the servers and domains on the network. This list is available to any workstation on the network requesting it. *See also* browse.

built-in groups Default groups, provided with Windows NT Workstation and Windows NT Server, that have been granted useful collections of rights and built-in abilities. In most cases, a built-in group provides all of 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 of the domain. To provide 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

cache A special memory subsystem that stores the contents of frequently accessed RAM locations and the addresses where these data items are stored. In Windows NT, for example, user profiles have a locally cached copy of part of the registry.

catalog *See* backup set catalog.

centralized network administration A centralized view of the entire network from any workstation on the network that provides the ability to track and manage information on users, groups, and resources in a distributed network.

check box A small box in a dialog box or property page that can be selected or cleared. Check boxes represent an option that you can turn on or off. When a check box is selected, an X or a check mark appears in the box.

Chooser The Macintosh desk accessory with which users select the network server and printers that they want to use.

clear To turn off an option by removing the X or check mark from a check box. To clear a check box, you can click it, or you can select it and then press the SPACEBAR.

click To press and release a mouse button quickly.

client A computer that accesses shared network resources provided by another computer, called a server. *See also* server; workstation.

client application A Windows NT application that can display and store linked or embedded objects. For distributed applications, the program that imitates a request to a server application. *See* Distributed Component Object Module (DCOM); server application.

Client Service for NetWare Included with Windows NT Workstation, enabling workstations to make direct connections to file and printer resources at NetWare servers running NetWare 2.*x* or later.

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 program.

close Remove a window or dialog box, or quit a program. To close a window, you can click **Close** on the **Control** menu, or you can click the close button icon in the upper right corner of the dialog box. When you close an application window, you quit the program.

collapse To hide additional directory levels below a selected directory in the directory tree.

command A word or phrase, usually found on a menu, that you click to carry out an action. You click a command on a menu or type a command at the Windows NT command prompt. You can also type a command in the **Run** dialog box, which you open by clicking **Run** on the **Start** menu.

command button A button in a dialog box that carries out or cancels the selected action. Two common command buttons are **OK** and **Cancel.** If you click a command button that contains an ellipsis (for example, **Browse...**), another dialog box appears.

common group Common groups appear in the program list on the **Start** menu for all users who log on to the computer. Only Administrators can create or change common groups.

communications settings Settings that specify how information is transferred from your computer to a device (usually a printer or modem).

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

Computer Browser service Maintains an up-to-date list of computers, and provides the list to programs when requested. Provides the computer lists displayed in the **Network Neighborhood, Select Computer**, and **Select Domain** dialog boxes; and (for Windows NT Server only) 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.

configure To change the initial setup of a client, a Macintosh-accessible volume, a server, or a network.

connect To assign a drive letter, port, or computer name to a shared resource so that you can use it with Windows NT.

connected user A user accessing a computer or a resource across the network.

connection A software link between a client and a shared resource such as a printer or a shared directory on a server. Connections require a network adapter or modem.

controller *See* backup domain controller (BDC); primary domain controller (PDC).

conventional memory Up to the first 640 KB of memory in your computer. MS-DOS uses this memory to run programs.

current directory The directory that you are currently working in. Also called "current folder."

D

default button In some dialog boxes, the command button that is selected or highlighted when the dialog box is initially displayed. The default button has a bold border, indicating that it will be chosen automatically if you press ENTER. To override a default button, you can click **Cancel** or another command button.

default gateway In TCP/IP, the intermediate network device on the local network that has knowledge of the network IDs of the other networks in the Internet, so it can forward the packets to other gateways until the packet is eventually delivered to a gateway connected to the specified destination. *See also* gateway.

default owner The person assigned ownership of a folder on the server when the account of the folder or volume's previous owner expires or is deleted. Each server has one default owner; you can specify the owner.

default printer The printer that is used if you choose the **Print** command without first specifying which printer you want to use with a program. 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.

default user Every user profile begins as a copy of *default user*, which is a default user profile stored on each computer running Windows NT Workstation or Windows NT Server.

dependent service A service that requires support of another service. For example, the Alerter service is dependent on the Messenger service. *See also* Alerter service; Messenger service.

desktop The background of your screen, on which windows, icons, and dialog boxes appear.

desktop pattern A design that appears across your desktop. You can create your own pattern or select a pattern provided by Windows NT.

destination directory The directory to which you intend to copy or move one or more files.

device Any piece of equipment that can be attached to a network—for example, a computer, a printer, or any other peripheral equipment.

device driver A program that enables a specific piece of hardware (device) to communicate with Windows NT. Although a device may be installed on your system, Windows NT cannot recognize the device until you have installed and configured the appropriate driver. If a device is listed in the Hardware Compatibility List, a driver is usually included with Windows NT. Drivers are installed when you run the Setup program (for a manufacturer's supplied driver) or by using Devices in Control Panel. *See also* Hardware Compatibility List (HCL).

DHCP *See* Dynamic Host Configuration Protocol.

dialog box A window that is displayed to request or supply information. Many dialog boxes have options that you must select before Windows NT can carry out a command.

dial-up line A standard dial-up connection such as telephone and ISDN lines.

dial-up networking The client version of Windows NT Remote Access Service (RAS), enabling users to connect to remote networks.

directory Part of a structure for organizing your files on a disk, a directory (also called a folder) is represented by the folder icon in Windows NT, Windows 95, and on Macintosh computers. A directory can contain files and other directories, called subdirectories or folders within folders.

With Services for Macintosh, directories on the computer running Windows NT Server appear to Macintosh users as volumes and folders if they are designated as Macintosh accessible.

See also directory tree; folder.

directory database A database of security information such as user account names and passwords, and the security policy settings. For Windows NT Workstation, the directory database is managed by using User Manager. For a Windows NT Server domain, it is managed by using User Manager for Domains. (Other Windows NT documents may refer to the directory database as the "Security Accounts Manager (SAM) database.") *See also* Windows NT Server Directory Services.

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 when they are added to an exported directory and every time 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 services *See* Windows NT Server Directory Services.

directory tree A graphical display of a disk's directory hierarchy. The directories and folders on the disk are shown as a branching structure. The top-level directory is the root directory.

disabled user account A user account that does not permit logons. The account appears in the user account list of the User Manager or User Manager for Domains window and can be re-enabled at any time. *See also* user account.

Distributed Component Object Model (DCOM) Use the DCOM Configuration tool to integrate client/server applications across multiple computers. DCOM can also be used to integrate robust Web browser applications. *See also* DCOM Configuration tool.

DLL *See* dynamic-link library.

document A self-contained file created with a program and, if saved on disk, given a unique file name by which it can be retrieved. A document can be a text file, a spreadsheet, or an image file, for example.

document file A file that is associated with a program. When you open a document file, the program starts and loads the file. *See also* associate.

Document file icon Represents a file that is associated with a program. When you double-click a document file icon, the program starts and loads the file. *See also* associate.

document icon Located at the left of a document window title bar, the document icon represents the open document. Clicking the document icon opens the window menu. Also known as the control menu box.

domain In Windows NT, a collection of computers, defined by the administrator of a Windows NT Server network, that share a common directory database. A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name. *See also* directory database; user account; workgroup.

domain controller In a Windows NT Server domain, refers to the computer running Windows NT Server that manages all aspects of user-domain interactions, and uses information in the directory database to authenticate users logging on to domain accounts. One shared directory database is used to store security and user account information for the entire domain. A domain has one primary domain controller (PDC) and one or more backup domain controllers (BDCs). *See also* backup domain controller (BDC); directory database; member server; primary domain controller (PDC).

domain database *See* directory database.

domain model A grouping of one or more domains with administration and communication links between them that are arranged for the purpose of user and resource management.

domain synchronization *See* synchronize.

double-click To rapidly press and release a mouse button twice without moving the mouse. Double-clicking carries out an action, such as starting a program.

down level A term that refers to earlier operating systems, such as Windows for Workgroups or LAN Manager, that can still interoperate with Windows NT Workstation or Windows NT Server.

drag To move an item on the screen by selecting the item and then pressing and holding down the mouse button while moving the mouse. For example, you can move a window to another location on the screen by dragging its title bar.

drive icon An icon in the All Folders column in Windows NT Explorer or the Names Column in My Computer 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.

driver *See* device driver.

dual boot A computer that can boot two different operating systems. *See also* multiple boot.

Dynamic Host Configuration Protocol (DHCP) A protocol that offers dynamic configuration of IP addresses and related information. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of IP addresses through centralized management of address allocation. *See also* IP address.

dynamic-link library (DLL) An operating system feature that allows executable routines (generally serving a specific function or set of functions) to be stored separately as files with .dll extensions and to be loaded only when needed by the program that calls them.

E

EISA *See* Extended Industry Standard Architecture.

embedded object Presents information, created in another program, which has been pasted inside your document. Information in the embedded object does not exist in another file outside of your document.

EMS *See* Expanded Memory Specification.

encapsulated PostScript (EPS) file A file that prints at the highest possible resolution for your printer. An EPS file may print faster than other graphical representations. Some Windows NT and non-Windows NT graphical programs can import EPS files. *See also* PostScript printer; print processor.

encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.

enterprise server Refers to the server to which multiple primary domain controllers (PDCs) in a large organization will replicate. *See also* primary domain controller (PDC).

environment variable A string consisting of environment information, such as a drive, path, or file name, associated with a symbolic name that can be used by Windows NT. To define environment variables, use System in Control Panel or use the **set** command from the Windows NT command prompt.

EPS *See* encapsulated PostScript file.

error logging The process by which errors that cannot readily be corrected by the majority of end users are written to a file instead of being displayed on the screen. System administrators, support technicians, and users can use this log file to monitor the condition of the hardware in a computer running Windows NT to tune the configuration of the computer for better performance, and to debug problems as they occur.

event Any significant occurrence in the system or a program 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. The Event Log service is located in Event Viewer.

expand To show hidden directory levels in the directory tree. With My Computer or Windows NT Explorer, directories that can expand have plus-sign icons which you click to expand.

expanded memory A type of memory, up to 8 megabytes, that can be added to an 8086 or 8088 computer, or to an 80286, 80386, 80486, or Pentium computer. The use of expanded memory is defined by the Expanded Memory Specification (EMS). Note: Windows NT requires an 80486 or higher computer.

Expanded Memory Specification (EMS) Describes a technique for adding memory to IBM PC systems. EMS bypasses the limits on the maximum amount of usable memory in a computer system by supporting memory boards containing a number of 16 KB banks of RAM that can be enabled or disabled by software. *See also* memory.

Explorer *See* Windows NT Explorer.

Extended Industry Standard Architecture (EISA) A 32-bit bus standard introduced in 1988 by a consortium of nine computer industry companies. EISA maintains compatibility with the earlier Industry Standard Architecture (ISA) but provides for additional features.

extended memory Memory beyond one megabyte in 80286, 80386, 80486, and Pentium computers. Note: Windows NT requires an 80486 or higher computer.

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 needs to be present to create an extended partition. *See also* free space; logical drive; primary partition.

extension A file name extension usually indicates the type of file or directory, or the type of program associated with a file. In MS-DOS, this includes a period and up to three characters at the end of a file name. Windows NT supports long file names, up to the file name limit of 255 characters.

extension-type association The association of an MS-DOS file name extension with a Macintosh file type and file creator. Extension-type associations allow users of the PC and Macintosh versions of the same program to share the same data files on the server. Services for Macintosh has many predefined extension-type associations. *See also* name mapping.

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. *See also* backup set.

FAT *See* file allocation table.

fault tolerance Ensures data integrity when hardware failures occur. In Windows NT, fault tolerance is provided by the Ftdisk.sys driver. In Disk Administrator, fault tolerance is provided using mirror sets, stripe sets with parity, and volume sets.

file A collection of information that has been given a name and is stored on a disk. This information can be a document or a program.

file allocation table (FAT) 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. Also referred to as the FAT file system.

File and Print Services for NetWare (FPNW) A Windows NT Server component that enables a computer running Windows NT Server to provide file and print services directly to NetWare-compatible client computers.

file name The name of a file. MS-DOS supports the 8.3 naming convention of up to eight characters followed by a period and a three-character extension. Windows NT supports the FAT and NTFS file systems with file names up to 255 characters. Since MS-DOS cannot recognize long file names, Windows NT Server automatically translates long names of files and folders to 8.3 names for MS-DOS users. *See also* long name; name mapping; short name.

file name extension The characters that follow the period in a file name, following the FAT naming conventions. File name extensions can have as many as three characters and are often used to identify the type of file and the program used to create the file (for example, spreadsheet files created by Microsoft Excel have the extension .xls). With Services for Macintosh, you can create extension-type associations that map PC file name extensions with Macintosh file creators and types.

File Replication service A Windows NT service that allows specified file(s) to be replicated to remote systems, ensuring that copies on each system are kept in synchronization. The system that maintains the master copy is called the exporter, and the systems that receive updates are known as importers.

file sharing The ability for a computer running Windows NT to share parts (or all) of its local file system(s) with remote computers. An administrator creates share points by using the file sharing command in My Computer or Windows NT Explorer or by using the **net share** command from the command prompt.

file system In an operating system, the overall structure in which files are named, stored, and organized. NTFS and FAT are types of file systems.

find tab Displays the words you can use to search for related topics. Use this tab to look for topics related to a particular word. It is located in the Help button bar near the top of the Help window.

floppy disk A disk that can be inserted in and removed from a disk drive. Floppies are most commonly available in a 3.5 or 5.25 inch format.

folder A grouping of files or other folders, graphically represented by a folder icon, in both the Windows NT and Macintosh environments. A folder is analogous to a PC's file system directory, and many folders are, in fact, directories. A folder may contain other folders as well as file objects. *See also* directory.

font A graphic design applied to a collection of numbers, symbols, and characters. A font describes a certain typeface along with other qualities such as size, spacing, and pitch.

FPNW *See* File and Print Services for NetWare.

free space Free space is an unused and unformatted portion of a hard disk that can be partitioned or subpartitioned. Free space within an extended partition is available for the creation of logical drives. Free space that is not within an extended partition is available for the creation of a partition, with a maximum of four partitions allowed per disk. *See also* extended partition; logical drive; primary partition.

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 and User Manager for Domains as part of the information identifying and defining a user account. *See also* user account.

full-screen application A non–Windows NT application that is displayed in the entire screen, rather than a window, when running in the Windows NT environment.

full synchronization Occurs when a copy of the entire database directory is sent to a backup domain controller (BDC). Full synchronization is performed automatically when changes have been deleted from the change log before replication takes place, and when a new BDC is added to a domain. *See also* backup domain controller (BDC); directory database.

G

gateway Describes a system connected to multiple physical TCP/IP networks, capable of routing or delivering IP packets between them. A gateway translates between different transport protocols or data formats (for example IPX and IP) and is generally added to a network primarily for its translation ability. Also referred to as an IP router. *See also* IP address; IP router.

global account For Windows NT Server, a normal user account in a user's 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 through the establishment of domain trust relationships. *See also* local account; trust relationship.

global group For Windows NT Server, a group that can be used in its own domain, member servers and workstations of the domain, and trusting domains. In all those places it can be granted rights and permissions and can become a member of local groups. However, it can only contain user accounts from its own domain. Global groups provide a way to create handy sets of users from inside the domain, available for use both in and out of the domain.

Global groups cannot be created or maintained on computers running Windows NT Workstation. However, for Windows NT Workstation computers 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* domain; group; local group; trust relationship.

group In User Manager or User Manager for Domains, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members, making groups a convenient way to grant common capabilities to collections of user accounts. For Windows NT Workstation, 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 account A collection of user accounts. Giving a user account membership in a group gives that user all the rights and permissions granted to the group. *See also* local account; user account.

group category One of three categories of users to which you can assign Macintosh permissions for a folder. The permissions assigned to the group category are available to the group associated with the folder.

group memberships The groups to which a user account belongs. Permissions and rights granted to a group are also provided 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 the user is logged on to. *See also* group.

group name A unique name identifying a local group or a global group to Windows NT. A group's name cannot be identical to any other group name or user name of its own domain or computer. *See also* global group; local group.

guest Users of Services for Macintosh who do not have a user account or who do not provide a password are logged on as a guest, using a user account with guest privileges. When a Macintosh user assigns permissions to everyone, those permissions are given to the group's guests and users.

guest account On computers running Windows NT Workstation or Windows NT Server, a built-in account used for logons by people who do not have a user account on the computer or domain or in any of the domains trusted by the computer's domain.

Guest privilege One of three privilege levels that you can assign to a Windows NT user account. The guest account used for Macintosh guest logons must have the Guest privilege. *See also* Administrator privilege; user account; User privilege.

H

Hardware Compatibility List (HCL) The Windows NT Hardware Compatibility List lists the devices supported by Windows NT. The latest version of the HCL can be downloaded from the Microsoft Web Page (microsoft.com) on the Internet.

HCL *See* Hardware Compatibility List.

heterogeneous environment An internetwork with servers and workstations running different operating systems, such as Windows NT, Macintosh, or Novell NetWare, using a mix of different transport protocols.

high memory area (HMA) The first 64 KB of extended memory (often referred to as HMA). *See also* memory.

High-Performance File System (HPFS) The file system designed for the OS/2 version 1.2 operating system.

HMA *See* high memory area.

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. Also referred to as a home folder.

home folder *See* home directory.

home page The initial page of information for a collection of pages. The starting point for a Web site or section of a Web site is often referred to as the home page. Individuals also post pages that are called home pages.

HPFS *See* High-Performance File System.

HTML *See* Hypertext Markup Language.

HTTP *See* Hypertext Transport Protocol.

hyperlink A way of jumping to another place on the Internet. Hyperlinks usually appear in a different format from regular text. You initiate the jump by clicking the link.

Hypertext Markup Language (HTML) A simple markup language used to create hypertext documents that are portable from one platform to another. HTML files are simple ASCII text files with codes embedded (indicated by markup tags) to indicate formatting and hypertext links. HTML is used for formatting documents on the World Wide Web.

Hypertext Transport Protocol (HTTP) The underlying protocol by which WWW clients and servers communicate. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

I

icon A graphical representation of an element in Windows NT, such as a disk drive, directory, group, program, or document. Click the icon to enlarge a program icon to a window when you want to use the program. Within programs, there are also toolbar icons for commands such as cut, copy, and paste.

IIS *See* Internet Information Server.

insertion point The place where text will be inserted when you type. The insertion point usually appears as a flashing vertical bar in a program's window or in a dialog box.

Integrated Services Digital Network (ISDN) A type of phone line used to enhance WAN speeds, ISDN lines can transmit at speeds of 64 or 128 kilobits per second, as opposed to standard phone lines, which typically transmit at only 9600 bits per second (bps). An ISDN line must be installed by the phone company at both the server site and the remote site. *See also* bits per second (bps).

internal command Commands that are stored in the file Cmd.exe and that reside in memory at all times.

internet In Windows NT, a collection of two or more private networks, or private inter-enterprise TCP/IP networks.

In Macintosh terminology, refers to two or more physical networks connected by routers, which maintain a map of the physical networks on the internet and forward data received from one physical network to other physical networks. Network users in an internet can share information and network devices. You can use an internet with Services for Macintosh by connecting two or more AppleTalk networks to a computer running Windows NT Server.

Internet The global network of networks. *See also* World Wide Web (WWW).

Internet Information Server (IIS) A network file and application server that supports multiple protocols. Primarily, Internet Information Server transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

Internet service provider (ISP) A company or educational institution that enables remote users to access the Internet by providing dial-up connections or installing leased lines.

internetworks Networks that connect local area networks (LANs) together.

interprocess communication (IPC) The ability, provided by a multitasking operating system, of one task or process to exchange data with another. Common IPC methods include pipes, semaphores, shared memory, queues, signals, and mailboxes. *See also* named pipe; queue.

intranet A TCP/IP network that uses Internet technology. May be connected to the Internet. *See also* Internet; Transmission Control Protocol/Internet Protocol (TCP/IP).

IP address Used to identify a node on a network and to specify routing information. Each node on the network must be assigned a unique IP address, which is made up of the *network ID*, plus a unique *host ID* assigned by the network administrator. This address is typically represented in dotted-decimal notation, with the decimal value of each octet separated by a period (for example, 138.57.7.27).

In Windows NT, the IP address can be configured statically on the client or configured dynamically through DHCP. *See also* Dynamic Host Configuration Protocol (DHCP).

IPC *See* interprocess communication.

IP router A system connected to multiple physical TCP/IP networks that can route or deliver IP packets between the networks. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

IPX *See* IPX/SPX.

IPX/SPX Acronym for Internetwork Packet Exchange/Sequenced Packet Exchange, which is a set of transport protocols used in Novell NetWare networks. Windows NT implements IPX through NWLink.

ISDN *See* Integrated Services Digital Network.

ISP *See* Internet service provider.

J

jump Text, graphics, or parts of graphics that provide links to other Help topics or to more information about the current topic. The pointer changes shape whenever it is over a jump. If you click a jump that is linked to another topic, that topic appears in the Help window. If you click a jump that is linked to more information, the information appears in a pop-up window on top of the main Help window.

L

LAN *See* local area network.

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 these changes.

list box In a dialog box, a type of box that lists available choices—for example, a list of all 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; trust relationship; user account.

local area network (LAN) A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

local group For Windows NT Workstation, a group that can be granted permissions and rights only for its own workstation. However, it 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.

For Windows NT Server, a group that can be granted permissions and rights only for the domain controllers 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 domain controllers of the domain. *See also* global group; group; trust relationship.

local guest logon Takes effect when a user logs on interactively at a computer running Window NT Workstation or at a member server running Windows NT Server, and specifies Guest as the user name in the **Logon Information** dialog box.

local printer A printer that is directly connected to one of the ports on your computer. *See also* port.

local user profiles User profiles that are created automatically on the computer at logon the first time a user logs on to a computer running Windows NT Workstation or Windows NT Server.

log books Kept by the system administrator to record the backup methods, dates, and contents of each tape in a backup set. *See also* backup set; backup types.

log files Created by Windows NT Backup and contain a record of the date the tapes were created and the names of files and directories successfully backed up and restored. Performance Monitor also creates log files.

logical drive A subpartition of an extended partition on a hard disk. *See also* extended partition.

log off To stop using the network and remove your user name from active use until you log on again.

log on To provide a user name and password that identifies you to the network.

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 will either be disconnected from all server connections or allowed to remain connected but denied any new connections.

logon script A file that can be assigned to user accounts. Typically a batch program, 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. *See also* batch program.

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\Imports\Scripts). *See also* authentication; logon script.

logon workstations In Windows NT Server, the computers from which a user is allowed to log on.

long name A folder name or file name longer than the 8.3 file name standard (up to eight characters followed by a period and a three-character extension) of the FAT file system. Windows NT Server automatically translates long names of files and folders to 8.3 names for MS-DOS users.

Macintosh users can assign long names to files and folders on the server, and by using Services for Macintosh, you can assign long names to Macintosh-accessible volumes when you create them. *See also* file allocation table (FAT); file name; name mapping; short name.

loopback driver A network driver that allows the packets to bypass the network adapter completely and be returned directly to the computer that is performing the test.

M

Macintosh-accessible volume Storage space on the server used for folders and files of Macintosh users. A Macintosh-accessible volume is equivalent to a shared directory for PC users. Each Macintosh-accessible volume on a computer running Windows NT Server will correspond to a directory. Both PC users and Macintosh users can be given access to files located in a directory that is designated as both a shared directory and a Macintosh-accessible volume.

Macintosh-style permissions Directory and volume permissions that are similar to the access privileges used on a Macintosh.

Make Changes The Macintosh-style permission that gives users the right to make changes to a folder's contents; for example, modifying, renaming, moving, creating, and deleting files. When Services for Macintosh translates access privileges into Windows NT Server permissions, a user who has the Make Changes privilege is given Write and Delete permissions.

mandatory user profile A profile that is downloaded to the user's desktop each time he or she logs on. A mandatory user profile is created by an administrator and assigned to one or more users to create consistent or job-specific user profiles. They cannot be changed by the user and remain the same from one logon session to the next. *See also* roaming user profile; user profile.

master domain In the master domain model, the domain that is trusted by all other domains on the network and acts as the central administrative unit for user and group accounts.

maximize To enlarge a window to its maximum size by using the **Maximize** button (at the right of the title bar) or the **Maximize** command on the window menu.

Maximize button The small button containing a window icon at the right of the title bar. Mouse users can click the **Maximize** button to enlarge a window to its maximum size. Keyboard users can use the **Maximize** command on the window menu.

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.

member server A computer that runs Windows NT Server but is not a primary domain controller (PDC) or backup domain controller (BDC) of a Windows NT domain. Member servers do not receive copies of the directory database. Also called a stand-alone server. *See also* backup domain controller (BDC); directory database; primary domain controller (PDC).

memory A temporary storage area for information and programs. *See also* expanded memory; extended memory.

menu A list of available commands in a program window. Menu names appear in the menu bar near the top of the window. The window menu, represented by the program icon at the left end of the title bar, is common to all programs for Windows NT. To open a menu, click the menu name.

menu bar The horizontal bar containing the names of all the program's menus. It appears below the title bar.

Messenger service Sends and receives messages sent by administrators or by the Alerter service. *See also* Alerter service.

minimize To reduce a window to a button on the taskbar by using the **Minimize** button (at the right of the title bar) or the **Minimize** command on the **Control** menu. *See also* maximize.

Minimize button The small button containing a short line at the right of the title bar. Mouse users can click the **Minimize** button to reduce a window to a button on the taskbar. Keyboard users can use the **Minimize** command on the **Control** menu.

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.

modem Short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line.

MS-DOS-based application An application that is designed to run with MS-DOS, and therefore may not be able to take full advantage of all Windows NT features.

multiple boot A computer that runs two or more operating systems. For example, Windows 95, MS-DOS, and Windows NT operating systems can be installed on the same computer. When the computer is started, any one of the operating systems can be selected. Also known as dual boot.

N

named pipe An interprocess communication mechanism that allows one process to communicate with another local or remote process.

name mapping Is provided by Windows NT Server and Windows NT Workstation to ensure access by MS-DOS users to NTFS and FAT volumes (which can have share names of up to 255 characters, as opposed to MS-DOS, which is restricted to eight characters followed by a period and a three-character extension). With name mapping, each file or directory with a name that does not conform to the MS-DOS 8.3 standard is automatically given a second name that does. MS-DOS users connecting the file or directory over the network see the name in the 8.3 format; Windows NT Workstation and Windows NT Server users see the long name. *See also* long name.

NDS *See* NetWare Directory Services.

NetBEUI A network protocol usually used in small, department-size local area networks of 1 through 200 clients. It can use Token Ring source routing as its only method of routing. *See also* router.

NetBIOS *See* network basic input/output system.

Net Logon service For Windows NT Server, performs authentication of domain logons, and keeps the domain's directory database synchronized between the primary domain controller (PDC) and the other backup domain controllers (BDCs) of the domain. *See also* backup domain controller (BDC); directory database; primary domain controller (PDC).

NetWare Directory Services (NDS) A NetWare service that runs on NetWare servers. The service enables the location of resources on the network.

network adapter An expansion card or other device used to connect a computer to a local area network (LAN). Also called a network card; network adapter card; adapter card; network interface card (NIC).

network adapter card *See* network adapter.

network administrator A person responsible for planning, configuring, and managing the day-to-day operation of the network. This person may also be referred to as a system administrator.

network basic input/output system (NetBIOS) An application programming interface (API) that can be used by applications on a local area network. NetBIOS provides applications with a uniform set of commands for requesting the lower-level services required to conduct sessions between nodes on a network and to transmit information back and forth. *See also* application programming interface (API).

network card *See* network adapter.

network card driver A network device driver that works directly with the network card, acting as an intermediary between the card and the protocol driver. With Services for Macintosh, the AppleTalk Protocol stack on the server is implemented as a protocol driver and is bound to one or more network drivers.

network device driver Software that coordinates communication between the network adapter and the computer's hardware and other software, controlling the physical function of the network adapters.

network directory *See* shared directory.

network driver *See* network device driver.

network interface card (NIC) *See* network adapter.

network protocol Software that enables computers to communicate over a network. TCP/IP is a network protocol, used on the Internet. *See also* Transmission Control Protocol/Internet Protocol (TCP/IP).

NIC Acronym for network interface card. *See* network adapter.

nonpaged memory Memory that cannot be paged to disk. *See also* memory; paging file.

non–Windows NT application Refers to an application that is designed to run with Windows 3.*x*, MS-DOS, OS/2, or POSIX, but not specifically with Windows NT, and that may not be able to take full advantage of all Windows NT features (such as memory management). *See also* POSIX.

NT *See* Windows NT Server; Windows NT Workstation.

NT file system *See* Windows NT file system.

NTFS *See* Windows NT file system.

NWLink IPX/SPX Compatible Transport A standard network protocol that supports routing, and can support NetWare client/server applications, where NetWare-aware Sockets-based applications communicate with IPX/SPX Sockets-based applications. *See also* IPX/SPX.

O

one-way trust relationship One domain (the trusting domain) "trusts" the domain controllers in the other domain (the trusted domain) to authenticate user accounts from the trusted domain to use resources in the trusting domain. *See also* trust relationship; user account.

open To display the contents of a directory, a document, or a data file in a window.

owner In Windows NT, every file and directory on an NTFS volume has an owner, who controls how permissions are set on the file or directory and who can grant permissions to others.

In the Macintosh environment, an owner is the user responsible for setting permissions for a folder on a server. A Macintosh user who creates a folder on the server automatically becomes the owner of the folder. The owner can transfer ownership to someone else. Each Macintosh-accessible volume on the server also has an owner.

owner category In the Macintosh environment, this refers to the user category to which you assign permissions for the owner of a folder or a Macintosh volume. *See also* Macintosh-accessible volume.

P

paging file A special file on a PC 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 into 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 swap file.

partial synchronization The automatic, timed delivery to all domain BDCs (backup domain controllers) of only those directory database changes that have occurred since the last synchronization. *See also* backup domain controller (BDC); synchronize.

partition A partition is a portion of a physical disk that functions as though it were a physically separate unit. *See also* volume; extended partition; system partition.

Partition Table An area of the Master Boot Record that the computer uses to determine how to access the disk. The Partition Table can contain up to four partitions for each physical disk. *See also* Master Boot Record.

pass-through authentication When the user account must be authenticated, but the computer being used for the logon is not a domain controller in the domain where the user account is defined, nor is it the computer where the user account is defined, the computer passes the logon information through to a domain controller (directly or indirectly) where the user account is defined. *See also* domain controller; user account.

password A security measure used to restrict logons to user accounts and access to computer systems and resources. A password is a unique string of characters that must be provided before a logon or an access is authorized. For Windows NT, a password for a user account can be up to 14 characters, and is case-sensitive. There are four user-defined parameters to be entered in the **Account Policy** dialog box in User Manager or User Manager for Domains: maximum password age, minimum password age, minimum password length, and password uniqueness.

With Services for Macintosh, each Macintosh user must type a user password when accessing the Windows NT Server. You can also assign each Macintosh-accessible volume a volume password if you want, which all users must type to access the volume. *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; password.

path A sequence of directory (or folder) names that specifies the location of a directory, file, or folder within the directory tree. Each directory name and file name within the path (except the first) must be preceded by a backslash (\). For example, to specify the path of a file named Readme.wri located in the Windows directory on drive C, you type **c:\windows\readme.wri**

PC Any personal computer (such as an IBM PC or compatible) using the MS-DOS, OS/2, Windows, Windows for Workgroups, Windows 95, Windows NT Workstation, or Windows NT Server operating systems.

peer Any of the devices on a layered communications network that operate on the same protocol level.

permissions Windows NT Server settings you set on a shared resource that determine which users can use the resource and how they can use it. *See also* access permission.

Services for Macintosh automatically translates between permissions and Macintosh access privileges, so that permissions set on a directory (volume) are enforced for Macintosh users, and access privileges set by Macintosh users are enforced for PC users connected to the computer running Windows NT Server.

personal group In the **Start** menu on the **Programs** list, a program group you have created that contains program items. Personal groups are stored with your logon information and each time you log on, your personal groups appear. *See also* group.

pipe An interprocess communication mechanism. Writing to and reading from a pipe is much like writing to and reading from a file, except that the two processes are actually using a shared memory segment to communicate data. *See also* named pipe.

pointer The arrow-shaped cursor on the screen that follows the movement of a mouse (or other pointing device) and indicates which area of the screen will be affected when you press the mouse button. The pointer changes shape during certain tasks.

port A location used to pass data in and out of a computing device. This term can refer to an adapter card connecting a server to a network, a serial 232 port, a TCP/IP port, or a printer port.

POSIX Acronym for Portable Operating System Interface, an IEEE (Institute of Electrical and Electronics Engineers) standard that defines a set of operating-system services. Programs that adhere to the POSIX standard can be easily ported from one system to another.

PostScript printer A printer that uses the PostScript page description language to create text and graphics on the output medium, such as paper or overhead transparency. Examples of PostScript printers include the Apple LaserWriter, the NEC LC-890, and the QMS PS-810.

primary domain controller (PDC) In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC. *See also* directory database.

primary group The group with which a Macintosh user usually shares documents stored on a server. You specify a user's primary group in the user's account. When a user creates a folder on the server, the user's primary group is set as the folder's associated group (by default).

primary partition A partition is 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. *See also* extended partition; partition.

print device Refers to the actual hardware device that produces printed output.

printer Refers to the software interface between the operating system and the print device. The printer defines where the document will go before it reaches the print device (to a local port, to a file, or to a remote print share), when it will go, and various other aspects of the printing process.

printer driver A program that converts graphics commands into a specific printer language, such as PostScript or PCL.

printer fonts Fonts that are built into your printer. These fonts are usually located in the printer's read-only memory (ROM). *See also* font.

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

printer window Shows 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.

printing pool Consists of two or more identical print devices associated with one printer.

print job In the Macintosh environment, a document or image sent from a client to a printer.

print processor A PostScript program that understands the format of a document's image file and how to print the file to a specific printer or class of printers. *See also* encapsulated PostScript (EPS) file.

print server Refers to the computer that receives documents from clients.

Print Server for Macintosh A Services for Macintosh service that enables Macintosh clients to send documents to printers attached to a computer running Windows NT; enables PC clients to send documents to printers anywhere on the AppleTalk network; and enables Macintosh users to spool their documents to the computer running Windows NT Server, thus freeing their clients to do other tasks. Also called MacPrint.

print sharing The ability for a computer running Windows NT Workstation or Windows NT Server to share a printer on the network. This is done by using the **Printers** folder or the **net share** command.

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

private volume A Macintosh-accessible volume that is accessible by only one Macintosh user. For a volume to be a private volume, the permissions on its root directory must give the volume's owner all three permissions (Make Changes, See Files, and See Folders), while giving the primary group and everyone categories no permissions at all. When a private volume's owner uses the Chooser to view the volumes available on the server, the private volume is listed; however, no other users can see the private volume when viewing the volumes available on the server. *See also* Macintosh-accessible volume.

privilege level One of three settings (User, Administrator, or Guest) assigned to each user account. The privilege level a user account has determines the actions that the user can perform on the network. *See also* Administrator privilege; Guest privilege; user account; User privilege.

process When a program runs, a Windows NT process is created. A process is an object type which consists of an executable program, a set of virtual memory addresses, and one or more threads.

program file A file that starts an application or program. A program file has an .exe, .pif, .com, or .bat file name extension.

program group On the **Start** menu, a collection of programs. Grouping your programs makes them easier to find when you want to start them. *See also* common group; personal group.

program icon Located at the left of the window title bar, the program icon represents the program being run. Clicking the program icon opens the window menu.

program item A program, accessory, or document represented as an icon in the **Start** menu or on the desktop.

protocol A set of rules and conventions for sending information over a network. These rules govern the content, format, timing, sequencing, and error control of messages exchanged among network devices.

protocol driver A network device driver that implements a protocol, communicating between Windows NT Server and one or more network adapter card drivers. With Services for Macintosh, the AppleTalk Protocol stack is implemented as an NDIS-protocol driver, and is bound to one or more network adapter card drivers.

Q

queue In Windows NT terminology, a queue refers to a group of documents waiting to be printed. (In NetWare and OS/2 environments, queues are the primary software interface between the program and print device; users submit documents to a queue. However, with Windows NT, the printer is that interface—the document is sent to a printer, not a queue.)

R

RAM An acronym for random-access memory. RAM can be read from or written to by the computer or other devices. Information stored in RAM is lost when you turn off the computer. *See also* memory.

RAS *See* Remote Access Service.

refresh To update displayed information with current data.

registry The Windows NT registry is a hierarchical database that provides a repository for information about a computer's configuration on Windows NT Workstation and about hardware and user accounts on Windows NT Server. It is organized in subtrees and their keys, hives, and value entries. *See also* user account.

Remote Access Service (RAS) A service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a Windows NT–based computer can dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

remote administration Administration of one computer by an administrator located at another computer and connected to the first computer across the network.

remote logon Occurs when a user is already logged on to a user account and makes a network connection to another computer. *See also* user account.

remote procedure call (RPC) A message-passing facility that allows a distributed program to call services available on various machines in a network. Used during remote administration of computers. *See also* remote administration.

resource Any part of a computer system or a network, such as a disk drive, printer, or memory, that can be allotted to a program or a process while it is running, or shared over a local area network.

resource domain A trusting domain that establishes a one-way trust relationship with the master (account) domain, enabling users with accounts in the master domain to use resources in all the other domains. *See also* domain; trust relationship.

right *See* permissions; user rights.

roaming user profile User profile that is enabled when an administrator enters a user profile path into the user account. The first time the user logs off, the local user profile is copied to that location. Thereafter, the server copy of the user profile is downloaded each time the user logs on (if it is more current than the local copy) and is updated each time the user logs off. *See also* user profile.

root directory The top-level directory on a computer, a partition, or Macintosh-accessible volume. *See also* directory tree.

router In the Windows NT environment, a router helps LANs and WANs achieve interoperability and connectivity and can link LANs that have different network topologies (such as Ethernet and Token Ring). Routers match packet headers to a LAN segment and choose the best path for the packet, optimizing network performance.

In the Macintosh environment, routers are necessary for computers on different physical networks to communicate with each other. Routers maintain a map of the physical networks on a Macintosh internet (network) and forward data received from one physical network to other physical networks. Computers running Windows NT Server with Services for Macintosh can act as routers, and you can also use third-party routing hardware on a network with Services for Macintosh. *See also* local area network (LAN); wide area network (WAN).

S

SAM Acronym for Security Accounts Manager. *See* directory database; Windows NT Server Directory Services.

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 elements The parts that make up a window or dialog box, such as the title bar, the **Minimize** and **Maximize** buttons, the window borders, and the scroll bars.

screen saver A moving picture or pattern that appears on your screen when you have not used the mouse or the keyboard for a specified period of time. To select a screen saver, either use Display in Control Panel or right-click on the desktop for properties.

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 arrow An arrow on either end of a scroll bar that you use to scroll through the contents of the window or list box. Click the scroll arrow to scroll one screen at a time, or continue pressing the mouse button while pointing at the scroll arrow to scroll continuously.

scroll bar A bar that appears at the right and/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 scroll through the contents of the window or list box.

scroll box In a scroll bar, a small box that shows the position of information currently visible in the window or list box relative to the contents of the entire window.

SCSI *See* small computer system interface.

Search button *See* find tab.

secure attention sequence A series of keystrokes (CTRL+ALT+DELETE) that will always display the Windows NT operating system logon screen.

security A means of ensuring that shared files can be accessed only by authorized users.

Security Accounts Manager (SAM)
See directory database; Windows NT Server Directory Services.

security database *See* directory database.

security ID (SID) 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 (SID).

security log Records security events. This helps track changes to the security system and identify any possible breaches of security. For example, depending on the Audit settings in User Manager or User Manager for Domains, attempts to log on to the local computer might be recorded in the security log. The security log contains both valid and invalid logon attempts as well as events related to resource use (such as creating, opening, or deleting files). *See also* event.

security policies For Windows NT Workstation, the security policies consist of the Account, User Rights, and Audit policies, and are managed by using 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 by using User Manager for Domains.

security token *See* access token.

See Files The Macintosh-style permission that give users the right to open a folder and see the files in the folder. For example, a folder that has See Files and See Folders Macintosh-style permissions is given the Windows NT-style R (Read) permission. *See also* permissions.

See Folders The Macintosh-style permission that gives users the right to open a folder and see the files contained in that folder. *See also* permissions.

select To mark an item so that a subsequent action can be carried out on that item. You usually select an item by clicking it with a mouse or pressing a key. After selecting an item, you choose the action that you want to affect the item.

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 In general, refers to a computer that provides shared resources to network users. *See also* member server.

server application A Windows NT application that can create objects for linking or embedding into other documents. For distributed applications, the application that responds to a client application. *See also* client application; Distributed Component Object Model (DCOM); embedded object; linked object.

Server Manager In Windows NT Server, a program used to view and administer domains, workgroups, and computers.

Server service Provides RPC (remote procedure call) support, and file, print, and named pipe sharing. *See also* named pipe; remote procedure call (RPC).

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. *See also* application programming interface (API); remote procedure call (RPC).

Services for Macintosh *See* Windows NT Server Services for Macintosh.

session A link between two network devices, such as a client and a server. A session between a client and server consists of one or more connections from the client to the server.

SFM Acronym for Windows NT Services for Macintosh.

share To make resources, such as directories and printers, available to others.

shared directory A directory that network users can connect to.

shared network directory *See* shared directory.

shared resource Any device, data, or program that is used by more than one other device or program. For Windows NT, shared resources refer to any resource that is made available to network users, such as directories, files, printers, and named pipes. Also refers to a resource on a server that is available to network users. *See also* named pipe.

share name A name that refers to a shared resource on a server. Each shared directory on a server has a share name, used by PC users to refer to the directory. Users of Macintosh use the name of the Macintosh-accessible volume that corresponds to a directory, which may be the same as the share name. *See also* Macintosh-accessible volume.

share permissions Are used to restrict a shared resource's availability over the network to only certain users.

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.

short name A valid 8.3 (up to eight characters followed by a period and a three-character extension) MS-DOS or OS/2 file name that the computer running Windows NT Server creates for every Macintosh folder name or file name on the server. PC users refer to files on the server by their short names; Macintosh users refer to them by their long names. *See also* long name; name mapping.

SID *See* security ID.

single user logon Windows NT network users can connect to multiple servers, domains, and programs with a single network logon.

small computer system interface (SCSI) A standard high-speed parallel interface defined by the American National Standards Institute (ANSI). A SCSI interface is used for connecting microcomputers to peripheral devices such as hard disks and printers, and to other computers and local area networks.

SMS *See* Systems Management Server.

source directory The directory that contains the file or files you intend to copy or move.

source document The document where a linked or embedded object was originally created. *See also* embedded object; linked object.

special access permission On NTFS volumes, a custom set of permissions. You can customize permissions on files and directories by selecting the individual components of the standard sets of permissions. *See also* access permission.

split bar Divides Windows NT Explorer into two parts: The directory tree is displayed on the left, and the contents of the current directory are on the right. *See also* directory tree.

spooler Software that accepts documents sent by a user to be printed, and then stores those documents and sends them, one by one, to available printer(s). *See also* spooling.

spooling A process on a server in which print documents are stored on a disk until a printing device is ready to process them. A spooler accepts each document from each client, stores it, then sends it to a printing device when it is ready.

SQL Acronym for structured query language, a database programming language used for accessing, querying, and otherwise managing information in a relational database system.

stand-alone server *See* member server.

status bar A line of information related to the program in the window. Usually located at the bottom of a window. Not all windows have a status bar.

subdirectory A directory within a directory. Also called a folder within a folder.

subnet A portion of a network, which may be a physically independent network segment, that shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

subnet mask A 32-bit value that allows the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID. *See also* IP address.

swap file *See* paging file.

synchronize To replicate the domain database from the primary domain controller (PDC) to one backup domain controller (BDC) of the domain, or to all the BDCs of a domain. This is usually performed automatically by the system, but can also be invoked manually by an administrator. *See also* backup domain controller (BDC); domain; primary domain controller (PDC).

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 In Windows NT Server, the user profile that is loaded when Windows NT is running and no user is logged on. When the **Begin Logon** dialog box is visible, the system default profile is loaded. *See also* user default profile, user profile.

system disk A disk that contains the MS-DOS system files necessary to start MS-DOS.

system log The system log contains events logged by the Windows NT components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. Use Event Viewer to view the system log.

system partition The volume that has the hardware-specific files needed to load Windows NT. *See also* partition.

system policy A policy, created by using the System Policy Editor, to control user work environments and actions, and to enforce system configuration for Windows 95. System policy can be implemented for specific users, groups, computers, or for all users. System policy for users overwrites settings in the current user area of the registry, and system policy for computers overwrites the current local machine area of the registry. *See also* registry.

systemroot The name of the directory that contains Windows NT files. The name of this directory is specified when Windows NT is installed.

Systems Management Server Part of the Microsoft BackOffice family of products. Systems Management Server includes desktop management and software distribution that significantly automates the task of upgrading software on client computers.

T

tape set A tape set (sometimes referred to as a tape family) in Windows NT Backup is a sequence of tapes in which each tape is a continuation of the backup on the previous tape. *See also* backup set; backup types.

Task list A window that shows all running programs and their status. View the Task list in the **Applications** tab in Task Manager.

Task Manager Task Manager enables you to start, end, or run programs, end processes (a program, program component, or system process), and view CPU and memory use data. Task Manager gives you a simple, quick view of how each process (program or service) is using CPU and memory resources. (Note: In previous versions of Windows NT, Task List handled some of these functions.)

To run Task Manager, right-click the toolbar and then click Task Manager.

TCP *See* Transmission Control Protocol.

TCP/IP *See* Transmission Control Protocol/Internet Protocol.

template accounts Accounts that are not actually used by real users but serve as a basis for the real accounts (for administrative purposes).

terminate-and-stay-resident program (TSR)
A program running under MS-DOS that remains loaded in memory even when it is not running so that it can be quickly invoked for a specific task performed while any other program is operating.

text box In a dialog box, a box in which you type information needed to carry out a command. The text box may be blank or may contain text when the dialog box opens.

text file A file containing text characters (letters, numbers, and symbols) but no formatting information. A text file can be a "plain" ASCII file that most computers can read. Text file can also refer to a word-processing file. *See also* ASCII file.

text-only An ASCII file that contains no formatting. *See also* ASCII file.

time-out If a device is not performing a task, the amount of time the computer should wait before detecting it as an error.

title bar The horizontal bar (at the top of a window) that contains the title of the window or dialog box. On many windows, the title bar also contains the program icon and the **Maximize**, **Minimize**, and **Close** buttons.

toolbar A series of icons or shortcut buttons providing quick access to commands. Usually located directly below the menu bar. Not all windows have a toolbar.

topic Information in the Help window. A Help topic usually begins with a title and contains information about a particular task, command, or dialog box.

Transmission Control Protocol (TCP)
A connection-based Internet protocol responsible for breaking data into packets, which the IP protocol sends over the network. This protocol provides a reliable, sequenced communication stream for network communication. *See also* Internet Protocol (IP).

Transmission Control Protocol/Internet Protocol (TCP/IP)
A set of networking protocols that provide communications across interconnected networks made up of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan horse A program that masquerades as another common program in an attempt to receive information. An example of a Trojan horse is a program that masquerades as a system logon to retrieve user names and password information, which the writers of the Trojan horse can use later to break into the system.

TrueType fonts Fonts that are scalable and sometimes generated as bitmaps or soft fonts, depending on the capabilities of your printer. TrueType fonts can be sized to any height, and they print exactly as they appear on the screen.

trust *See* trust relationship.

trust relationship A link between domains that enables pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain. With trust relationships, a user who has only one user account in one domain can potentially 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 directory database. *See also* directory database; global group; pass-through authentication; user account.

trust relationships policy A security policy that determines which domains are trusted and which domains are trusting domains. *See also* trust relationship.

TSR *See* terminate-and-stay-resident program.

two-way trust relationship Each domain trusts user accounts in the other domain to use its resources. Users can log on from computers in either domain to the domain that contains their account. *See also* trust relationship.

U

unavailable An unavailable button or command is displayed in light gray instead of black, and it cannot be clicked.

UNC name *See* universal naming convention name.

uninterruptible power supply (UPS) A battery-operated power supply connected to a computer to keep the system running during a power failure.

universal naming convention (UNC) name A full Windows NT name of a resource on a network. It conforms to the \\server_name\share_name syntax, where *server_name* is the server's name and *share_name* is the name of the shared resource. UNC names of directories or files can also include the directory path under the share name, with the following syntax: \\server_name\*share_name**directory*\file*_name*

UPS *See* uninterruptible power supply.

UPS service Manages an uninterruptible power supply connected to a computer. *See also* uninterruptible power supply (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 Workstation, user accounts are managed with User Manager. For Windows NT Server, user accounts are managed with User Manager for Domains. *See also* group.

user account database *See* directory database.

user default profile In 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. User Manager 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. User Manager for Domains administers user accounts, groups, and security policies.

user name A unique name identifying a user account to Windows NT. An account's user name cannot be identical to any other group name or user name of its own domain or workgroup. *See also* user account.

user password The password stored in each user's account. Each user generally has a unique user password and must type that password when logging on or accessing a server. *See also* password; volume password.

User privilege One of three privilege levels you can assign to a Windows NT user account. Every user account has one of the three privilege levels (Administrator, Guest, and User). Accounts with User privilege are regular users of the network; most accounts on your network probably have User privilege. *See also* Administrator privilege; Guest privilege; user account.

user profile Configuration information that can be retained on a user-by-user basis, and is saved in user profiles. This 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. When a user logs on, the user's profile is loaded and the user's Windows NT environment is configured according to that profile. *See also* personal group; program item.

user rights Define a user's access to a computer or domain and the actions that a user can perform on the computer or domain. User rights permit actions such as logging onto a computer or network, adding or deleting users in a workstation or domain, and so forth.

user rights policy Manages the assignment of rights to groups and user accounts. *See also* user account; user rights.

users In the Macintosh environment, a special group that contains all users who have user permissions on the server. When a Macintosh user assigns permissions to everyone, those permissions are given to the groups users and guests. *See also* guest.

V

variables In programming, a variable is a named storage location capable of containing a certain type of data that can be modified during program execution. System environment variables are defined by Windows NT Server and are the same no matter who is logged on at the computer. (Administrator group members can add new variables or change the values, however.) User environment variables can be different for each user of a particular computer. They include any environment variables you want to define of variables defined by your programs, such as the path where program files are located.

virtual memory The space on your hard disk that Windows NT uses as if it were actually memory. Windows NT does this through the use of paging files. The benefit of using virtual memory is that you can run more programs at one time than your system's physical memory would otherwise allow. The drawbacks are the disk space required for the virtual-memory paging file and the decreased execution speed when paging is required. *See also* paging file.

virtual printer memory In a PostScript printer, a part of memory that stores font information. The memory in PostScript printers is divided into two areas: banded memory and virtual memory. The banded memory contains graphics and page-layout information needed to print your documents. The virtual memory contains any font information that is sent to your printer either when you print a document or when you download fonts. *See also* PostScript printer.

virus A program that attempts to spread from computer to computer and either cause damage (by erasing or corrupting data) or annoy users (by printing messages or altering what is displayed on the screen).

volume A partition or collection of partitions that have been formatted for use by a file system. *See also* Macintosh-accessible volume; partition.

volume password An optional, case-sensitive password you can assign to a Macintosh-accessible volume when you configure the volume. To access the volume, a user must type the volume password. *See also* Macintosh-accessible volume; user password.

volume set A combination of partitions on a physical disk that appear as one logical drive. *See also* logical drive; partition.

W

WAN *See* wide area network.

warning beep The sound that your computer makes when you encounter an error or try to perform a task that Windows NT does not recognize.

Web browser A software program, such as Microsoft Internet Explorer, that retrieves a document from a Web server, interprets the HTML codes, and displays the document to the user with as much graphical content as the software can supply.

Web server A computer equipped with the server software to respond to HTTP requests, such as requests from a Web browser. A Web server uses the HTTP protocol to communicate with clients on a TCP/IP network.

wide area network (WAN) A communications network that connects geographically separated areas.

wildcard 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 file names.

window A rectangular area on your screen in which you view a program or document. You can open, close, and move windows, and change the size of most windows. You can open several windows at a time, and you can often reduce a window to an icon or enlarge it to fill the entire desktop.

Windows NT–based application Used as a shorthand term to refer to an application that is designed to run with Windows NT and does not run without Windows NT. All Windows NT–based applications follow similar conventions for arrangement of menus, style of dialog boxes, and keyboard and mouse use.

Windows NT Explorer A program that enables you to view and manage the files and folders on your computer and make network connections to other shared resources, such as a hard disk on a server. Windows NT Explorer replaces Program Manager and File Manager, which were programs available in earlier versions of Windows NT. Program Manager and File Manager are still available, and can be started in the same way you start other Windows-based programs.

Windows NT file system (NTFS) An advanced file system designed for use specifically within the Windows NT operating system. It supports file system recovery, extremely large storage media, long file names, and various features for the POSIX subsystem. It also supports object-oriented programs by treating all files as objects with user-defined and system-defined attributes. *See also* POSIX.

Windows NT Server A superset of Windows NT Workstation, Windows NT Server provides centralized management and security, fault tolerance, and additional connectivity. *See also* fault tolerance; Windows NT Workstation.

Windows NT Server Directory Services
A Windows NT protected subsystem that maintains the directory database and provides an application programming interface (API) for accessing the database. *See also* application programming interface (API); directory database.

Windows NT Server Services for Macintosh
A software component of Windows NT Server that allows Macintosh users access to the computer running Windows NT Server. The services provided with this component allow PC and Macintosh users to share files and resources, such as printers on the AppleTalk network or those attached to a computer running Windows NT Server. *See also* Print Server for Macintosh.

Windows NT Workstation The portable, secure, 32-bit, preemptive multitasking member of the Microsoft Windows operating system family.

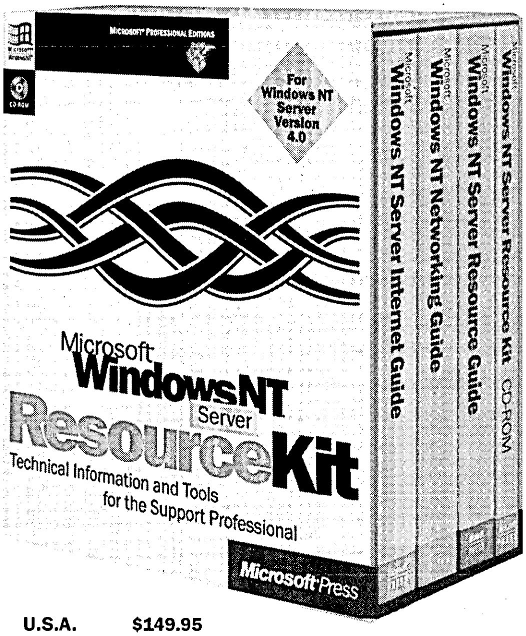
workgroup For Windows NT, a workgroup is a collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name. *See also* domain.

workstation Any networked Macintosh or PC using server resources. *See also* backup domain controller (BDC); member server; primary domain controller (PDC).

Workstation service Provides network connections and communications.

World Wide Web (WWW) The software, protocols, conventions, and information that enable hypertext and multimedia publishing of resources on different computers around the world. *See also* Hypertext Markup Language (HTML); Internet.

Index



Microsoft Professional Editions
CD-ROM
For Windows NT Server Version 4.0
Microsoft Windows NT Server Resource Kit
Technical Information and Tools for the Support Professional
Microsoft Press
Microsoft Windows NT Server Internet Guide
Microsoft Windows NT Networking Guide
Microsoft Windows NT Server Resource Guide
Microsoft Windows NT Server Resource Kit CD-ROM

Preparation for Microsoft Certified Professional Exams

Teach yourself to manage Microsoft® Windows NT® Workstation 4.0 and Microsoft Windows NT Server 4.0. Work through this self-paced training kit and you'll be able to provide critical day-to-day administration of single-user, single-domain, or enterprise networks.

With this text, you can learn to:

- Create and administer user and group accounts
- Troubleshoot logon problems
- Plan and manage resource sharing
- Set up and administer permissions for files and folders
- Set up, administer, and troubleshoot a printing environment
- Use auditing functions to generate and view security logs
- Monitor resources to obtain key information about network and computer resources
- Use tapes to back up and restore files and folders

Microsoft® Press

Part No. 097-0001830