Microsoft® Official Curriculum

Microsoft®
Training &
Certification

Implementing Microsoft® Windows® 2000 Professional and Server

Delivery Guide

Course Number: 2152B

Part Number: X05-78414
Released: 5/2000

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulations and interactive exercises were made with Macromedia Authorware

Course Number: 2152b
Part Number: X05-78414
Released: 5/2000

Contents

Introduction

Course Materials 2
Prerequisites 3
Course Outline 4
Microsoft Official Curriculum 9
Microsoft Certified Professional Program 10
Facilities 12

Module 1: Installing or Upgrading to Windows 2000

Overview 1
Preparing for Installation 2
Installing Windows 2000 Professional from a Compact Disc 13
Installing Windows 2000 Advanced Server from a Compact Disc 17
Lab A: Installing Windows 2000 23
Upgrading to Windows 2000 Professional 34
Upgrading to Windows 2000 Advanced Server 42
Identifying Setup Errors 46
Review 48

Module 2: Configuring the Windows 2000 Environment

Overview 1
Configuring and Managing Hardware 2
Lab A: Creating and Using Hardware Profiles 11
Configuring Display Options 17
Configuring System Settings 24
Configuring the Desktop Environment 29
Lab B: Modifying Startup and Recovery Options 36
Configuring Internet Options for Client Computers 40
Lab C: Configuring Internet Options 43
Review 46

Module 3: Connecting Windows 2000–based Clients to Networks

Overview 1
Windows 2000 Connectivity 2
Connecting to a Microsoft Network 4
Lab A: Configuring and Testing IP Addresses 13
Connecting to a Novell NetWare Network 24
Lab B: Installing and Configuring Gateway (and Client) Services for NetWare 32
Review 33

Module 4: Creating and Managing User Accounts

Overview 1
Introduction to User Accounts 2
Guidelines for New User Accounts 3
Creating Local User Accounts 7
Lab A: Creating Local User Accounts 9
Creating and Configuring Domain User Accounts 14

Setting Properties for Domain User Accounts 20
Customizing User Settings with User Profiles 29
Lab B: Creating and Modifying Domain User Accounts 33
Best Practices 39
Review 40

Module 5: Managing Access to Resources by Using Groups

Overview 1
Introduction to Windows 2000 Groups 2
Implementing Groups in a Workgroup 5
Implementing Groups in a Domain 10
Lab A: Creating a Global Group 19
Best Practices 23
Review 24

Module 6: Managing Data by Using NTFS

Overview 1
Introduction to NTFS Permissions 2
How Windows 2000 Applies NTFS Permissions 4
Using NTFS Permissions 11
Using Special NTFS Permissions 15
Lab A: Using NTFS Permissions 19
Compressing Data on an NTFS Partition 24
Configuring Disk Quotas on NTFS Partitions 29
Lab B: Configuring Disk Compression and Quotas 33
Securing Data by Using EFS 39
Lab C: Securing Files by Using EFS 44
Review 50

Module 7: Providing Network Access to File Resources

Overview 1
Introduction to Shared Folders 2
Creating Shared Folders 3
Combining NTFS and Shared Folder Permissions 13
Using Administrative Shared Folders 14
Publishing a Shared Folder in Active Directory 16
Lab A: Sharing and Securing Network Resources 17
Configuring Shared Folders by Using Dfs 25
Lab B: Configuring Domain-based Dfs 34
Review 40

Module 8: Monitoring and Optimizing Performance in Windows 2000

Overview 1
Monitoring Event Logs 2
Using Task Manager to Monitor System Resources 11
Lab A: Using Task Manager and Event Viewer 17
Using System Monitor to Monitor System Performance 27
Using Alerts 33
Lab B: Monitoring System Performance 35
Optimizing Performance 42
Review 53

Module 9: Implementing Security in Windows 2000

Overview....1
Securing Desktops and Services by Using Security Policies....2
Lab A: Configuring Windows 2000 Security Settings....15
Auditing Access to System Resources....23
Lab B: Configuring Auditing....32
Review....42

Module 10: Configuring Printing

Overview....1
Introduction to Windows 2000 Printing....2
Adding a Printer....6
Lab A: Installing Printers on a Print Server....13
Configuring a Network Printer....19
Configuring Internet Printing....25
Lab B: Installing a Client Printer and Managing Printers....29
Review....35

Module 11: Configuring Windows 2000 for Mobile Computing

Overview....1
Configuring Hardware for Mobile Computing....2
Configuring Power Management Options for Mobile Computing....4
Lab A: Configuring Power Management Options....8
Making Files Available for Offline Use....11
Lab B: Configuring Offline Files....18
Connecting to Networks and Computers....25
Identifying Solutions to Mobile Computing Problems....29
Review....30

Module 12: Configuring and Managing Disks

Overview....1
Windows 2000 Disk Types....2
Creating Partitions on a Basic Disk....7
Creating Volumes on a Dynamic Disk....8
Lab A: Working with Dynamic Disks....13
Performing Common Disk Management Tasks....19
Lab B: Creating and Mounting a New Volume....29
Best Practices....33
Review....34

Module 13: Implementing Disaster Protection

Overview....1
Introduction to Disaster Protection....2
Configuring an Uninterruptible Power Supply....4
Implementing Fault Tolerance by Using RAID....6
Lab A: Implementing Fault-Tolerant Volumes....19
Backing Up and Restoring Data....20
Lab B: Backing Up and Restoring System State Data....30
Using Disaster Recovery Tools....34
Review....41

Module 14: Installing and Configuring Terminal Services

Overview ... 1
Introduction to Terminal Services ... 2
Planning the Installation ... 8
Installing Terminal Services ... 17
Configuring Terminal Services ... 19
Establishing a Terminal Session ... 23
Configuring Session Settings ... 26
Lab A: Installing Terminal Services ... 27
Installing Applications on a Terminal Server ... 33
Lab B: Installing an Application ... 37
Review ... 40
Course Evaluation ... 42

Module 15: Implementing Windows 2000 Clients

Overview ... 1
Deploying Windows 2000 ... 2
Performing a Manual Network Installation ... 3
Customizing Installations and Upgrades by Using Switches ... 5
Installing Windows 2000 Using the Setup Manager Wizard ... 10
Using Disk Duplication ... 15
Lab A: Creating an Answer File for an Unattended Installation ... 18
Installing Windows 2000 Using RIS ... 23
Troubleshooting Windows 2000 Setup ... 28
Lab B: Running the System Preparation Tool ... 30
Review ... 34

Module 16: Implementing Windows 2000-based Servers

Overview ... 1
Common Implementation Features ... 2
Implementing a File Server ... 11
Implementing a Print Server ... 20
Implementing an Application Server ... 26
Implementing a Web Server ... 29
Routine Administration Tasks ... 33
Review ... 37
Course Evaluation ... 39

About This Course

This section provides you with a brief description of the course, audience, suggested prerequisites, and course objectives.

Description

This course provides students with the knowledge and skills necessary to install and configure Microsoft® Windows® 2000 Professional on stand-alone computers and on client computers that are part of a workgroup or a domain. In addition, this course provides the skills and knowledge necessary to install and configure Microsoft Windows 2000 Server to create file, print, and Terminal servers. It also provides students with the prerequisite knowledge and skills required for course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Audience

This course is intended for new-to-product support professionals who will be responsible for installing and configuring Microsoft Windows 2000 Professional and Windows 2000 Server, and for those who are on the Microsoft Certified Systems Engineer (MCSE) Windows 2000 certification track.

Student Prerequisites

This course requires that students meet the following prerequisites:

- Successful completion of course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*, or have equivalent knowledge. This includes the ability to:
  - Describe the principal features of the Windows 2000 operating system and basics of networking in a Windows 2000 environment.
  - Describe the types of user accounts and the principal security features of a Windows 2000 environment.
  - Identify the tools used to perform various administrative tasks.
  - Describe the features of the common protocols used in the Windows 2000 networking environment.
  - Describe the fundamentals of Transmission Control Protocol/Internet Protocol (TCP/IP).
  - Describe the network communication models used in a Windows 2000 network.
  - Differentiate between the various types of network architectures.
  - Describe physical components commonly used for network communication.

- Describe the concepts for remote access services and the protocols used for communication with a remote host.
- Describe the requirements for Internet access and Web security.
- Summarize network support tasks and utilities, and identify the purpose of key networking utilities in Windows 2000.

The course materials, lectures, and lab exercises are in English. To benefit fully from our instruction, students need an understanding of the English language and successful completion of the prerequisites.

Course Objectives

At the end of this course, the student will be able to:

- Install or upgrade to Windows 2000
- Configure the Windows 2000 environment
- Connect clients running Windows 2000 to networks
- Create and manage user accounts
- Manage access to resources by using groups
- Manage data by using NTFS
- Provide network access to file resources
- Monitor and optimize performance in Windows 2000
- Implement Windows 2000 Security
- Configure Windows 2000 Printing
- Configure Windows 2000 for mobile users
- Configure and manage disks and partitions
- Implement disaster protection
- Install and configure Terminal Services
- Implement Windows 2000-based clients
- Implement Windows 2000-based servers

Course Timing

The following schedule is an estimate of the course timing. Your timing may vary.

Day 1

Start	End	Module
9:00	9:30	Introduction
9:30	10:00	Module 1: Installing or Upgrading to Windows 2000
10:00	10:15	Break
10:15	11:30	Lab A: Installing Windows 2000
11:30	12:00	Module 1: Installing or Upgrading to Windows 2000 (*continued*)
12:00	1:00	Lunch
1:00	1:15	Module 2: Configuring the Windows 2000 Environment
1:15	1:30	Lab A: Creating and Using Hardware Profiles
1:30	2:15	Module 2: Configuring the Windows 2000 Environment (*continued*)
2:15	2:30	Lab B: Modifying Startup and Recovery Options
2:30	2:45	Break
2:45	2:50	Module 2: Configuring the Windows 2000 Environment (*continued*)
2:50	3:00	Lab C: Configuring Internet Options
3:00	3:30	Module 3: Connecting Windows 2000–based Clients to Networks
3:30	4:00	Lab A: Configuring and Testing IP Addresses
4:00	4:30	Module 3: Connecting Windows 2000–based Clients to Networks (*continued*)
4:30	4:45	Lab B: Installing and Configuring Gateway (and Client) Services for NetWare

Day 2

Start	End	Module
9:00	9:30	Day 1 review
9:30	10:00	Module 4: Creating and Managing User Accounts
9:45	10:30	Lab A: Creating Local User Accounts
10:30	10:45	Break
10:45	11:30	Module 4: Creating and Managing User Accounts (*continued*)
11:30	12:00	Lab B: Creating and Modifying Domain User Accounts
12:00	1:00	Lunch
1:00	1:45	Module 5: Managing Access to Resources by Using Groups
1:30	2:15	Lab A: Creating a Global Group
2:15	2:30	Break
2:30	3:00	Module 6: Managing Data by Using NTFS
3:00	3:30	Lab A: Using NTFS Permissions
3:30	4:00	Module 6: Managing Data by Using NTFS (*continued*)
4:00	4:30	Lab B: Configuring Disk Compression and Quotas
4:30	4:45	Module 6: Managing Data by Using NTFS (*continued*)
4:45	5:00	Lab C: Securing Files by Using EFS

Day 3

Start	End	Module
9:00	9:30	Day 2 review
9:30	10:00	Module 7: Providing Network Access to File Resources
10:00	10:30	Lab A: Sharing and Securing Network Resources
10:30	10:45	Break
10:45	11:30	Module 7: Providing Network Access to File Resources (*continued*)
11:30	12:00	Lab B: Configuring Domain-based Dfs
12:00	1:00	Lunch
1:00	1:15	Module 8: Monitoring and Optimizing Performance in Windows 2000
1:15	1:45	Lab A: Using Task Manager and Event Viewer
1:45	2:15	Module 8: Monitoring and Optimizing Performance in Windows 2000 (*continued*)
2:15	2:30	Break
2:30	3:00	Lab B: Monitoring System Performance
3:00	3:30	Module 9: Implementing Security in Windows 2000
3:30	4:00	Lab A: Configuring Windows 2000 Security Settings
4:00	4:30	Module 9: Implementing Security in Windows 2000 (*continued*)
4:30	5:00	Lab B: Configuring Auditing

Day 4

Start	End	Module
9:00	9:30	Day 3 review
9:30	10:00	Module 10: Configuring Printing
10:00	10:30	Lab A: Installing Printers on a Print Server
10:30	10:45	Break
10:45	11:30	Module 10: Configuring Printing (*continued*)
11:30	12:00	Lab B: Installing a Client Printer and Managing Printers
12:00	1:00	Lunch
1:00	1:30	Module 11: Configuring Windows 2000 for Mobile Computing
1:30	1:45	Lab A: Configuring Power Management Options
1:45	2:00	Module 11: Configuring Windows 2000 for Mobile Computing (*continued*)
2:00	2:30	Lab B: Configuring Offline Files
2:30	2:45	Break
2:45	3:30	Module 12: Configuring and Managing Disks
3:30	4:00	Lab A: Working with Dynamic Disks
4:00	4:30	Module 12: Configuring and Managing Disks (*continued*)
4:30	5:00	Lab B: Creating and Mounting a New Volume

Day 5

Start	End	Module
9:00	9:30	Day 4 review
9:30	10:15	Module 13: Implementing Disaster Protection
10:15	10:30	Lab A: Implementing Fault-Tolerant Volumes
10:30	10:40	Module 13: Implementing Disaster Protection (*continued*)
10:40	11:00	Lab B: Backing Up and Restoring System State Data
11:00	11:30	Module 14: Installing and Configuring Terminal Services
11:30	12:00	Lab A: Installing Terminal Services
12:00	1:00	Lunch
1:00	1:15	Module 14: Installing and Configuring Terminal Services (*continued*)
1:15	2:00	Lab B: Installing an Application
2:00	2:30	Module 15: Implementing Windows 2000 Clients
2:30	3:00	Lab A: Creating an Answer File for an Unattended Installation
3:00	3:15	Break
3:15	3:30	Module 15: Implementing Windows 2000 Clients (*continued*)
3:30	4:15	Lab B: Running the System Preparation Tool
4:15	5:00	Module 16: Implementing Windows 2000-based Servers

Trainer Materials Compact Disc Contents

The Trainer Materials compact disc contains the following files and folders:

- *Default.htm*. This file opens the Trainer Materials Web page.
- *Readme.txt*. This file contains a description of the compact disc contents and setup instructions in ASCII format (non-Microsoft Word document).
- *2152B_sg.doc*. This file is the Classroom Setup Guide. It contains a description of classroom requirements, classroom configuration, and classroom setup instructions.
- *Errorlog*. This folder contains a template that is used to record any errors and corrections that you find in the course.
- *Fonts*. This folder contains fonts that are required to view the Microsoft PowerPoint® presentation and Web-based materials.
- *Manual*. This folder contains the script files and documentation that is used for a manual classroom setup.
- *Powerpnt*. This folder contains the PowerPoint slides that are used in this course.
- *Pptview*. This folder contains the PowerPoint Viewer, which is used to display the PowerPoint slides.
- *Setup*. This folder contains the standard Microsoft Official Curriculum automated setup scripts that install and configure Windows 2000 on the instructor and student computers.
- *Studntcd*. This folder contains the Web page that provides students with links to resources pertaining to this course, including additional reading, review and lab answers, lab files, multimedia presentations, and course-related Web sites.
- *Tools*. This folder contains the post-installation scripts used to configure the instructor and student computers specifically for this course.
- *Tprep*. This folder contains the Trainer Preparation Presentation, a narrated slide show that explains the instructional strategy for the course and presentation tips and caveats. To open the presentation, on the Trainer Materials Web page, click **Trainer Preparation Presentation**.

Student Materials Compact Disc Contents

The Student Materials compact disc contains the following files and folders:

- *Default.htm*. This file opens the Student Materials Web page. It provides students with resources pertaining to this course, including additional reading, review and lab answers, lab files, multimedia presentations, and course-related Web sites.
- *Readme.txt*. This file contains a description of the compact disc contents and setup instructions in ASCII format (non-Microsoft Word document).
- *AddRead*. This folder contains additional reading pertaining to this course. If there are no additional reading files, this folder does not appear.
- *Answers*. This folder contains answers to the module review questions and hands-on labs.
- *Appendix*. This folder contains appendix files for this course. If there are no appendix files, this folder does not appear.
- *Courses*. This folder contains the self-paced courses that are included with this course.
- *Fonts*. This folder contains fonts that are required to view the PowerPoint presentation and Web-based materials.
- *Labfiles*. This folder contains files that are used in the hands-on labs. These files may be used to prepare the student computers for the hands-on labs.
- *Media*. This folder contains the multimedia presentations that are included with the course.
- *Simulation.* This folder contains the files for the simulated labs for this course.
- *Webfiles*. This folder contains the files that are required to view the course Web page. To open the Web page, open Windows Explorer, and in the root directory of the compact disc, double-click **Default.htm**.
- *Wordview*. This folder contains the Word Viewer that is used to view any Word document (.doc) files that are included on the compact disc. If no Word documents are included, this folder does not appear.

Document Conventions

The following conventions are used in course materials to distinguish elements of the text.

Convention	Use
◆	Indicates an introductory page. This symbol appears next to a slide title when additional information on the topic is covered on the page or pages that follow it.
bold	Represents commands, command options, and portions of syntax that must be typed exactly as shown. It also indicates commands on menus and buttons, icons, dialog box titles and options, and icon and menu names.
italic	In syntax statements, indicates placeholders for variable information. Italic is also used for introducing new terms, for book titles, and for emphasis in the text.
Title Capitals	Indicate domain names, user names, computer names, directory names, folders, and file names, except when specifically referring to case-sensitive names. Unless otherwise indicated, you can use lowercase letters when you type a directory name or file name in a dialog box or at a command prompt.
ALL CAPITALS	Indicate the names of keys, key sequences, and key combinations—for example, ALT+SPACEBAR.
`monospace`	Represents code samples, examples of screen text, or entries that you type at a command prompt or in initialization files.
[ ]	In syntax statements, enclose optional items. For example, [*filename*] 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.
{ }	In syntax statements, enclose required items. Type only the information within the braces, not the braces themselves.
|	In syntax statements, separates an either/or choice.
▶	Indicates a procedure with sequential steps.
...	In syntax statements, specifies that the preceding item may be repeated.
. . .	Represents an omitted portion of a code sample.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Introduction

Contents

Introduction	1
Course Materials	2
Prerequisites	3
Course Outline	4
Microsoft Official Curriculum	9
Microsoft Certified Professional Program	10
Facilities	12

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
30 Minutes

The Introduction module provides students with an overview of the course content, materials, and logistics for Course 2152B, *Implementing Microsoft® Windows® 2000 Professional and Server*.

Course Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this course, you need the following materials:

- Delivery Guide
- Trainer Materials compact disc

Preparation Tasks

To prepare for this course, you should:

- Complete the Course Preparation Checklist that is included with the trainer course materials.

Module Strategy

Use the following strategy to present this module:

- Course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*

  Show the slide that displays the course number and course title.

- Introduction

  Welcome students to the course and introduce yourself. Provide a brief overview of your background to establish credibility.

  Have students introduce themselves and provide their background, product experience, and expectations of the course.

  Record student expectations on a whiteboard or flip chart that you can reference later in class.

- Course Materials

  Explain the purpose of all materials used in this course.

  Tell students that they will have an opportunity at the end of class to provide feedback on the course and facilities by using the Microsoft Online Evaluation System.

- Prerequisites

  Provide the students with the list of prerequisites that they should have met before taking this course. This is an opportunity for you to identify students who may not have the appropriate background or experience to attend this course.

- Course Outline

  Provide an overview of each module and what students will learn.

  Explain how this course will meet students' expectations by relating the information covered in individual modules to their expectations.

- Microsoft Official Curriculum

  Inform students about the Microsoft Official Curriculum program and refer them to the Microsoft Official Curriculum Web page at http://www.microsoft.com/traincert/moc/

- Microsoft Certified Professional Program

  Inform students about the Microsoft Certified Professional (MCP) program and the various certification options.

- Facilities

  Explain the facility information for the training site.

Introduction

Topic Objective
To introduce yourself, establish credibility, meet students, and set student expectations for the course.

Lead-in
Good morning. Welcome to Course 2152B, *Implementing Microsoft Windows 2000 Professional and Server.*

My name is...

- **Name**
- **Company Affiliation**
- **Title/Function**
- **Job Responsibility**
- **Network Administration Experience**
- **Windows 2000 Experience**
- **Expectations for the Course**

**********ILLEGAL FOR NON-TRAINER USE**********

Introduce yourself.

Provide a brief overview of your background to establish credibility as a Windows 2000 instructor.

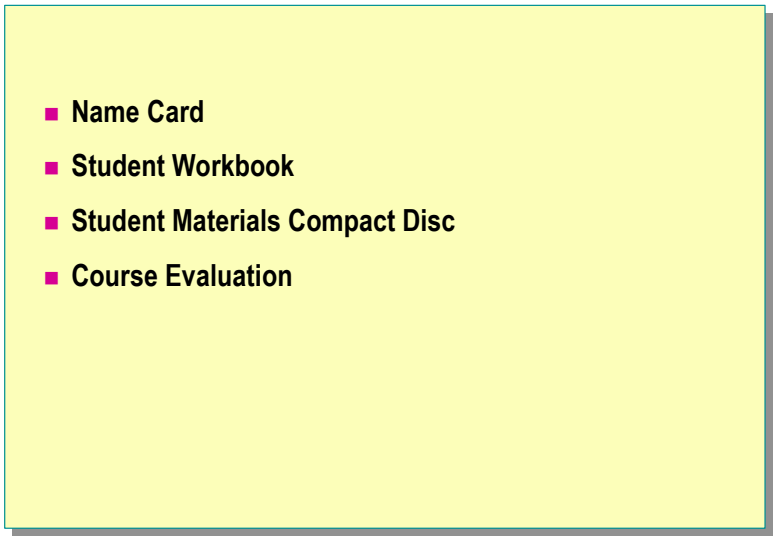
Ask students to introduce themselves, addressing the bulleted items on the slide.

Delivery Tip
Ask students to introduce themselves, use a whiteboard or flip chart to record their expectations of the course.

Course Materials

Topic Objective
To identify and describe the course materials.

Lead-in
We have provided everything you need for this course. You will find the following materials at your desk...



**********ILLEGAL FOR NON-TRAINER USE**********

Describe the contents of the student workbook and the Student Materials compact disc.

Have students write their names on both sides of the name card.

Tell students that a course evaluation must be completed at the end of the course.

Tell students where they can send comments.

Delivery Tip
Demonstrate how to open the Web page provided on the Student Materials compact disc. On the Trainer Materials compact disc, double-click **Default.htm** in the StudntCD folder.

The following materials are included with your kit:

- *Name card.* Write your name on both sides of the name card.
- *Student workbook.* The student workbook contains the material covered in class, in addition to the hands-on lab exercises.
- *Student Materials compact disc.* The Student Materials compact disc contains the Web page that provides students with links to resources pertaining to this course, including additional readings, review and lab answers, lab files, multimedia presentations, and course-related Web sites.

Note To open the Web page, insert the Student Materials compact disc into the CD-ROM drive, and then in the root directory of the compact disc, double-click **Default.htm**.

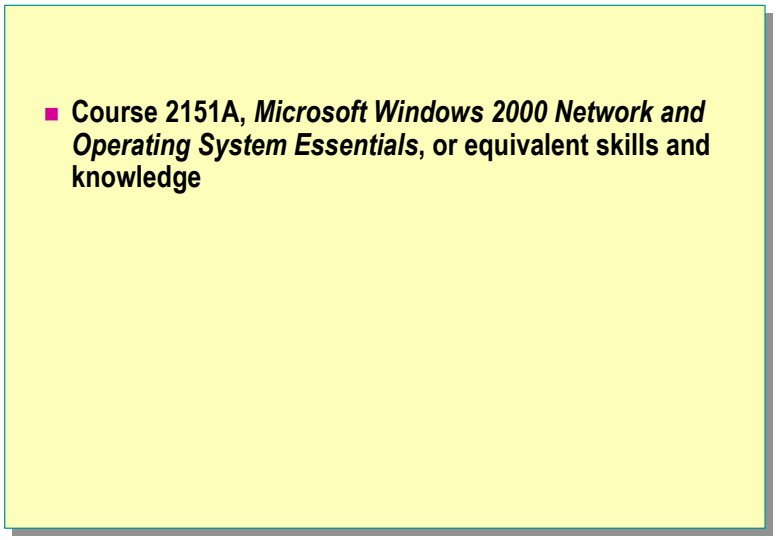
- *Course evaluation.* To provide feedback on the course, training facility, and instructor, you will have the opportunity to complete an online evaluation near the end of the course.

  To provide additional comments or inquire about the Microsoft Certified Professional program, send e-mail to mcphelp@microsoft.com.

Prerequisites

Topic Objective
To present and describe the prerequisites for this course.

Lead-in
The following prerequisite knowledge is needed for this course.



**********ILLEGAL FOR NON-TRAINER USE**********

This course requires that you meet the following prerequisites:

- Course 2151A, *Microsoft® Windows® 2000 Network and Operating System Essentials*, or equivalent skills and knowledge. To successfully complete Course 2152B, you should be able to:
  - Describe the principal features of the Windows 2000 operating system and the basics of a Windows 2000 network environment.
  - Describe the types of user accounts and the principal security features of a Windows 2000 environment.
  - Identify the tools used to perform various administrative tasks.
  - Describe the features of the common protocols used in the Windows 2000 network environment.
  - Describe the fundamentals of Transmission Control Protocol/Internet Protocol (TCP/IP).
  - Describe the network communication models used in a Windows 2000 network.
  - Differentiate between the various types of network architectures.
  - Describe physical components commonly used for network communication.
  - Describe the concept of remote access and the protocols used for communication with a remote host.
  - Describe the requirements for Internet access and Web security.
  - Summarize network support tasks and utilities, and identify the purpose of key networking utilities in Windows 2000.

Course Outline

Topic Objective
To provide an overview of each module and what students will learn.

Lead-in
In this course, we will cover...

- **Module 1: Installing or Upgrading to Windows 2000**
- **Module 2: Configuring the Windows 2000 Environment**
- **Module 3: Connecting Windows 2000-based Clients to Networks**
- **Module 4: Creating and Managing User Accounts**
- **Module 5: Managing Access to Resources by Using Groups**
- **Module 6: Managing Data by Using NTFS**

**********ILLEGAL FOR NON-TRAINER USE**********

Briefly describe each module.

As you describe each module, acknowledge any information that will meet the student expectations that you recorded earlier.

Module 1, "Installing or Upgrading to Windows 2000," presents the procedures for installing and upgrading to Windows 2000 Professional and Server. It starts by covering the preparation necessary for installation. The module then steps through the actual installation of Windows 2000 Professional and Advanced Server from a compact disc. Next, the module presents the procedures for upgrading to Windows 2000 Professional and Server. Finally, the module presents potential installation errors and their solutions. At the end of this module, you will be able to install or upgrade to Windows 2000 Professional and Server.

Module 2, "Configuring the Windows 2000 Environment," provides the knowledge and skills necessary to configure the Windows 2000 environment. The module begins with an explanation of how to configure and manage hardware, including how to configure and manage hardware profiles. Next, the module describes how to configure display settings and support for multiple monitors to expand the usable desktop area. The module continues by discussing how to configure operating system settings, including how to set environment variables and change startup and recovery options. The module concludes by describing how to configure the desktop environment. At the end of this module, you will be able to configure the Windows 2000 environment.

Module 3, "Connecting Windows 2000–based Clients to Networks," provides the knowledge and skills necessary to connect client computers running Windows 2000 to networks. The module begins with information on connecting to Microsoft networks, including how to configure TCP/IP manually and how to obtain settings automatically. Next, the module describes how to connect to networks running Novell NetWare, including the process for installing and configuring NWLink and Client Services for NetWare. At the end of this module, you will be able to connect Windows 2000 clients to networks.

Module 4, “Creating and Managing User Accounts,” provides the knowledge and skills necessary to create and manage user accounts. The module begins by introducing the concept of user accounts and what they are used for. The module then explains the requirements for local user accounts and the process for creating a local user account. Next, the module explains how to create and configure domain user accounts. The module also covers the steps for setting properties for domain user accounts. Finally, the module explains how to customize user settings with user profiles. At the end of this module, you will be able to create and manage user accounts.

Module 5, “Managing Access to Resources by Using Groups,” provides the knowledge and skills necessary to understand the purpose and use of groups, develop group strategies, and implement groups. The module begins with an overview of groups. It continues by explaining how to develop a group strategy. Next, it covers the process for creating groups in a domain and creating local groups. Finally, the module discusses best practices relating to groups. At the end of this module, you will be able to manage access to resources by using groups.

Module 6, “Managing Data by Using NTFS,” presents the skills and knowledge necessary to manage data by using the NTFS file system. The module starts by describing the purpose of NTFS file and folder permissions, and continues with information on how permissions apply in Windows 2000. Next, the module presents the process of assigning NTFS permissions to files and folders, and the process of controlling permissions inheritance. Next, the module describes NTFS data compression and how to configure disk quotas to manage user storage limits. Finally, the module describes how to secure data using Encrypting File System (EFS). At the end of this module, you will be able to manage data by using NTFS.

Course Outline *(continued)*

- Module 7: Providing Network Access to File Resources
- Module 8: Monitoring and Optimizing Performance in Windows 2000
- Module 9: Implementing Security in Windows 2000
- Module 10: Configuring Printing
- Module 11: Configuring Windows 2000 for Mobile Computing
- Module 12: Configuring and Managing Disks
- Module 13: Implementing Disaster Protection

**********ILLEGAL FOR NON-TRAINER USE**********

Module 7, “Providing Network Access to File Resources,” provides the knowledge and skills necessary to create shared folders, combine NTFS permissions and shared folders, and configure shared folders by using Distributed file system (Dfs). The module starts by defining shared folders, and explaining the process for creating them. The module describes how to combine NTFS permissions and shared folders. Next, the module explains how to use administrative shared folders. Finally, the module presents content on configuring shared folders by using Dfs. At the end of this module, you will be able to provide network access to file resources.

Module 8, “Monitoring and Optimizing Performance in Windows 2000,” provides the knowledge and skills necessary to maintain and optimize performance in Windows 2000 by monitoring system resources, monitoring event logs, optimizing performance, and resolving maintenance and optimization problems. The module starts by explaining how to monitor event logs. It follows by explaining how to use Task Manager and System Monitor to monitor system performance. Next, the module explains how to use alerts. The module concludes by explaining how to optimize system performance. At the end of this module, you will be able to monitor and optimize performance in Windows 2000.

Module 9, “Implementing Security in Windows 2000,” presents the knowledge and skills necessary to implement Windows 2000 security. The module begins by describing how to implement security policies, including how to create a security template and how to analyze security. The module concludes by demonstrating how to configure an Audit policy. At the end of this module, you will be able to implement Windows 2000 security.

Module 10, “Configuring Printing,” provides the knowledge and skills necessary to understand the printing environment in Windows 2000, add printers, configure a network printer, and configure Internet printer support. The module begins by introducing Windows 2000 printing concepts. The module details the steps for adding a printer. Finally, the module explains how to configure both a network printer and Internet printing. At the end of this module, you will be able to configure printing.

Module 11, “Configuring Windows 2000 for Mobile Computing,” provides the knowledge and skills necessary to configure Windows 2000 for mobile computing by configuring hardware, configuring power management options, configuring files and folders for offline use, and connecting to computers from a remote location. The module begins by explaining how to configure hardware for mobile computing. Next, the module explains how to configure power management options. The module continues by explaining how to make files and folders available for offline use. Next, the module explains how mobile users can connect to networks and other computers. The module concludes by presenting common mobile computing problems and their solutions. At the end of this module, you will be able to configure Windows 2000 for mobile computing.

Module 12, “Configuring and Managing Disks,” discusses the disk storage options in Windows 2000. The module begins by explaining the Windows 2000 disk storage types. The module continues with a discussion of how to create basic partitions. Then, the module defines dynamic storage and dynamic volume types, and presents the process for converting a basic disk to a dynamic disk and configuring dynamic volumes. The module continues by describing the procedures for other common disk management tasks. The module concludes by identifying disk configuration and storage recommendations. At the end of this module, you will be able to configure and manage disks and partitions.

Module 13, “Implementing Disaster Protection,” is designed to provide students with the knowledge and skills necessary to implement disaster protection in Windows 2000. The module begins with an overview of disaster protection features in Windows 2000, and continues with information on configuring an uninterruptible power supply. Next, the module describes the purpose and function of fault-tolerant volumes, how to configure them, and how to recover in the event of a fault-tolerant drive failure. The module continues by describing how to use the Backup utility to back up and restore files and the system state data, and to schedule a backup. The module concludes with a description of the process for recovering from a computer disaster, and how to identify and resolve problems related to implementing disaster protection. At the end of this module, you will be able to implement disaster protection.

Course Outline *(continued)*

- **Module 14: Installing and Configuring Terminal Services**
- **Module 15: Implementing Windows 2000 Clients**
- **Module 16: Implementing Windows 2000-based Servers**

**********ILLEGAL FOR NON-TRAINER USE**********

Module 14, “Installing and Configuring Terminal Services,” provides students with the knowledge and skills necessary to plan a Terminal Services installation, install and configure Terminal Services, connect to a Terminal server, install applications on a Terminal server, and administer a remote server by using Terminal Services. The module begins with an introduction to Terminal Services. It continues with instructions for planning a Terminal Services installation. Next, the module describes how to install and configure Terminal Services. The module then explains how to establish a Terminal session, and then configure session settings. Finally, the module explains how to install applications on a Terminal server. At the end of this module, you will be able to install and configure Terminal Services.

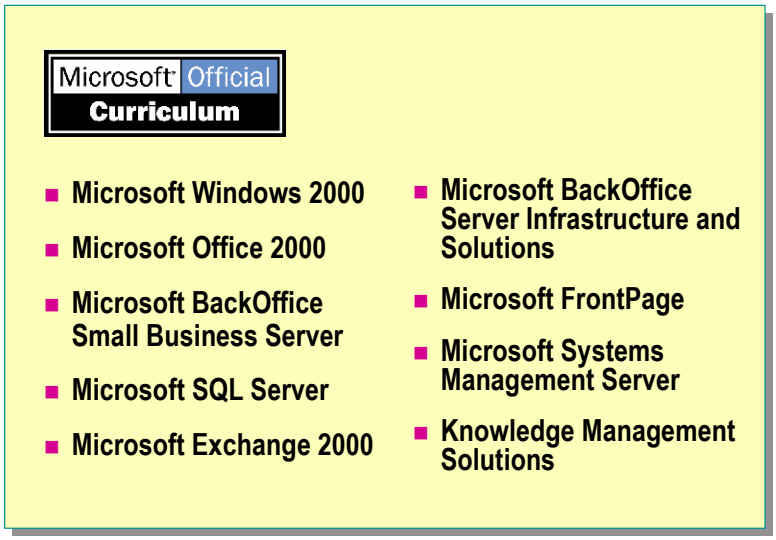
Module 15, “Implementing Windows 2000 Clients,” provides the knowledge and skills necessary to implement Windows 2000 Professional on a client computer. The module begins by explaining how to deploy Windows 2000 Professional. The module continues with details on performing a manual installation. Next, the module explains how to customize installations and upgrades by using switches. The module continues by explaining how to use the Setup Manager wizard. Then, the module covers the process for using disk duplication. The module continues with content on performing a remote installation of Windows 2000. The module concludes with Windows 2000 troubleshooting suggestions. At the end of this module, you will be able to implement Windows 2000 clients.

Module 16, “Implementing Windows 2000–based Servers,” provides the knowledge and skills necessary to implement servers running Windows 2000. The module begins by explaining common Windows 2000 Server implementation features. The module then explains how to implement a file server, a print server, an application server, and a Web server. The module concludes with an explanation of common administration tasks. At the end of this module, you will be able to implement Windows 2000–based servers.

Microsoft Official Curriculum

Topic Objective
To explain the Microsoft Official Curriculum program and provide information about curriculum paths.

Lead-in
Let's briefly talk about the Microsoft Official Curriculum program.



**********ILLEGAL FOR NON-TRAINER USE**********

Microsoft Official Curriculum (MOC) is hands-on instructor-led, Web-based, or self-paced technical training. Microsoft develops MOC courses to educate computer professionals who develop, support, and implement solutions by using Microsoft products, solutions, and technologies. MOC courses are available or in development for the following products and solutions:

- Microsoft Windows 2000
- Microsoft Office 2000
- Microsoft BackOffice Small Business Server
- Microsoft SQL Server
- Microsoft Exchange 2000
- Microsoft BackOffice Server Infrastructure and Solutions
- Microsoft FrontPage®
- Microsoft Systems Management Server
- Knowledge Management Solutions

MOC provides a curriculum path for each product and solution. For more information on the curriculum paths, see the Microsoft Official Curriculum Web page at: http://www.microsoft.com/traincert/moc/

The Microsoft Official Curriculum Web page provides information about MOC courses. In addition, you can find recommended curriculum paths for people who are entering the Information Technology (IT) industry, who are continuing their training on Microsoft products and solutions, or who currently support non-Microsoft products.

Microsoft Certified Professional Program

Topic Objective
To provide students with information about the Microsoft Certified Professional Program.

Lead-in
The Microsoft Certified Professional Program includes these certifications…

**********ILLEGAL FOR NON-TRAINER USE**********

The Microsoft Certified Professional program is a leading certification program that validates your experience and skills to keep you competitive in today's changing business environment. The following table describes each certification in more detail.

Certification	Description
MCSA on Microsoft Windows 2000	The Microsoft Certified Systems Administrator (MCSA) certification is designed for professionals who implement, manage, and troubleshoot existing network and system environments based on Microsoft Windows 2000 platforms, including the Windows .NET Server family. Implementation responsibilities include installing and configuring parts of the systems. Management responsibilities include administering and supporting the systems.
MCSE on Microsoft Windows 2000	The Microsoft Certified Systems Engineer (MCSE) credential is the premier certification for professionals who analyze the business requirements and design and implement the infrastructure for business solutions based on the Microsoft Windows 2000 platform and Microsoft server software, including the Windows .NET Server family. Implementation responsibilities include installing, configuring, and troubleshooting network systems.
MCSD	The Microsoft Certified Solution Developer (MCSD) credential is the premier certification for professionals who design and develop leading-edge business solutions with Microsoft development tools, technologies, platforms, and the Microsoft Windows DNA architecture. The types of applications MCSDs can develop include desktop applications and multi-user, Web-based, N-tier, and transaction-based applications. The credential covers job tasks ranging from analyzing business requirements to maintaining solutions.
MCDBA on Microsoft SQL Server 2000	The Microsoft Certified Database Administrator (MCDBA) credential is the premier certification for professionals who implement and administer Microsoft SQL Server databases. The certification is appropriate for individuals who derive physical database designs, develop logical data models, create physical databases, create data services by using Transact-SQL, manage and maintain databases, configure and manage security, monitor and optimize databases, and install and configure SQL Server.

(*continued*)

Certification	Description
MCP	The Microsoft Certified Professional (MCP) credential is for individuals who have the skills to successfully implement a Microsoft product or technology as part of a business solution in an organization. Hands-on experience with the product is necessary to successfully achieve certification.
MCT	Microsoft Certified Trainers (MCTs) demonstrate the instructional and technical skills that qualify them to deliver Microsoft Official Curriculum through Microsoft Certified Technical Education Centers (Microsoft CTECs).

Certification Requirements

The certification requirements differ for each certification category 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.

For More Information See the Microsoft Training and Certification Web site at http://www.microsoft.com/traincert/.

You can also send e-mail to mcphelp@microsoft.com if you have specific certification questions.

Acquiring the Skills Tested by an MCP Exam

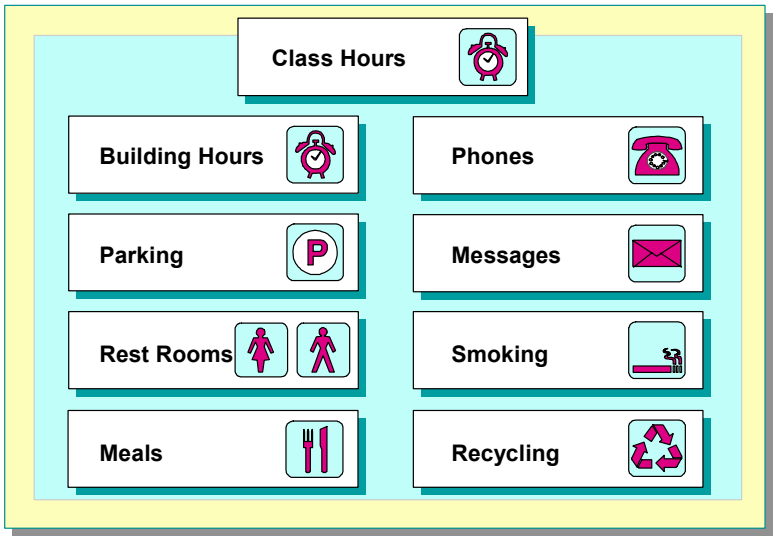
Microsoft Official Curriculum (MOC) and MSDN® Training Curriculum can help you develop the skills that you need to do your job. They also complement the experience that you gain while working with Microsoft products and technologies. However, no one-to-one correlation exists between MOC and MSDN Training courses and MCP exams. Microsoft does not expect or intend for the courses to be the sole preparation method for passing MCP exams. Practical product knowledge and experience is also necessary to pass the MCP exams.

To help prepare for the MCP exams, use the preparation guides that are available for each exam. Each Exam Preparation Guide contains exam-specific information, such as a list of the topics on which you will be tested. These guides are available on the Microsoft Training and Certification Web site at http://www.microsoft.com/traincert/.

Facilities

Topic Objective
To inform students of class logistics and rules for the training site.

Lead-in
Before we start, let's go over the class logistics.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain the class hours, extended building hours for labs, parking, rest room location, meals, phones, message posting, and where smoking is or isn't allowed.

Also make sure that the students are aware of the recycling program if one is available.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 1: Installing or Upgrading to Windows 2000

Contents

Overview	1
Preparing for Installation	2
Installing Windows 2000 Professional from a Compact Disc	13
Installing Windows 2000 Advanced Server from a Compact Disc	17
Lab A: Installing Windows 2000	23
Upgrading to Windows 2000 Professional	34
Upgrading to Windows 2000 Advanced Server	42
Identifying Setup Errors	46
Review	48

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
60 Minutes

Lab:
75 Minutes

This module provides students with the knowledge and skills to install Microsoft® Windows® 2000 Professional and Windows 2000 Advanced Server, and to upgrade from earlier versions of Windows. In addition, students will be able to provide solutions to common setup errors.

At the end of this module, students will:

- Prepare for a Windows 2000 installation.
- Install Windows 2000 Professional from a compact disc.
- Install Windows 2000 Advanced Server from a compact disc.
- Upgrade to Windows 2000 Professional.
- Upgrade to Windows 2000 Advanced Server.
- Identify setup errors.

Materials and Preparation

This section provides you with the required materials and preparation tasks needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- The Microsoft PowerPoint® file 2152B_01.ppt.
- The Windows 2000 Professional Installation Simulation on the Student Materials compact disc. The path is: *StudntCD*\Simulation\2152B_PIN.exe.

Preparation Tasks

To prepare for this module, you should:

- Read all the materials for this module.
- Complete the lab.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Preparing for Installation

  In this section present the issues students must consider before they install Windows 2000. First, present information on the Windows 2000 suite of operating systems, present the system requirements, and then present information on partitioning the hard disk. After this, present the different file systems option. Emphasize that the NTFS file system is the recommended file system for Windows 2000. Then, present the information on licensing modes. Emphasize that they can change from Per Server to Per Seat once at no charge. Therefore, if they have doubts on which to use, they should choose Per Server.

  Next, present information on the network types: workgroup or domain. Make sure they clearly understand where the user accounts are stored in a workgroup and domain and how this affects gaining access to resources. If they are unclear, use the whiteboard to illustrate the differences. In addition, present the information on the computer and user accounts required when joining a domain. Finally, present the pre-installation checklist.

- Installing Windows 2000 Professional from a Compact Disc

  In this section you will use the Windows 2000 Professional Simulation to demonstrate the installation. First, present the tasks for running the Setup program. Mention to the student that if they do not have a bootable CD-ROM drive, they can start the computer from the Startup disks. In addition, mention that a simulation of the Windows 2000 Professional installation is on the Student Materials compact disc. Then, present the tasks for completing the Setup wizard. Finally, present the tasks on installing network components.

- Installing Windows 2000 Advanced Server from a Compact Disc

  First, present the tasks for running the Setup program. Then, present the tasks for completing the Setup wizard. Next, present the tasks for installing network components. Finally, present information on configuring the server.

- Upgrading to Windows 2000 Professional

  First, present information on the different upgrade paths. Mention that Windows 3.1 cannot be upgraded directly to Windows 2000 Professional, but must be upgraded to Windows 95 or Windows 98 first. Then, present the more detailed information on upgrading from Windows 95 and Windows 98. Mention that Windows 2000 can generate compatibility reports.

  Next, present more detailed information on upgrading Windows NT® Workstation version 3.1 or 4.0. Emphasize the easiest upgrade path to Windows 2000 Professional. Finally, present information on installing the Directory Services client. Emphasize that Microsoft Internet Explorer 4.0.1 or later must be installed and that the Active Desktop™ component is enabled.

- Upgrading to Windows 2000 Advanced Server

  First, present information on the different upgrade paths. The paths include domain controllers, member servers, and Windows NT 3.1 and 3.5. Then, present information on backing up critical data files and settings. Emphasize that backing up is important in preventing data loss in the event of an upgrade failure.

- Identifying Setup Errors

  Present the common setup errors that can occur and their possible solutions.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

The lab in this module requires that you perform the procedure specified in the Classroom Setup Guide before performing this lab. To ensure the lab functions properly, do not run any other lab activities after completing classroom setup and starting this lab.

Lab Results

Performing the lab in this module introduces the following configuration changes:

- Student computers are configured as member servers running Windows 2000 Advanced Server.
- Student computers are configured with a static IP (Internet Protocol) address and a subnet mask of 255.255.255.0.
- Student computers are configured with the name of a major international city and are member servers of the Nwtraders.msft domain.
- Student computers are configured with an Administrator account with a password of **password**.
- Student computers are configured with the NTFS file system.
- Student computers are configured with the Per Server Client Access Licensing (CAL) mode with 20 concurrent connections.
- Student computers are configured with the display resolution set to 800 x 600 x 256 colors.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about installing and upgrading to Windows 2000.

- **Preparing for Installation**
- **Installing Windows 2000 Professional from a Compact Disc**
- **Installing Windows 2000 Advanced Server from a Compact Disc**
- **Upgrading to Windows 2000 Professional**
- **Upgrading to Windows 2000 Advanced Server**
- **Identifying Setup Errors**

**********ILLEGAL FOR NON-TRAINER USE**********

One of your first tasks as a Microsoft® Windows® 2000 support professional may be to install or upgrade the operating system. You can install Windows 2000 in several different ways, and there are multiple options and system requirements for each method of installation. Familiarity with the available options and setup procedures will help you deploy Windows 2000 efficiently.

At the end of this module, you will be able to:

- Prepare for a Windows 2000 installation.
- Install Windows 2000 Professional from a compact disc.
- Install Windows 2000 Advanced Server from a compact disc.
- Upgrade to Windows 2000 Professional.
- Upgrade to Windows 2000 Advanced Server.
- Identify setup errors.

Note Although this module presents the tasks for installing or upgrading to Windows 2000 Advanced Server, these tasks are similar for all of the Windows 2000-based server operating systems.

◆ Preparing for Installation

Topic Objective
To identify preparation tasks.

Lead-in
Thorough preparation will help you to avoid problems both during and after the installation.

- Determining Which Operating System to Use
- Identifying System Requirements
- Determining Disk Partition Options
- Determining Which File System to Select
- Determining Which Licensing Mode to Select
- Determining Whether to Join a Workgroup or Domain
- Completing a Pre-Installation Checklist

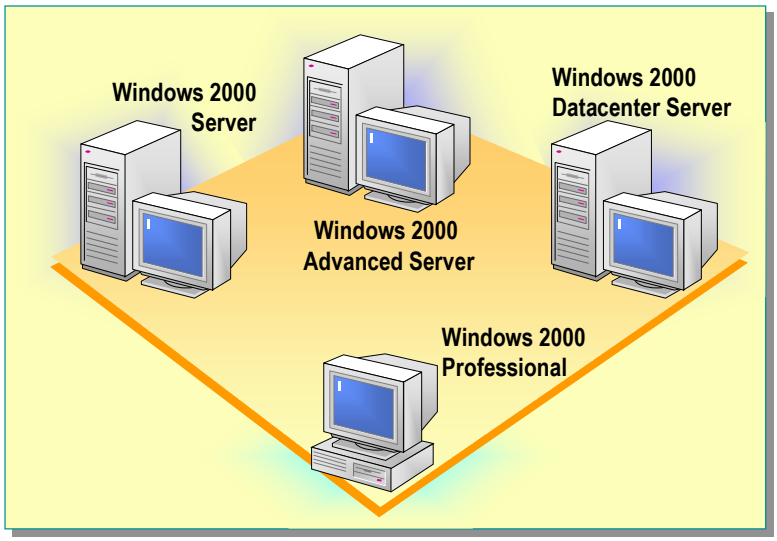
**********ILLEGAL FOR NON-TRAINER USE**********

Installing Windows 2000 requires a certain amount of preparation. When you run the Windows 2000 Setup program, you need to provide information about how to install and configure the operating system. Thorough preparation helps you to avoid problems during installation and to troubleshoot problems after installation. An understanding of the available configuration options also helps to ensure that you have a properly configured operating system.

Determining Which Operating System to Use

Topic Objective
To present the different Windows 2000 operating systems.

Lead-in
The first step in preparing for installation is to select which operating system in the Windows 2000 suite you are going to install.



**********ILLEGAL FOR NON-TRAINER USE**********

Understanding the capabilities of each of the Microsoft Windows 2000 operating systems will enable you to select the best product to meet the current and future needs of your organization.

The following table describes the operating systems that are included in the Windows 2000 suite.

Operating system	Description	Examples of when to use
Windows 2000 Professional	Replaces Microsoft Windows 95, Microsoft Windows 98, and Microsoft Windows NT® Workstation version 4.0 in a business environment.	This version is the desktop operating system for businesses of all sizes.
Windows 2000 Server	Contains all of the features found in Windows 2000 Professional and provides services that simplify network management. In addition, Windows 2000 Server includes Terminal Services.	This version is ideal for file and print servers, Web servers, and workgroups. It also provides improved network access for branch offices.

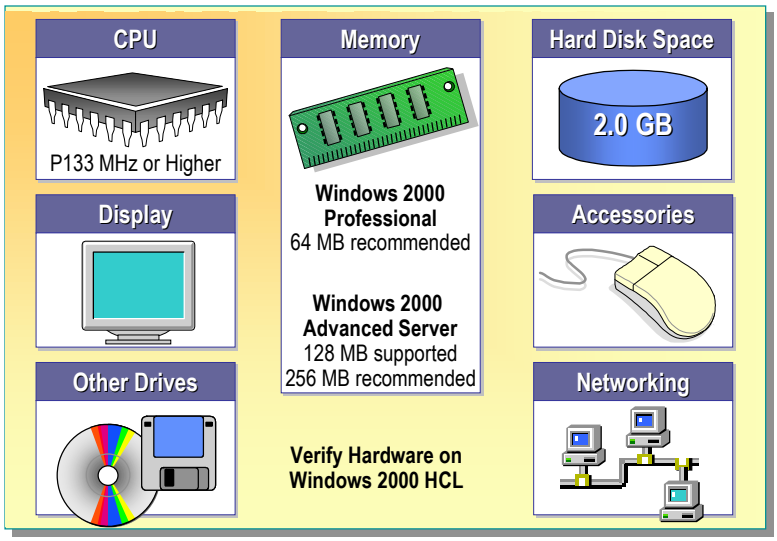
(*continued*)

Operating system	Description	Examples of when to use
Windows 2000 Advanced Server	Contains all of the features in Microsoft Windows 2000 Server and provides increased scalability and system availability. In addition, Windows 2000 Advanced Server includes the Windows Clustering and Load balancing.	This version is designed for servers used in a large enterprise network, and database-intensive work.
Windows 2000 Datacenter Server	Contains all of the features in Microsoft Windows 2000 Advanced Server and supports more memory and more CPUs per computer. This version of Windows 2000 is the most powerful server operating system in the Windows 2000 suite.	This version is designed for large data warehouses, online transaction processing (OLTP), large-scale simulations, and server consolidation projects.

Identifying System Requirements

Topic Objective
To illustrate the system requirements for Windows 2000 Advanced Server and Windows 2000 Professional.

Lead-in
The first task in preparing for the installation is to ensure that your hardware meets the minimum requirements for Windows 2000.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
It is recommended that you allow more disk space than the minimum amount to allocate space for optional components, such as user accounts, Active Directory information, logs, future service packs, and the paging file used by the operating system.

The following table lists the system requirements (sometimes known as hardware requirements) for Windows 2000.

Component	Windows 2000 Professional requirements	Windows 2000 Server requirements
CPU	Pentium 133-megahertz (MHz) or higher microprocessor (or equivalent compatible) Windows 2000 Professional supports up to 2 processors. Windows 2000 Server supports up to 4 processors. Windows 2000 Advanced Server supports up to 8 processors. Windows 2000 Datacenter supports up to 16 processors.	
Memory	64 megabytes (MB) recommended minimum. More memory generally improves responsiveness. 4 gigabytes (GB) maximum	256 MB recommended minimum (128 MB supported). Server: 4 GB maximum Advances Server: 8 GB maximum
Hard disk space	2 GB with a minimum of 1 GB of free space	2 GB with a minimum of 1 GB of free space. Additional hard disk space is required if you are installing over a network.
Display	Video graphics array (VGA) resolution or higher resolution monitor	
Accessories	Keyboard and mouse or other pointing device	
For CD-ROM installation	CD-ROM drive, 12x or faster recommended If the computer does not support starting the Setup program from a compact disc, a high-density 3.5-inch disk is also required.	
For network installation	One or more Windows 2000-compatible network adapter cards and related cables.	

Key Points
Although 640 x 480 screen resolution can be used, the Windows 2000 user interface is viewed optimally by using an 800 x 600 or higher screen resolution.

Key Point
Administrators should verify that their hardware is on the Windows 2000 HCL to ensure they do not have problems during an installation or upgrade.

Before you install Windows 2000, verify that your hardware is on the Windows 2000 Hardware Compatibility List (HCL). Microsoft provides tested drivers for only those devices that are listed on the Windows 2000 HCL. Using hardware that is not listed on the HCL may cause problems during and after installation. For a copy of the HCL, see the Hcl.txt file in the Support folder on the Windows 2000 compact disc.

For the most recent version of the HCL, see the Microsoft Windows Hardware Compatibility List Web site at http://www.microsoft.com/hwtest/hcl.

In addition, for more information about system requirements, see the Windows 2000 Product Guide Web site at http://www.microsoft.com/windows2000/guide

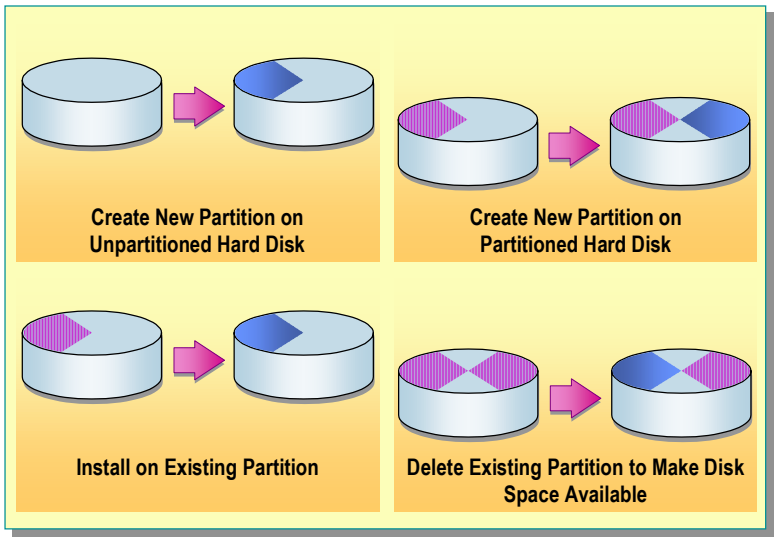
---

Important Microsoft supports only those devices that are listed on the HCL. If you have hardware that is not on this list, contact the hardware manufacturer to determine if there is a manufacturer-supported driver for the component that is Windows 2000 compliant.

Determining Disk Partition Options

Topic Objective
To illustrate the disk partition options for installing Windows 2000.

Lead-in
During installation, you can create and size the partition on which to install Windows 2000 or you can use an existing partition.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Disk partition options are available only if you install Windows 2000 from a compact disc.

Disk partitioning is a way of dividing your physical disk so that each section functions as a separate unit. When you create partitions on a disk, you divide the disk into one or more areas that can be formatted for use by a file system, such as file allocated table (FAT) or the NTFS file system.

When you are performing a new installation from a compact disc, the Setup program examines the hard disk to determine its existing configuration, and offers the following options:

- A new partition on an unpartitioned hard disk. If the hard disk is unpartitioned, you can create and size the Windows 2000 partition.
- A new partition on a partitioned hard disk. If the hard disk is partitioned, but has enough unpartitioned disk space, you can create the Windows 2000 partition in the unpartitioned space.
- Install on existing partition. If the hard disk has an existing partition that is large enough, you can install Windows 2000 on that partition. If there is an operating system on an existing partition, performing a new installation overwrites that operating system.
- Delete existing partition. If the hard disk has an existing partition, you can delete it to create more unpartitioned disk space for the Windows 2000 partition. Deleting an existing partition also erases any data on that partition.

Key Point
During Setup, create and size only the partition on which you will install Windows 2000.

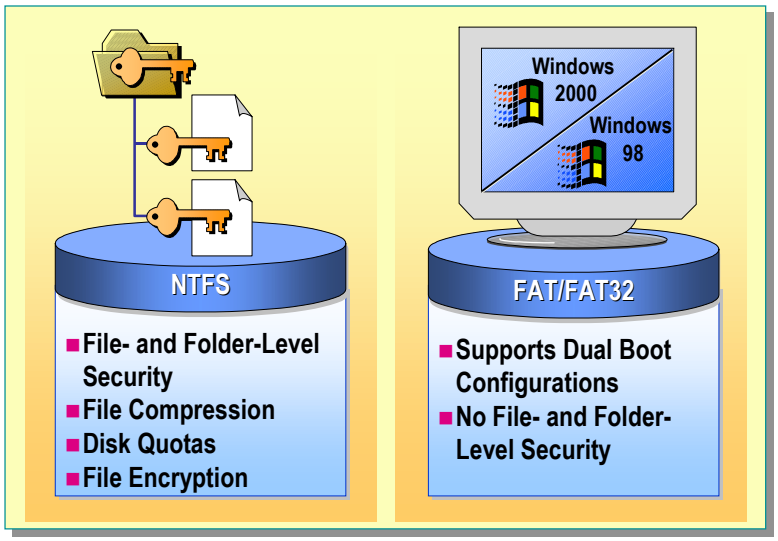
If you select a new partition during Setup, create and size only the partition on which you will install Windows 2000. After you install Windows 2000, use Disk Management to partition remaining space on the hard disk.

Note Disk Management is a system utility for managing hard disks and the volumes, or partitions, that they contain. For more information about disk management, see module 12, "Configuring and Managing Disks," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Determining Which File System to Select

Topic Objective
To illustrate the file system options that Windows 2000 supports.

Lead-in
After you choose a disk partition option, select a file system with which to format the partition.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Tell students that in most situations, they should format the hard disk with NTFS. The only reason to use FAT or FAT32 is for a dual boot configuration. Microsoft does not recommend having a dual boot configuration on a server.

After you create the partition on which you will install Windows 2000, Setup allows you to select the file system with which to format the partition. Windows 2000 supports the NTFS, FAT, and FAT 32 file systems.

NTFS

NTFS is the recommended file system for Windows 2000. Use NTFS for partitions that require:

- File- and folder-level security. NTFS allows you to control access to files and folders.
- File compression. NTFS compresses files to create more storage space.
- Disk quotas. NTFS allows you to control disk usage on a per-user basis.
- File encryption. NTFS allows you to transparently encrypt file data.

Windows 2000 and Windows NT are the only operating systems that can access data on a local hard disk that is formatted with NTFS.

FAT and FAT32

Normally, you would not format the partition on which Windows 2000 resides with FAT or FAT32 unless you require a dual boot configuration.

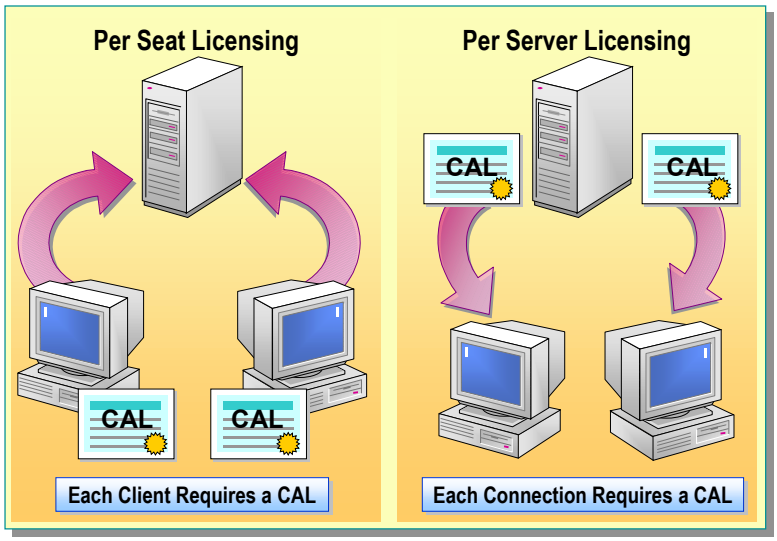
Note A dual boot configuration allows you to choose between two or more operating systems each time you restart the computer. When the operating system starts, a display appears for a specified number of seconds, allowing you to select between the operating systems.

The FAT file system does not support partitions larger than 2 GB. If you attempt to format a partition larger than 2 GB with FAT, Setup automatically formats the partition with FAT32.

Determining Which Licensing Mode to Select

Topic Objective
To illustrate the licensing modes for Windows 2000 Advanced Server.

Lead-in
Selecting a licensing mode for your environment is required during Setup.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
A CAL is required for client access to file and print services.

When you install Windows 2000 Advanced Server, you need a Client Access License (CAL) for each client computer that connects to the server in addition to the license that is required to install and run Windows 2000. You can select either Per Seat or Per Server licensing modes.

Per Seat. Requires a separate CAL for each client computer that accesses a Windows 2000 Advanced Server. With one CAL, a client computer can connect to any number of computers running Windows 2000 Advanced Server. Organizations with more than one server running Windows 2000 Advanced Server commonly use Per Seat licensing mode.

Per Server. Requires a CAL for each concurrent connection to the server. This means that at any given time, a server running Windows 2000 Advanced Server supports a fixed number of connections. This option is preferred for organizations whose users will not always be connected to a server.

Key Point
The licensing mode can be converted from Per Server to Per Seat, but not from Per Seat to Per Server.

Important If you are unsure which mode to use, choose Per Server because you can change from Per Server to Per Seat once at no cost. You cannot convert from Per Seat to Per Server.

CALs are not required for:

- Anonymous access to a computer running Windows 2000 Advanced Server with Internet Information Services (IIS) or another Web server application.
- Telnet and File Transfer Protocol (FTP) connections.

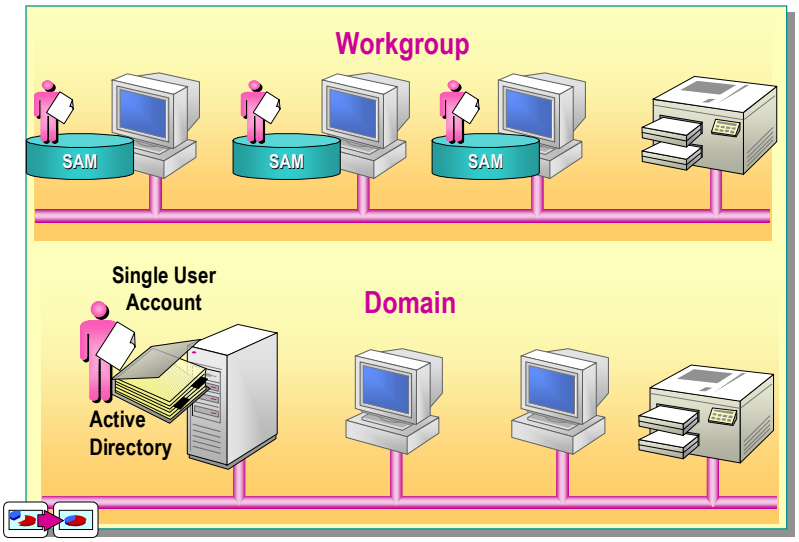
Explain that licensing for the client operating system does not include a CAL.

When you install Windows 2000 Professional, licensing for the operating system is accomplished by entering the Product ID found on the packaging material.

Determining Whether to Join a Workgroup or Domain

Topic Objective
To identify the difference between a domain and workgroup.

Lead-in
During installation you must provide the name of workgroup or domain the computer is joining.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
When presenting the information user accounts in workgroups and domains, use the whiteboard to draw how the different authentication processes take place.

The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

Key Point
Each computer in a workgroup has its own security database, while there is only one directory database in a domain.

When you install Windows 2000 you need to have the computer join either a workgroup or a domain. You must provide the name of the workgroup or domain during the installation.

Workgroup

A workgroup is a small group of networked computers that work together and where centralized administration is not required.

A workgroup has the following characteristics:

- Resources, administration, and authentication of users are performed on each computer in the workgroup.
- Each computer has its own local Security Accounts Manager (SAM) database, which is the local security accounts database. A user must have a user account on each computer to which she or he wants to gain access.
- There are 10 or fewer computers. These can be computers running one of the Windows 2000 server products, but each has its own SAM. Workgroups become more difficult to manage when there are more than 10 computers. In addition, the number of simultaneous connections a computer running Windows 2000 Professional can have is 10.

In Windows 2000, a domain is a logical grouping of networked computers that share a common security database for storing security information. Security and centralized administration are important for computers in a domain.

Key Point
A user only needs one user account to gain access to network resources residing on multiple computers in the domain.

Characteristics of the Domain

A domain has the following characteristics:

- Resources, administration, and authentication of users are centralized.
- There is only one directory database in Windows 2000 that stores all of the user accounts for the domain. This database is called the Active Directory™ directory service. A user needs only one domain user account in Active Directory to gain access to all shared network resources in the domain.
- Domains are scalable. They can easily support a small group of computers to several thousand computers.

Key Points
To add a computer to a domain, you must have a domain user account. For a computer to join a domain, it must have an existing domain computer account, or you must have the ability to create a domain computer account during installation.

User and Computer Accounts Required When Joining a Domain

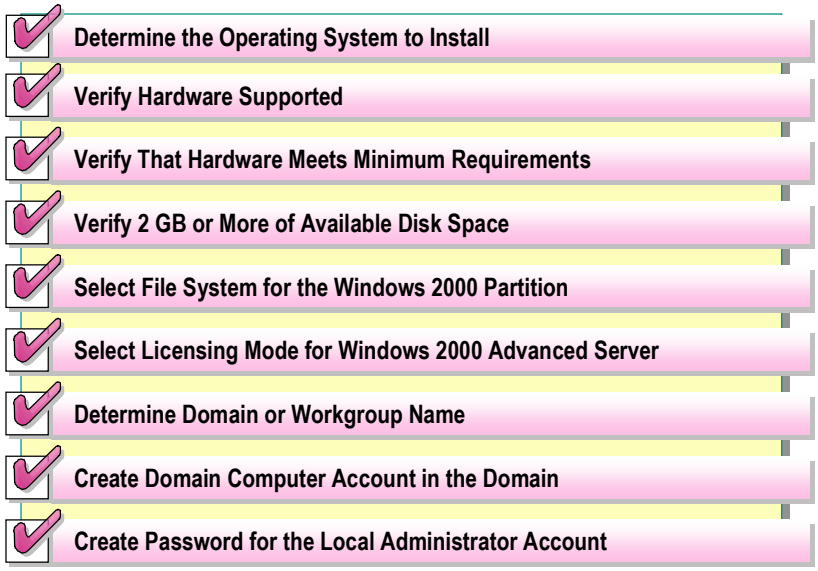
In a Windows 2000 domain, each computer in the domains as a computer account. When a computer joins a domain the appropriate user and computer account must exist. To join a domain:

- You must have a user account that exists in Active Directory. This does not need to be the domain Administrator account, but any domain user account.
- The computer must have either:
  - An existing computer account in the Active Directory database of the domain that the computer is joining. You must use a computer name that matches the computer name listed in Active Directory.
  - A computer account created in the Active Directory database during the installation by a user with the ability to create a domain computer account. By default, any domain user account can create up to 10 computer accounts.

Completing a Pre-Installation Checklist

Topic Objective
To identify the tasks to complete before you install Windows 2000.

Lead-in
Completing this checklist of pre-installation tasks will help you to perform a successful installation.



**********ILLEGAL FOR NON-TRAINER USE**********

Before you install Windows 2000, complete the following pre-installation tasks:

- Select which Windows 2000 operating system to install.
- Verify that all of your hardware appears on the HCL.

Explain that domain controllers will require a larger amount of free disk space.

- Verify that your computers meet the minimum system requirements. For more information about system requirements, see the Windows 2000 Product Guide Web site at http://www.microsoft.com/windows2000/guide
- Verify that the hard disk on which you will install Windows 2000 has at least 2 GB of hard disk space with the recommended minimum amount of free disk space (650 MB for Windows 2000 Professional and 850 MB for Windows 2000 Advanced Server).
- Select the file system for the partition on which you will install Windows 2000. Unless you need a dual boot configuration, format this partition with NTFS.

Key Points
To complete an installation, there must be a computer account for the computer on which the administrator is installing Windows 2000.

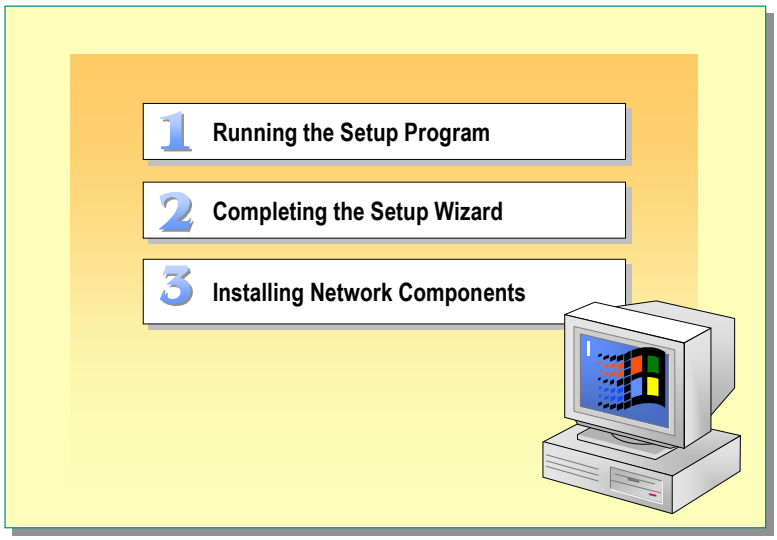
This computer account must exist before the installation or the user must have the ability to create it during the installation.

- If installing Windows 2000 Advanced Server, determine whether to use the Per Server or Per Seat licensing mode. If you select the Per Server licensing mode, verify the number of CALs that were purchased for the server.
- Determine the name of the domain or workgroup that you will join or create. If you will be joining a domain, enter the server name and domain name. If you will be joining a workgroup, enter the workgroup name.
- Verify that a computer account exists in the domain that you are joining or that you have the ability to create an account during installation.
- Decide on a password for the Administrator account for the local computer that will be created during installation.

◆ Installing Windows 2000 Professional from a Compact Disc

Topic Objective
To identify the steps for installing Windows 2000 Professional from a compact disc.

Lead-in
There are three parts to installing Windows 2000 Professional from a compact disc. They are running the Setup program, completing the Setup wizard, and installing network components.



**********ILLEGAL FOR NON-TRAINER USE**********

Mention that this installation is on a computer that has an operating system installed.

You want to ensure that Windows 2000 is successfully installed on client computers so that users are able to focus on their work and not on operating system problems. To install Windows 2000 Professional from a compact disc, you start the computer from the compact disc or Setup disks, run the Setup program, complete the Setup wizard, and then configure network settings for a workgroup.

Running the Setup Program

Topic Objective
To identify the tasks involved in running the Setup program.

Lead-in
Now you will look at running the Setup program on a computer that has an operating system installed. Starting the Setup program is very easy.

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Use the Windows 2000 Professional Installation simulation for this topic and the following two topics.

Mention to students that the simulation is on the Student Materials compact disc. To view the Windows 2000 Professional Installation simulation, open the Web page on the Student Materials compact disc, click **Lab Simulations**, and then click the title of the simulation.

The first part of the Setup program is text based. To run the Setup program, perform the following tasks:

1. Start the computer from the compact disc or the Setup disks (if you do not have a bootable CD-ROM drive), and insert the additional Setup disks when prompted.

Note To create the Setup disks, run the Makeboot.exe program from another computer running Windows 2000. Makeboot.exe is located in the Bootdisk folder on the Windows 2000 compact disc. To create a Setup disk, click **Start**, click **Run**, type **makeboot a:** in the **Open** box, and then click **OK**.

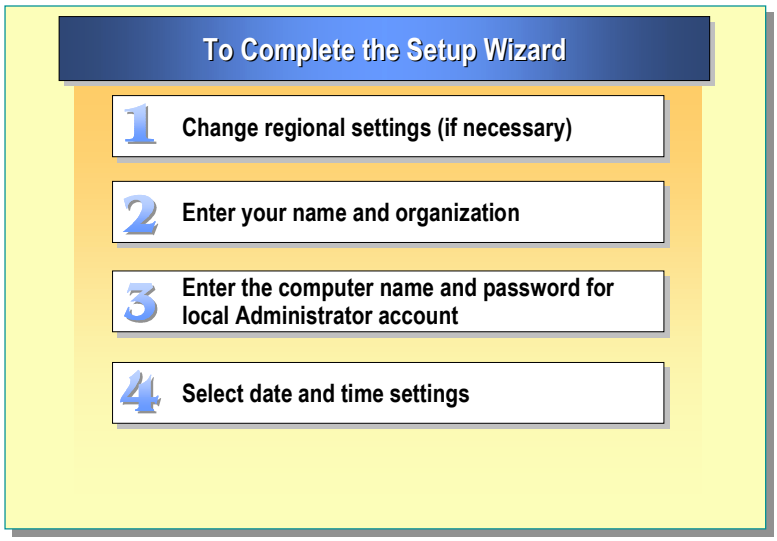
---

2. Select to install a new copy of Windows 2000.
3. Read and accept the licensing agreement.
4. Select the partition on which to install Windows 2000.
5. Select a file system for the new partition. If installing the operating system on an existing FAT or FAT 32 partition, you can specify whether you want to convert the partition to NTFS.

Completing the Setup Wizard

Topic Objective
To identify the tasks involved in completing the Setup wizard.

Lead-in
After you finish the text-based portion of the installation, you must complete the Setup wizard.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Continue using the Windows 2000 Professional Installation simulation to demonstrate the steps.

After running the text-based portion of the Setup program, complete the Setup wizard by performing the following steps:

1. Change regional settings, if necessary.

Setting	Description
Current System Locale	Affects the way programs display dates, times, currency, and numbers. You usually choose the locale that matches your location, for example, French (Canada).
Current Keyboard Layout	Accommodates the special characters and symbols used in different languages. Your keyboard layout determines which characters appear when you press keys on the keyboard.

2. Enter your name and organization.
3. Enter the computer name and password for the local Administrator account. This user account resides in the SAM of the computer and not in Active Directory.

Mention the Tip to the students. Stress the importance of using complex passwords to enhance network security.

Tip To increase security on your network, it is recommended that you use complex passwords that are hard to guess.

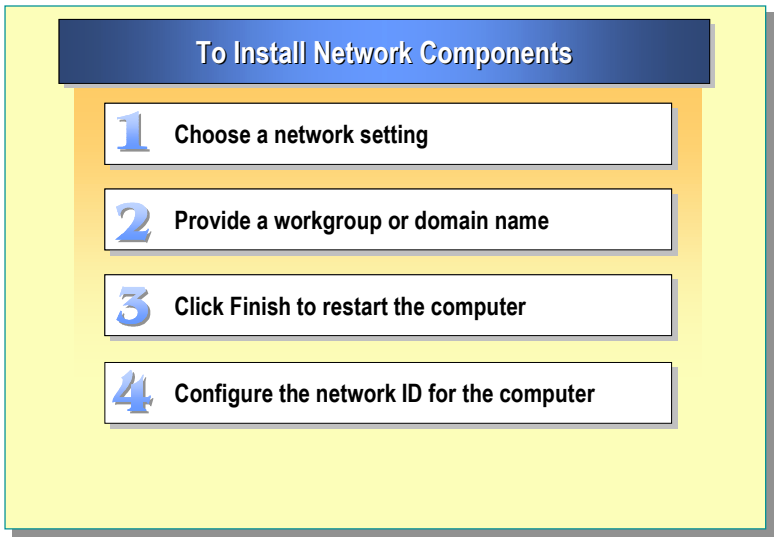
4. Select the date, time, and time zone settings.

   Configuring the correct date and time settings is critical. A date or time setting that differs from that of servers on the network can cause problems when joining a domain.

Installing Network Components

Topic Objective
To identify the tasks involved in installing network components.

Lead-in
The final step in the installation of Windows 2000 Professional is to install the network components.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Continue using the Windows 2000 Professional Installation simulation to demonstrate the steps.

After completing the Setup wizard, install network components by performing the following steps:

1. Choose a networking setting.

Setting	Description
Typical	Installs Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks, and Transmission Control Protocol/Internet Protocol (TCP/IP).
Custom	Creates custom network connections: for example, configuring a static IP address, configuring the computer as a WINS client, or adding NetBIOS Enhanced User Interface (NetBEUI).

2. Provide a workgroup or domain name.
3. Click **Finish** to restart the computer.
4. Configure the network ID for the computer.

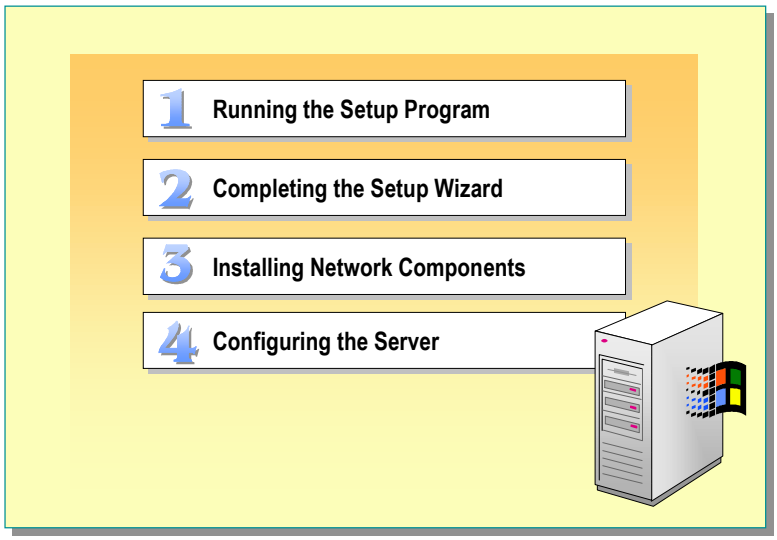
   After the computer restarts, Windows 2000 Professional displays the Network ID wizard. In this wizard, you do either of the following.

   - Configure a specific user account and password for the computer. When a user starts the computer, Windows 2000 automatically logs on using the configured user name and password.
   - Choose not to configure a specific user account for the computer. When a user starts the computer, the **Log On to Windows** dialog box appears.

◆ Installing Windows 2000 Advanced Server from a Compact Disc

Topic Objective
To describe the installation process for Windows 2000 Advanced Server.

Lead-in
The steps to install Windows 2000 Advanced Server are almost identical to installing Windows 2000 Professional. There are extra options available that you can configure for Windows 2000 Advanced Server.



**********ILLEGAL FOR NON-TRAINER USE**********

Mention to the student that this installation is performed on a computer without an operating system.

To install Windows 2000 Advanced Server from a compact disc, you must start the computer from a compact disc or from the Setup disks, and then complete the Setup wizard. With the exception of the optional components, the information you provide during an installation of Windows 2000 Advanced Server is the same as the information you provide during an installation of Windows 2000 Professional. In addition, with Windows 2000 Advanced Server, you are provided the option to further configure the server after the installation finishes by using the Configure Your Server wizard.

Running the Setup Program

Topic Objective
To identify the tasks in running the Setup program when installing Windows 2000 Advanced Server.

Lead-in
The tasks involved in the running the Setup program for Windows 2000 Advanced Server are the same as for Windows 2000 Professional.

**********ILLEGAL FOR NON-TRAINER USE**********

To run the text-based portion of the Setup program, perform the following tasks:

1. Start the computer from the compact disc or from the Setup disks.

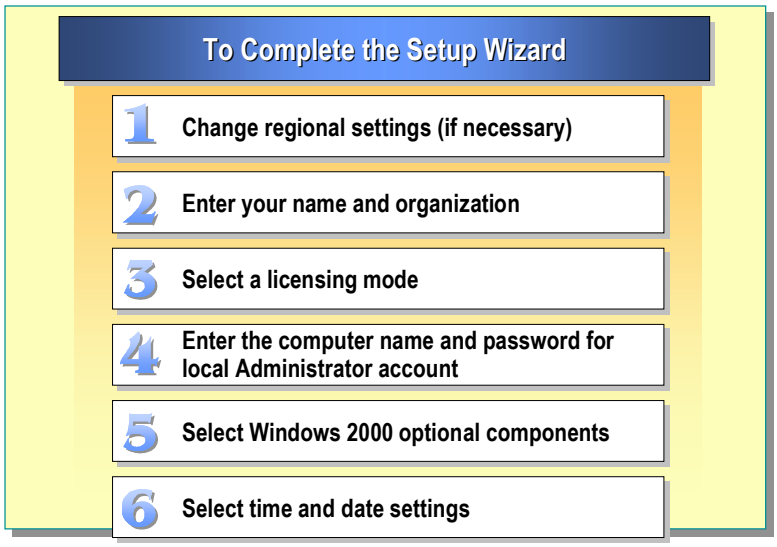
   Note To create the Setup disks, run the Makeboot.exe program from another computer running Windows 2000. Makeboot.exe is located in the Bootdisk folder on the Windows 2000 compact disc. To create a Setup disk, click **Start**, click **Run**, type **makeboot a**: in the **Open** box, and then click **OK**.

2. Select to install a new copy of Windows 2000.
3. Read and accept the licensing agreement.
4. Select the partition on which to install Windows 2000.
5. Select a file system for the new partition. You can also choose to format the new partition.

Completing the Setup Wizard

Topic Objective
To identify the tasks involved in completing the Setup wizard for Windows 2000 Advanced Server.

Lead-in
After the Setup program is finished, you then complete the Setup wizard.



**********ILLEGAL FOR NON-TRAINER USE**********

After running the text-based portion of the Setup program, complete the Setup wizard by providing the following information:

1. Change regional settings, if necessary.
2. Enter your name and organization.
3. Select a licensing mode.
4. Enter the computer name and password for the local Administrator account.
5. Select the Windows 2000 optional components. Optional components provide additional functionality to Windows 2000, such as Web services, Remote Installation Services (RIS), and management tools. The components you choose are determined by how you intend to use your server. The following table describes these optional components.

Key Points
You can install optional components during Setup, or you can add them later through Add/Remove Programs in Control Panel.

Component	Description
Certificate Services	Allows you to create and request digital certificates for authentication. Certificates provide a verifiable means of identifying users on nonsecure networks, such as the Internet.
Windows Clustering	Enables two or more servers to work together to keep server-based applications available, regardless of individual component features. This service is available only in Windows 2000 Advanced Server and Windows 2000 Datacenter Server.
IIS	Includes FTP and Web servers, the administrative interface for IIS, common IIS components, and documentation.

(continued)

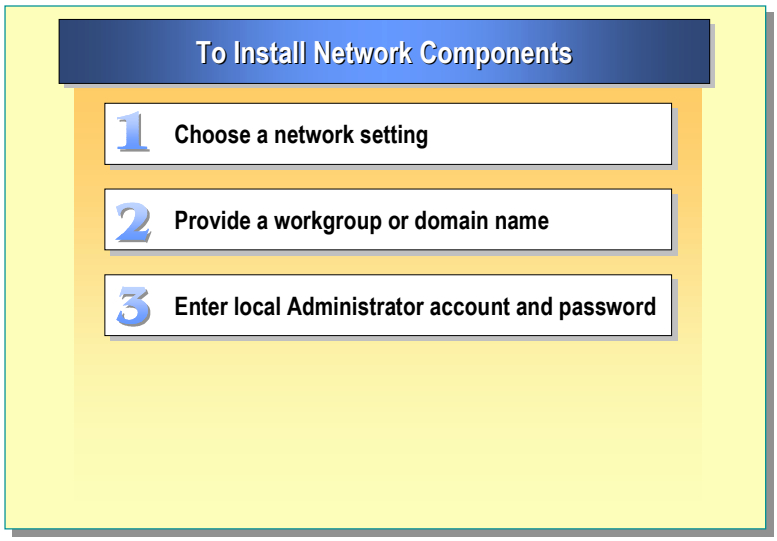
Component	Description
Management and Monitoring Tools	Includes tools for monitoring and improving network performance.
Message Queuing	Supports applications that send messages to queues. Queues act like caches, controlling the flow of data to destinations, and ensuring that messages reach their destinations. Message Queuing also allows applications to communicate across heterogeneous networks and with computers that may be temporarily offline.
Microsoft Indexing Service	Enables dynamic full-text searches of data that is stored on the computer or network.
Microsoft Script Debugger	Allows client- and server-side debugging of Microsoft ActiveX® script engines, such as a script written in Microsoft Visual Basic®, Scripting Edition (VBScript), or Microsoft JScript®.
Networking Services	Includes the DHCP Server service, DNS Server service, TCP/IP, and other networking components.
Other Network File and Print Services	Enables sharing of files and printers on this computer with Macintosh and UNIX-based computers.
Remote Installation Services	Enables remote installation of Windows 2000 Professional over a network connection.
Remote Storage	Allows the user to use tape libraries as extensions of NTFS volumes, automatically moving data to and from tape media.
Terminal Services	Enables Windows-based clients to gain access to a virtual Windows 2000 Advanced Server desktop session and Windows-based applications.

6. Set the date, time, and time zone settings.

Installing Network Components

Topic Objective
To identify the task in installing network components during an installation of Windows 2000 Advanced Server.

Lead-in
After completing the Setup wizard, you install of the network components.



**********ILLEGAL FOR NON-TRAINER USE**********

After completing the Setup wizard, install network components by performing the following steps:

1. Click **Typical** or **Customized** for the networking components.
2. Provide a workgroup or domain name.

Note For more information about workgroups and domains, see course 2153A, *Implementing a Microsoft Windows 2000 Networking Infrastructure*.

3. After completing the installation process, Setup displays the **Welcome to Windows** screen. You must enter the Administrator account password for the local computer in order to log on.

Configuring the Server

Topic Objective
To identify what can be configured on the **Windows 2000 Configure Your Server** page.

Lead-in
After the installation is completed, Windows 2000 Advanced Server provides you with the opportunity to configure the server.

**********ILLEGAL FOR NON-TRAINER USE**********

After the installation is completed, Windows 2000 Advanced Server offers you the opportunity to further configure the server.

Note If you choose not to configure the server at this point, you can do it later. To gain access to the **Windows 2000 Configure Your Server** page, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Configure Your Server**.

On the **Windows 2000 Configure Your Server** page, you can configure the following.

- *Active Directory*. You can configure the server as a domain controller and set up Domain Name System (DNS) if it is not already available on the network.
- *File server*. You can create the shared folders to be stored on the server.
- *Print server*. You can set up a local or network printer and have them publish to Active Directory.
- *Web/Media server*. You can use this to gain a strong internal or external Web presence. This includes using IIS to set up a Web or FTP site on your corporate intranet and creating a streaming multimedia presentation.
- *Networking*. You can select the networking services you want to use.
- *Application server*. You can set up the computer as an application server.
- *More advanced configurations*. You can set up advanced configurations, such as message queuing, Windows 2000 support tools, and advanced services.

Lab A: Installing Windows 2000

Topic Objective
To introduce the lab.

Lead-in
In this lab, install Windows 2000 Advanced Server from a compact disc.

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
If time is critical, you can start lecturing before the end of the lab. Start lecturing during the text portion of the installation when the files are being copied from the CD-ROM to the hard drive.

Objectives

After completing this lab, you will be able to:

- Install Windows 2000 Advanced Server as a member server of a workgroup.
- Move a computer running Windows 2000 Advanced Server from a workgroup to a domain.

Prerequisites

Before working on this lab, you must have a computer meeting the minimum hardware requirements for installing Windows 2000 Advanced Server.

Lab Setup

To complete this lab, you need the following:

- The Windows 2000 Advanced Server compact disc.
- The four Windows 2000 Advanced Server Setup disks (optional). If your computer is configured with a bootable CD-ROM drive, you can install Windows 2000 without using the Setup disks.
- A computer name and IP address; refer to the Student Computer Names and IP Addresses section of the lab for this information.

For More Information

For more information about installing Windows 2000 Advanced Server, see the Release Notes, which can be found on the Windows 2000 Advanced Server compact disc.

Student Computer Names and IP Addresses

The organization of the classroom is meant to simulate a worldwide trading firm named Northwind Traders. Its fictitious domain name is nwtraders.msft. The primary DNS server for nwtraders.msft is the instructor computer, which has an IP address of 192.168.*x*.200 (where *x* is the assigned classroom number). The name of the instructor computer is London.

The following table provides the computer name and IP address of each student computer in the fictitious domain nwtraders.msft. Find the student number that the instructor has assigned you, and make a note of the computer name and IP address for your student number (where *x* is the assigned classroom number).

Student number	Computer name	IP address
01	Vancouver	192.168.*x*.1
02	Denver	192.168.*x*.2
03	Perth	192.168.*x*.3
04	Brisbane	192.168.*x*.4
05	Lisbon	192.168.*x*.5
06	Bonn	192.168.*x*.6
07	Lima	192.168.*x*.7
08	Santiago	192.168.*x*.8
09	Bangalore	192.168.*x*.9
10	Singapore	192.168.*x*.10
11	Casablanca	192.168.*x*.11
12	Tunis	192.168.*x*.12
13	Acapulco	192.168.*x*.13
14	Miami	192.168.*x*.14
15	Auckland	192.168.*x*.15
16	Suva	192.168.*x*.16
17	Stockholm	192.168.*x*.17
18	Moscow	192.168.*x*.18
19	Caracas	192.168.*x*.19
20	Montevideo	192.168.*x*.20
21	Manila	192.168.*x*.21
22	Tokyo	192.168.*x*.22
23	Khartoum	192.168.*x*.23
24	Nairobi	192.168.*x*.24

Estimated time to complete this lab: 75 minutes

Exercise 1
Installing Windows 2000 Advanced Server

Scenario

Your company, Northwind Traders, needs to set up a server in the domain.

Goal

In this exercise, you will install Windows 2000 Advanced Server from a compact disc. As part of the installation, you will create a 2-gigabyte (GB) partition formatted as an NTFS partition. The default settings will be used for everything except the computer name and TCP/IP settings. You will configure the computer name and TCP/IP settings using the chart at the beginning of this exercise. First, you install the server as a member of a workgroup named workgroup, and then you join the server to the domain named nwtraders.msft.

Tasks	Detailed Steps
1. Begin text-mode Setup of Windows 2000 Advanced Server. Create a new 2000 megabyte (MB) partition specifying the NTFS file system.	**a.** Start the computer with the Windows 2000 Advanced Server compact disc.
Note: If your computer does not have a bootable CD-ROM drive, start the computer from the Windows 2000 boot disk, and then insert the other three disks when prompted.	
1. (*continued*)	**b.** When the **Setup Notification** screen appears, press ENTER. **c.** When the **Welcome to Setup** screen appears, press ENTER.
Note: If a screen appears indicating that the hard disk is new or has been erased, press C to continue.	
1. (*continued*)	**d.** When the **Windows 2000 Licensing Agreement** screen appears, read the agreement, and then press F8 to accept the licensing terms. **e.** In the list of existing partitions, press C to create a partition on disk 0. **f.** When you are prompted to select a partition size, in the **Create partition of size (in MB)** box, delete the existing value, type **2000** and then press ENTER. **g.** In the list of existing partitions, press ENTER to select the **C: New (Unformatted) 2001 MB** partition. *Setup displays a list of options for formatting the partition.*

Tasks	Detailed Steps
If you were installing Windows 2000 on a computer that was currently running Microsoft Windows 98 and you wanted to have a dual boot configuration, which file system should you choose for the C partition? Why? **FAT (file allocation table) or FAT32. Windows 98 cannot access a partition formatted with NTFS.**	
1. (*continued*)	**h.** Press ENTER to select **Format the partition using the NTFS file system**. *Setup formats the partition, examines the hard disk, and then copies files to the Windows 2000 installation folders.* **i.** If you started the installation from a floppy disk, remove it from the drive. **j.** Leave the Windows 2000 Advanced Server compact disc in the CD-ROM drive. *The computer restarts automatically.*
2. Begin GUI-mode Setup of Windows 2000 Advanced Server by using the following information: • For the computer name, use your computer name as listed in the table at the beginning of this exercise. • For the Product Key, use the product key provided by your instructor. • For the name and organization, use your name and Northwind Traders. • For the licensing mode, use Per Server with 20 connections. • For the account, use the administrator account with a password of **password**. • Do not install any additional components and join the workgroup named workgroup.	**a.** On the **Welcome to the Windows 2000 Server Setup Wizard** page, click **Next**, or wait a few seconds for the installation process to continue automatically. *The **Installing Devices** page appears, indicating that you should wait while Setup detects and installs devices. Next, the **Regional Settings** page appears, prompting you to customize Windows 2000 for different regions and languages.* **b.** On the **Regional Settings** page, click **Next**. **c.** On the **Personalize Your Software** page, in the **Name** box, type your name, in the **Organization** box, type **Northwind Traders** and then click **Next**. **d.** On the **Your Product Key** page, type the product key provided by your instructor. *The **Licensing Modes** page appears, prompting you to choose a licensing mode.*

Tasks	Detailed Steps
?	Which licensing mode should you choose if you have one server running Windows 2000, 20 client computers, and the need for no more than five concurrent connections? **Per Server.**
?	Which licensing mode should you choose if you have five servers running Windows 2000, 20 client computers, and the need for all client computers to be concurrently connected to all servers? **Per Seat.**
?	Which licensing mode should you select if users in your organization require frequent access to multiple servers? Why? **Per Seat. The Per Seat licensing mode requires the least number of licenses when users make connections to multiple servers. Per Server licensing requires a license for each concurrent connection to the server. Per Server is the best option for organizations in which users make connections to only one server.**

Tasks	Detailed Steps
2. (*continued*)	**e.** Verify that **Per server** is selected, in the **Number of concurrent connections** box, type **20** and then click **Next**. **f.** On the **Computer Name and Administrator Password** page, type the following information, and then click **Next**: Computer name: *Server* (where *Server* is your assigned computer name, refer to the table at the beginning of the lab) Password: **password** Confirm password: **password** *The **Windows 2000 Components** page appears, which you can use to add or remove components. Do not install any additional components at this time as you will be installing additional components in later labs.* **g.** On the **Windows 2000 Components** page, click **Next**. **h.** On the **Date and Time Settings** page, adjust the date, time, and time zone on your computer as necessary, and then click **Next**. *The **Networking Settings** page appears, indicating that Windows 2000 is installing networking components, and then prompts you to choose typical or custom network settings.*
3. Complete the networking portion of the installation wizard using the following information: • The static IP address listed in the table at the beginning of this exercise, and the instructor's IP address for the DNS server. • Join a workgroup using the default workgroup name.	**a.** In the **Network Settings** dialog box, click **Custom settings**, and then click **Next**. **b.** On the **Networking Components** page, click **Internet Protocol (TCP/IP)**, and then click **Properties**. **c.** In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Use the following IP address**, type the IP address that is assigned to your computer (refer to the table at the beginning of the lab), and then press TAB. *The default subnet mask of 255.255.255.0 appears.* **d.** Verify that **Use the following DNS server addresses** is selected. **e.** In the **Preferred DNS server** box, type the IP address of the instructor's computer, and then click **OK**.
Important: On the **Networking Components** page be sure to click **Next** only once. Clicking **Next** twice will bypass the **Workgroup or Computer Domain** page.	
3. (*continued*)	**f.** On the **Networking Components** page, click **Next**. *The **Workgroup or Computer Domain** page appears, prompting you to join either a domain or a workgroup.*

Tasks	Detailed Steps
What type of account must exist before a Windows 2000 computer can join a domain, and when can you create the account? **A computer account for your computer must exist or be created in the domain that you are joining. This can be done as part of the installation process by any user, or can be created by a user with administrative rights in the domain before the computer joins the domain.**	
3. (*continued*)	**g.** Verify that **No, this computer is not on a network, or is on a network without a domain** is selected. **h.** In the **Workgroup or computer domain** box, verify that **WORKGROUP** appears, and then click **Next**. *The **Installing Components** page appears, indicating that Setup is installing Windows 2000 components. Next, the **Performing Final Tasks** page appears, indicating that Setup is completing a final set of tasks.* **i.** Leave the Windows 2000 Advanced Server compact disc in the CD-ROM drive. **j.** On the **Completing the Windows 2000 Setup Wizard** page, click **Finish**. *The computer restarts.*

Exercise 2
Joining a Domain

Scenario

You have installed a server and fully tested it for proper operation. You now want to make it a member server of a domain.

Goal

In this exercise, you will configure your computer to be a member server in the nwtraders.msft domain. You will use a domain-based user account with administrative rights over your assigned domain to create a computer account in the domain, thereby allowing the computer to join the domain.

Tasks	Detailed Steps
1. Log on as Administrator with the password of **password** and complete the Configure Your Server wizard specifying that there are other servers present on the network and you do not want the Configure Your Server wizard to appear each time you restart.	**a.** Press CTRL+ALT+DELETE. **b.** In the **Log On to Windows** dialog box, click **Options**. **c.** Verify that the options **User name**, **Password**, and **Log on using dial-up connection** display.
Is your computer a member of a domain? How can you tell from the **Log On to Windows** dialog box? **No. Because you cannot select the domain.**	
1. (*continued*)	**d.** In the **Log On to Windows** dialog box, click **Options**. **e.** In the **Log On to Windows** dialog box, in the **Password** box, type **password** and then press ENTER. *The system verifies your user credentials, you are logged on, and the Configure Your Server wizard appears.* **f.** In the **Windows 2000 Configure your Server** wizard, click **One or more servers are already running in my network**, and then click **Next**. **g.** Clear the **Show this screen at startup** check box, and then close the Configure Your Server wizard. **h.** Press CTRL+ALT+DELETE.

Tasks	Detailed Steps
	On the **Windows Security** dialog box, under **Logon Information**, what account is logged on? What is this account logged on to? **The administrator account is logged on to *Server* (where *Server* is your computer name).**
1. (*continued*)	**i.** Click **Cancel** to close the Windows Security dialog box.
2. Configure your server to be a member server of the nwtraders.msft domain. The user account you will use to join the domain is Admin*x* (where *x* is your assigned student number) with a password of **domain**.	**a.** Click **Start**, point to **Settings**, and then click **Control Panel**. **b.** In Control Panel, double-click **System**. **c.** In the **System Properties** dialog box, on the **Network Identification** tab, click **Properties**. **d.** In the **Identification Changes** dialog box, under **Member of**, select **Domain**. **e.** In the **Domain** box, type **nwtraders.msft** and then click **OK**. *A dialog box appears requesting user credentials for the domain.* **f.** In the **Domain Username and Password** dialog box, in the **Name** box, type **nwtraders\admin***x* (where *x* is your assigned student number). **g.** In the **Password** box, type **domain** and then click **OK**. *A welcome message appears indicating that the computer was successful in joining the domain.* **h.** In the **Network Identification** message box, click **OK**. *Another message appears indicating that you must restart the computer for the changes you made to take effect.* **i.** Click **OK** to close the **Network Identification** message box. **j.** Click **OK** to close the **System Properties** dialog box. **k.** Close Control Panel. **l.** In the **System Settings Change** dialog box, click **Yes**. *Your computer restarts*.

Exercise 3
Configuring Windows 2000 Advanced Server for the Classroom Environment

Scenario

To properly configure you computer for the classroom environment, you must configure your display settings and install student files that will be used in later labs.

Goal

In this exercise you will configure Windows 2000 Advanced Server for the classroom lab environment by installing the student lab files and by reconfiguring the display settings to 800 x 600 with 256 colors.

Tasks	Detailed Steps
1. Log on to *Server* (where *Server* is your computer name) as Administrator with the password of **password** and configure the display settings to 800 x 600 with 256 colors.	**a.** Press CTRL+ALT+DELETE. **b.** In the **Log On to Windows** dialog box, click **Options**. **c.** In the **Log on to** box, click the down arrow.
Is your computer a member of a domain? How can you tell from the **Log On to Windows** dialog box? **Yes. Because the domain nwtraders displays.**	
1. (*continued*)	**d.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **e.** Press CTRL+ALT+DELETE.
On the **Windows Security** dialog box, under Logon Information what account is logged on? What is this account logged on to? **The administrator account is logged on to *Server* (where *Server* is your computer name).**	

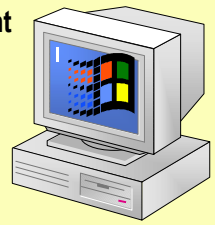
Tasks	Detailed Steps
1. (*continued*)	**f.** Right-click the desktop, and then click **Properties**. **g.** On the **Settings** tab, under **Colors**, click **256 Colors**, and under **Screen area**, specify 800 by 600 pixels, and then click **OK**. *The **Display Properties** message appears, indicating that Windows 2000 will now apply your new desktop settings.* **h.** Click **OK**, and then when prompted to keep these settings, click **Yes**.
2. Run student.vbs from the shared folder \\London\Setup.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\london\setup\student.vbs** and then click **OK**. **c.** In the **VBScript** message box, click **OK**. *A status window appears indicating the progress of the student computer setup.* **d.** When the **Setup of this student computer is now complete** message appears, close the status window. **e.** Close any open windows, and then log off.

◆ Upgrading to Windows 2000 Professional

Topic Objective
To identify the topics for upgrading client computers to Windows 2000 Professional.

Lead-in
Windows client operating systems can be upgraded to Windows 2000, but you must check hardware compatibility before attempting the upgrade.

- **Identifying Client Upgrade Paths**
- **Upgrading Clients Running Windows 95 or Windows 98**
- **Upgrading Clients Running Windows NT Workstation 3.5.1 or 4.0**
- **Installing the Directory Service Client**



**********ILLEGAL FOR NON-TRAINER USE**********

You can upgrade most Windows client operating systems directly to Windows 2000 Professional. If you upgrade, instead of installing, you do not lose the settings and applications already installed.

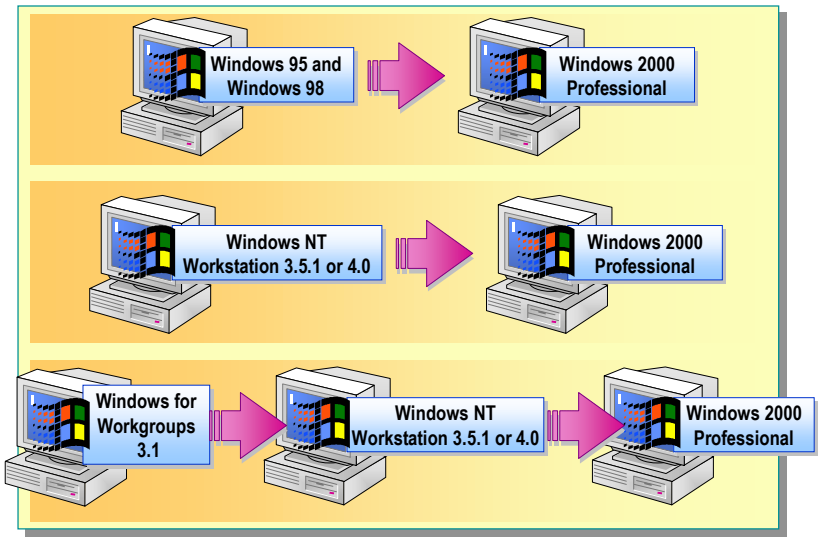
Before upgrading the operating systems on a client computer to Windows 2000 Professional, you must ensure that the computer hardware meets the Windows 2000 Professional hardware requirements.

If client computers running Windows 95 and Windows 98 use incompatible or insufficient hardware and you do not want to upgrade them, you can install Windows 2000 Directory Services Client. Then, these client computers can take advantage of a Windows 2000 network.

Identifying Client Upgrade Paths

Topic Objective
To identify the client upgrade paths for Windows 2000 Professional.

Lead-in
Windows NT 4.0 Workstation provides the best migration path for Windows 2000 Professional.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Windows 3.1 cannot be upgraded directly to Windows 2000 Professional. Windows 3.1 must first be upgraded to Windows 95 or Windows 98.

You can upgrade most client computers running earlier versions of Windows and Windows NT Workstation directly to Windows 2000 Professional. However, computers running Windows NT for Workgroups versions 3.1 or 3.5 require an additional step.

The following table lists the Windows 2000 Professional upgrade paths for client operating systems.

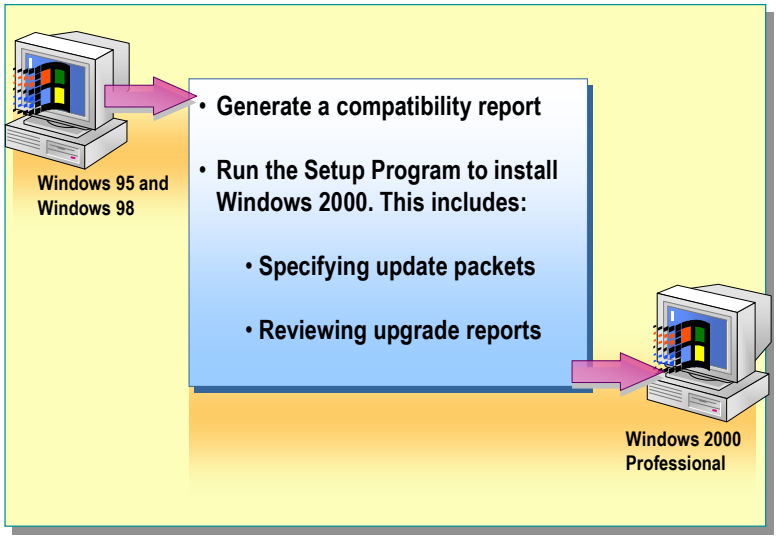
From	Upgrade to
Windows 95 and Windows 98	Windows 2000 Professional.
Windows NT Workstation 3.5.1 or 4.0	Windows 2000 Professional.
Windows for Workgroups 3.1	Windows NT Workstation versions 3.5.1 or 4.0 first, and then upgrade to Windows 2000 Professional.

Important You cannot upgrade Windows 3.1 directly to Windows 2000 Professional. You must first upgrade to Windows 95 or Windows 98, and then upgrade to Windows 2000 Professional.

Upgrading Clients Running Windows 95 or Windows 98

Topic Objective
To illustrate the upgrade process for clients running Windows 95 or Windows 98.

Lead-in
Windows 95 and Windows 98 upgrades can require more planning and testing than upgrades from Windows NT.



**********ILLEGAL FOR NON-TRAINER USE**********

Upgrading from Windows 95 or Windows 98 can require more planning and testing than an upgrade from Windows NT. Because of the differences in the system registry and setup procedures, many applications install differently on computers running Windows 95 and 98 than they do on computers running Windows NT Workstation 4.0 or Windows 2000 Professional.

Key Point
Setup provides a report-only mode that can generate compatibility reports. These reports provide you with information about incompatible features and applications before you perform the upgrade.

Generating a Compatibility Report

Windows 2000 provides a report-only mode that can generate compatibility reports. These reports provide you with information about incompatible features and applications before you perform the upgrade. You can analyze these reports to determine whether you need to install update packs or new versions of applications.

You can generate a compatibility report in two ways:

- Run the winnt32 /checkupgradeonly command

  This starts the first part of the Windows 2000 Setup program. Instead of running the entire Setup program, it only checks for compatible hardware and software, and then generates a compatibility report.

- Run the Windows 2000 Readiness Analyzer

  Use the Windows 2000 Readiness Analyzer to ensure that computers running Windows 95, Windows 98, or Windows NT can be upgraded to Windows 2000. The Windows 2000 Readiness Analyzer identifies installed devices and applications that are known to be incompatible with Windows 2000.

  Access the Windows 2000 Readiness Analyzer at http://www.microsoft.com/windows2000/upgrade/compat/default.asp After you download the Windows 2000 Readiness Analyzer RTW, start the utility. To start the utility, run Chkupgrd.exe.

Running the Setup Program

To run the Setup program, perform the following tasks:

1. Start the computer from the compact disc.
2. Select the **Upgrade to Windows 2000 (Recommended)** check box, and then click **Next**.
3. Read and accept the licensing agreement.
4. Specify any update packs required to make your applications work properly with Windows 2000. Update packs contain migration dynamic-link libraries (DLLs) that update an application so that it works in Windows 2000 Professional.
5. Select the partition on which to install Windows 2000. If you are installing the system onto an existing FAT partition, specify whether you want to convert the partition to NTFS.
6. Review the upgrade report.

   Setup generates an upgrade report to alert you to any compatibility problems. Every application on the computer is scanned for known problems and upgrade packs are recommended as needed.

   Note Stop the installation process only if the compatibility problems prevent the user from operating the computer. In most cases, these errors are associated with a specific application and you can resolve them after completing setup. You can print or save this report.

Explain that an administrator can also create a computer account prior to users performing the upgrade in order to control the names given to computers.

7. Join a domain.

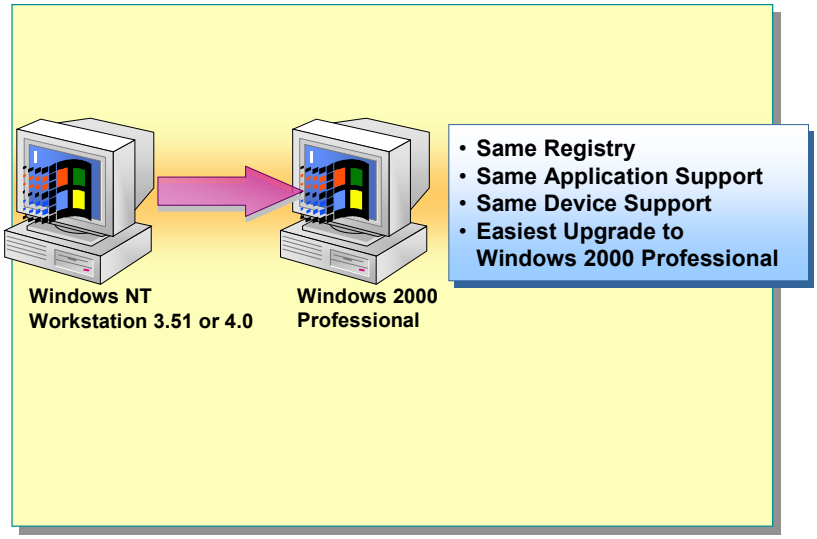
   Client computers running Windows 95 and Windows 98 do not have domain computer accounts. If the computer being upgraded is going to join a domain, a computer account must exist or you must create the domain computer account. This process is identical to the process for creating a domain user account during installation.
8. Finish running the Setup program, which migrates as much information as possible from the Windows 95 or Windows 98 registry and installs Windows 2000 Professional.

When the upgrade is complete, log on as the local administrator to review any errors that may have occurred.

Upgrading Clients Running Windows NT Workstation 3.5.1 or 4.0

Topic Objective
To illustrate the upgrade process for clients running Windows NT Workstation.

Lead-in
Upgrading from Windows NT is easier than upgrading from Windows 95 or Windows 98.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Upgrading from Windows NT Workstation to Windows 2000 Professional is easier than any other upgrade to Windows 2000.

Because Windows NT Workstation 3.5.1, Windows NT Workstation 4.0, and Windows 2000 Professional share common registry, file system, security, and operating system kernel structures, nearly all applications that run on Windows NT Workstation 4.0 will run without modification on Windows 2000 Professional. Upgrading from Windows NT Workstation to Windows 2000 Professional is easier than upgrading from other Windows operating systems because:

- Almost all peripherals and devices that worked with Windows NT Workstation 4.0 will work with Windows 2000 Professional.
- The version of NTFS used in Windows NT Workstation 4.0 is transparently upgraded to the version of NTFS used in Windows 2000 Professional during the upgrade process.

Note A few minor incompatibilities exist between the version of NTFS used in Windows NT Workstation 4.0 and the version of NTFS used in Windows 2000 Professional. For example, the anti-virus software that may use filters to scan files and drives. Because of updates to NTFS in Windows 2000 Professional, some Windows NT Workstation 4.0 file system filters will not work on Windows 2000 Professional.

Mention that when upgrading from Windows NT Workstation, an administrator can install the operating system onto a converted NTFS partition.

The upgrade process for client computers running Windows NT Workstation 3.5.1 and 4.0 is similar to the upgrade process for client computers running Windows 95 and Windows 98. To upgrade clients running Windows NT Workstation 3.5.1 or 4.0, perform the following tasks:

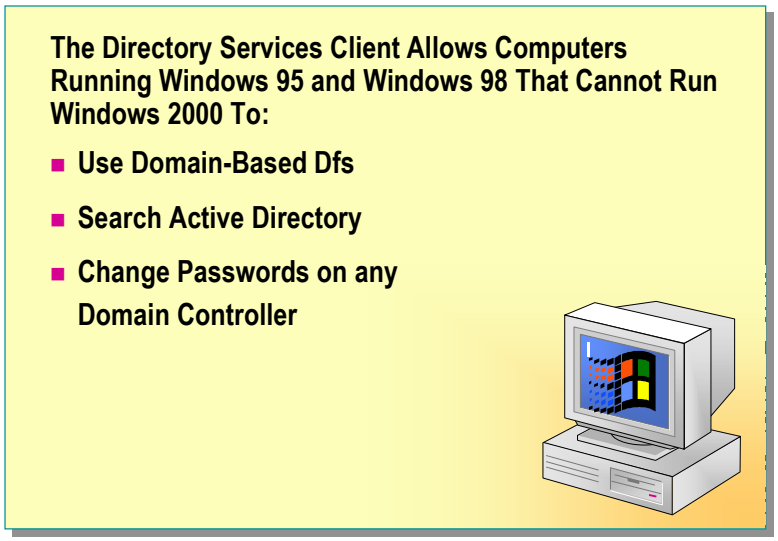
1. Start the computer from the compact disc.
2. Select the **Upgrade to Windows 2000 (Recommended)** check box, and then click **Next**.
3. Read and accept the licensing agreement.
4. If you are installing the system onto an existing FAT partition, specify whether you want to convert the partition to NTFS.

The files are copied, the computer restarts, and the upgrade finishes without further intervention.

Installing the Directory Services Client

Topic Objective
To identify the benefits of the Directory Services Client for computers that are not compatible with Windows 2000.

Lead-in
Client computers running Windows 95 or Windows 98 that are not compatible with Windows 2000 can still take advantage of Active Directory.



**********ILLEGAL FOR NON-TRAINER USE**********

Client computers running Windows 95 or Windows 98 that cannot run Windows 2000 Professional due to hardware compatibility requirements can still take advantage of Active Directory by using the Windows 2000 Directory Services Client. The Directory Services Client upgrades computers running Windows 95 and Windows 98 so that they support Active Directory features, including the ability to:

- Use domain-based Distributed file system (Dfs). Dfs is a service that allows you to organize data into a logical hierarchy even through is it physically spread over multiple computers.

  Note For more information about Dfs, see module 7, "Providing Network Access to File Resources," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

- Search Active Directory.
- Change passwords on any domain controller.

Key Point
Before installing Directory Services Client on a computer, an administrator must install Microsoft Internet Explorer 4.0.1 or later and enable the Active Desktop component. Otherwise, the Directory Services Client Setup wizard does not run.

Important Before installing the Directory Services Client on a computer running Windows 95, you must install Microsoft Internet Explorer 4.0.1 or later and enable the Active Desktop™ component. Otherwise, the Directory Services Client Setup wizard does not run.

To install the Directory Services Client, perform the following steps:

1. Insert the Windows 2000 Server or Advanced Server compact disc into the CD-ROM drive.
2. In the \Clients\Win9x folder, on the Windows 2000 Server or Windows 2000 Advanced Server compact disc, run Dsclient.exe.
3. In the Directory Services Client Setup wizard, click **Next**.
4. On the **License Agreement** page, read the license agreement, and then click **I accept this agreement**.

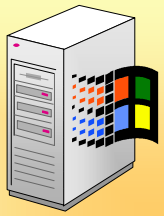
   The **Confirm Installation** page appears, prompting you to confirm that you want to install Directory Services Client.
5. Click **Finish** to complete the installation.
6. Click **OK**. When prompted, click **Yes** to restart the computer.

◆ Upgrading to Windows 2000 Advanced Server

Topic Objective
To identify the tasks for upgrading to Windows 2000 Advanced Server.

Lead-in
The configuration for an upgrade is easier than a new installation.

- Identifying Server Upgrade Paths
- Backing Up Critical Data Files and Settings



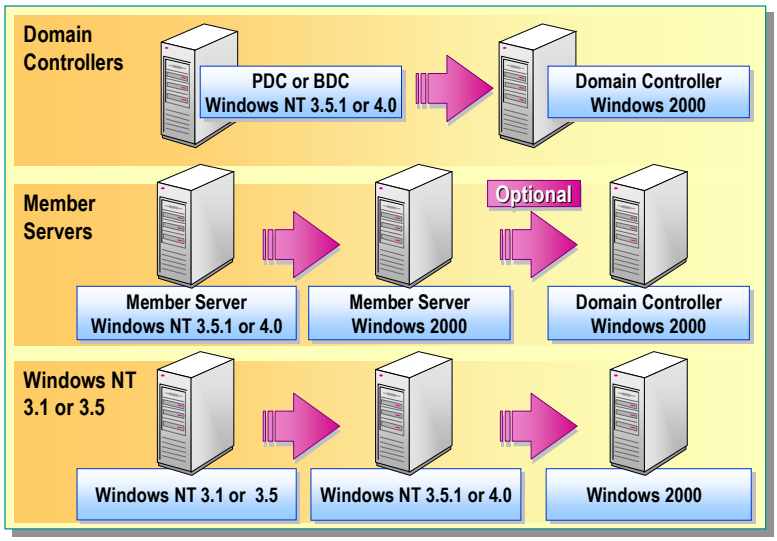
**********ILLEGAL FOR NON-TRAINER USE**********

There are several reasons to choose an upgrade from earlier versions of Windows to Windows 2000 Advanced Server instead of a new installation. First, the configuration is easier for an upgrade, and your existing users, settings, groups, rights, and permissions are retained. In addition, you do not need to reinstall files and applications. There are some tasks that you need to perform to help ensure a successful upgrade to Windows 2000. These tasks include identifying the upgrade path and backing up critical data files and settings.

Identifying Server Upgrade Paths

Topic Objective
To illustrate the server upgrade paths for Windows 2000.

Lead-in
You upgrade domain controllers and member servers running previous versions of Windows NT to either Windows 2000 Server or Windows 2000 Advanced Server.



**********ILLEGAL FOR NON-TRAINER USE**********

To upgrade domain controllers and member servers running previous versions of Windows NT to Windows 2000 Advanced Server, identify the upgrade paths for server operating systems in the following table.

Mention that a server running Windows NT Server 3.1 or Windows NT Server 3.5 cannot upgrade directly to Windows 2000 Advanced Server.

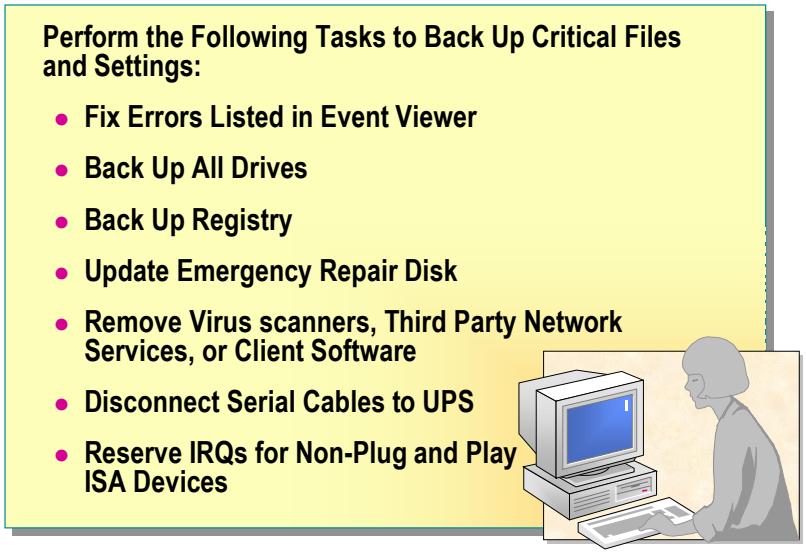
From	Upgrade to
A primary domain controller (PDC) or a backup domain controller (BDC) running Windows NT Server versions 3.5.1 or 4.0	A domain controller running Windows 2000 Server or Windows 2000 Advanced Server.
A member server running Windows NT Server 3.5.1 or 4.0	A member server running Windows 2000 Server or Windows 2000 Advanced Server.
A computer running Windows NT Server 3.1 or Windows NT Server 3.5	A computer running Windows NT Server 3.5.1 or 4.0 first, and then upgrade to Windows 2000 Server or Windows 2000 Advanced Server.

Note Many servers running Windows NT 3.1 or Windows NT 3.5 will not have the necessary hardware to run Windows 2000. To upgrade these servers and preserve the system configuration, you must first upgrade the system hardware to meet the Windows 2000 hardware requirements. You can then upgrade the operating system to Windows NT 3.5.1 or Windows NT 4.0, and then to Windows 2000 Advanced Server.

Backing Up Critical Data Files and Settings

Topic Objective
To identify the critical data files and settings to backup before upgrading.

Lead-in
Before you upgrade to Windows 2000 Advanced Server, it is important that you back up critical files to ensure that your data is saved if the upgrade process fails.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
It is important to back up data and settings in the unlikely case that the upgrade process fails.

Before you upgrade to Windows 2000 Advanced Server, it is important that you back up critical files to ensure that your data is saved if the upgrade process fails. Perform the following tasks to back up critical files and settings:

- Fix errors listed in Event Viewer. Check Event Viewer to ensure that there are no unresolved errors or issues. If errors are found, they should be corrected before upgrading to Windows 2000 Advanced Server.
- Back up all drives. Back up all drives in the system using a tape drive or some other type of system backup device. If you are using the Windows NT Backup utility, confirm that there were no errors after the backup process by checking the backup logs.
- Back up registry. Back up the registry of the computer using the Windows NT Backup utility or another backup program.

Note You can back up the registry without using tape by running Regback.exe in the Windows NT Server Resource Kit. You can restore the registry by running Regrest.exe, which is also found in the Windows NT Server Resource Kit.

- Update the Emergency Repair Disk. Update the Emergency Repair Disk (ERD) by running Rdisk.exe at the command prompt.
- Remove any virus scanners, third-party network services, or client software. Refer to the Release Notes file on the Windows 2000 Advanced Server compact disc for information about any known problems with specific hardware and applications.

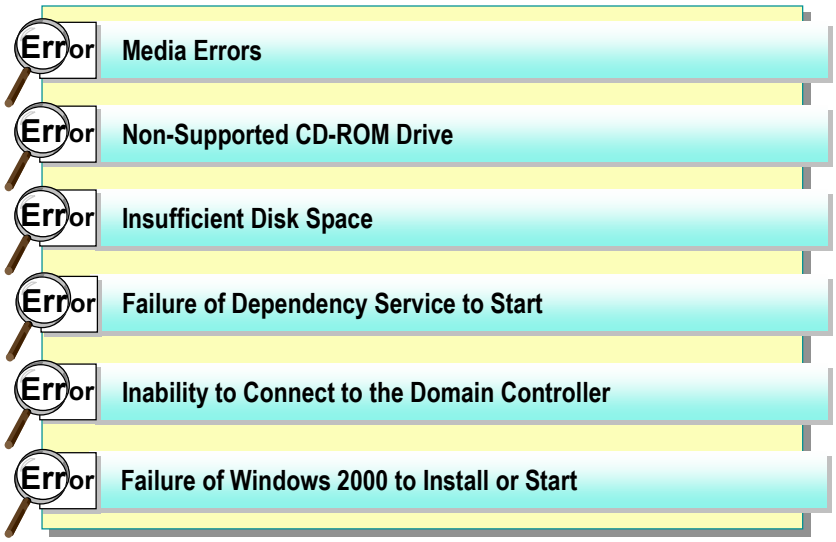
- Disconnect serial cables to UPS. Disconnect the serial cable that connects any uninterruptible power supply (UPS) devices. Windows 2000 Advanced Server will attempt to automatically detect devices connected to serial ports, which can cause problems with UPS equipment.
- Reserve IRQs for non-Plug and Play ISA devices. If your system contains non-Plug and Play Industry Standard Architecture (ISA) devices, set your system BIOS (basic input/output system) to reserve all IRQs (interrupt requests) currently in use by non-Plug and Play ISA devices. Failure to do so may result in the error message INACCESSIBLE_BOOT_DEVICE. In some cases, the non-Plug and Play ISA devices may not function.

After you complete the preparation tasks and back up your critical files and settings, you can begin the Windows 2000 installation procedure. The installation procedure for upgrading to Windows 2000 Advanced Server is similar to the procedure for a new installation. Refer to the installation procedure that was presented previously in the module to complete the upgrade process.

Identifying Setup Errors

Topic Objective
To identify common setup errors.

Lead-in
Sometimes problems occur during installation. Knowing the solutions to the most common problems will help you resolve setup failures.



**********ILLEGAL FOR NON-TRAINER USE**********

The following table lists common setup errors and possible solutions.

Problem	Solution
Media errors	Use a different compact disc. To request a replacement compact disc, contact Microsoft or your vendor.
Non-supported CD-ROM drive	Replace the CD-ROM drive with one that is supported. Try another method of installing Windows 2000, such as installing over the network, and then add the CD-ROM driver.
Insufficient disk space	Use the Setup program to create a partition that uses existing free space on the hard disk. You can also delete and create partitions as necessary to create a partition that is large enough for installation.
Failure of dependency service to start	In the Windows 2000 Setup wizard, return to the **Network Settings** page and verify that you installed the correct protocol and network adapter. Verify that the network adapter has the proper configuration settings, such as transceiver type, and that the local computer name is unique on the network.

(continued)

Problem	Solution
Inability to connect to the domain controller	Verify that the domain name is correct and the IP Address is correct. Verify that the server running the DNS Server service and the domain controller are both online. If you cannot locate a domain controller, join a workgroup and then join the domain after installation. Verify that the network adapter and protocol settings are set correctly. If you are reinstalling Windows 2000 and using the same computer name, delete and then recreate the computer account.
Failure of Windows 2000 to install or start	Verify that Windows 2000 is detecting all of the hardware and that all of the hardware is on the HCL.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Preparing for Installation
- Installing Windows 2000 Professional from a Compact Disc
- Installing Windows 2000 Advanced Server from a Compact Disc
- Upgrading to Windows 2000 Professional
- Upgrading to Windows 2000 Advanced Server
- Identifying Setup Errors

**********ILLEGAL FOR NON-TRAINER USE**********

1. Your small organization's network consists of only five computers, with one computer running Windows 2000 Advanced Server and the rest running Windows 2000 Professional. The data used in your company requires a high degree of security. What decisions should you make regarding file system and licensing mode?

   Because a high degree of security is needed, each computer should be using the NTFS file system. The licensing mode could be either Per Seat or Per Server.

2. Your company has decided to install Windows 2000 Professional on new computers that will be purchased for desktop users. What should you do before you purchase the new computers to ensure that Windows 2000 can be installed and run without difficulty?

   Verify that the hardware components meet the minimum requirements for Windows 2000 Professional. Also, verify that all of the hardware components that are installed in the new computers are on the Windows 2000 Professional HCL. If a component is not listed, contact the manufacturer to verify that a Windows 2000 Professional driver is available.

3. You are attempting to install Windows 2000 Advanced Server from a compact disc; however, you have discovered that your computer does not support starting from the CD-ROM drive. How can you install Windows 2000?

   Start the computer by using the Setup disks. When prompted, insert the Windows 2000 Advanced Server compact disc, and then continue Setup.

4. You have a server running Windows NT 3.5. Can this server be upgraded to Windows 2000? If so, what is the upgrade path?

   Yes. You must first upgrade to Windows NT Server 3.5.1 or 4.0, and then upgrade to Windows 2000.

5. You have a portable computer running Windows 95 and you want to upgrade it to Windows 2000. The computer has 16 MB of RAM that can be upgraded to 24 MB. How would you enable this computer to search Active Directory?

   You can install the Directory Services Client for Windows 95 or Windows 98. The portable computer would then be able to search Active Directory.

6. You are about to upgrade a computer running Windows NT Workstation 4.0 to Windows 2000 Professional. List two things that you should check before starting the upgrade process.

   Check that you have at least 32 MB of RAM and enough available hard disk space to complete the upgrade. You should also generate a compatibility report to check that all hardware and software currently installed is compatible with Windows 2000.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 2: Configuring the Windows 2000 Environment

Contents

Overview	1
Configuring and Managing Hardware	2
Lab A: Creating and Using Hardware Profiles	11
Configuring Display Options	17
Configuring System Settings	24
Configuring the Desktop Environment	29
Lab B: Modifying Startup and Recovery Options	36
Configuring Internet Options for Client Computers	39
Lab C: Configuring Internet Options	42
Review	45

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart

Simulation and interactive exercises were built with Macromedia Authorware.

Instructor Notes

Presentation:
65 Minutes

Labs:
40 Minutes

This module provides the knowledge and skills necessary to configure the Microsoft® Windows® 2000 environment, which includes configuring hardware, software, system, regional, accessibility, and Internet settings.

At the end of this module, students will be able to:

- Configure and manage hardware.
- Configure display options.
- Configure system settings.
- Configure the desktop environment.
- Configure Internet options.

Materials and Preparation

This section provides you with the required materials and preparation tasks needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_02.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all the materials for this module.
- Complete the labs.

Module Strategy

Use the following strategy to present this module:

- Configuring and Managing Hardware

  In this topic, provide information about configuring and managing hardware. Explain how to install hardware devices and briefly explain device configuration. Demonstrate the steps for updating device drivers. Explain how driver signing is managed in Windows 2000 and describe the three options an administrator has for managing unsigned drivers. Discuss hardware profiles before beginning the first lab.

- Configuring Display Options

  In this topic, provide information about configuring display options. Briefly explain some of the more critical display settings and show students how to gain access to these settings in Control Panel. Introduce the multimedia presentation on multiple monitors. After the presentation, briefly review how to configure multiple monitors.

- Configuring System Settings

  In this topic, describe how to configure system settings. Explain how to set environment variables, and change startup and recovery settings in Control Panel.

- Configuring the Desktop Environment

  In this topic, provide information about configuring regional and accessibility options and managing software using Control Panel. Briefly describe how regional options change the display of numerical data, and then explain input locales. Describe accessibility options available for users with special needs. Demonstrate the Accessibility wizard. Describe the process of managing applications by using **Add/Remove Programs**. Explain the three levels of applications listed by the online Directory of Windows 2000 Applications.

- Configuring Internet Options for Client Computers

  In this topic, provide information about configuring basic Internet options for client computers. Demonstrate and discuss configuring home pages, disk space for temporary files, proxy server settings, and access restrictions to undesirable Web content.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

To prepare student computers for the labs in this module, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- Disables the **Display list of operating systems for *x* seconds** option in the **Startup and Recovery** area on the **Advanced** tab of the **System** dialog box.
- Configures Microsoft Internet Explorer for use in the classroom environment.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about the different ways to configure the Windows 2000 environment.

- **Configuring and Managing Hardware**
- **Configuring Display Options**
- **Configuring System Settings**
- **Configuring the Desktop Environment**
- **Configuring Internet Options for Client Computers**

**********ILLEGAL FOR NON-TRAINER USE**********

Microsoft® Windows® 2000 provides options that you can use to customize the Windows 2000 environment and ensure that all hardware operates correctly. Understanding the available options and how to configure these options will help you configure a Windows 2000 environment that meets the requirements of your organization.

At the end of this module, you will be able to:

- Configure and manage hardware.
- Configure display options.
- Configure system settings.
- Configure the desktop environment.
- Configure Internet options.

◆ Configuring and Managing Hardware

Topic Objective
To introduce the topics associated with configuring hardware settings.

Lead-in
Windows 2000 includes tools to help you verify and configure hardware settings and configure display settings.

- **Installing Hardware**
- **Updating Drivers**
- **Managing Driver Signing**
- **Using Hardware Profiles**

**********ILLEGAL FOR NON-TRAINER USE**********

In most cases, it is easy to install hardware with Windows 2000. You simply plug in the new hardware device. Windows 2000 then automatically detects the device, installs any necessary drivers, and updates the system, allocating resources. If Windows 2000 does not automatically detect new hardware during installation, you can use **Add/Remove Hardware** in Control Panel to install and configure the new hardware.

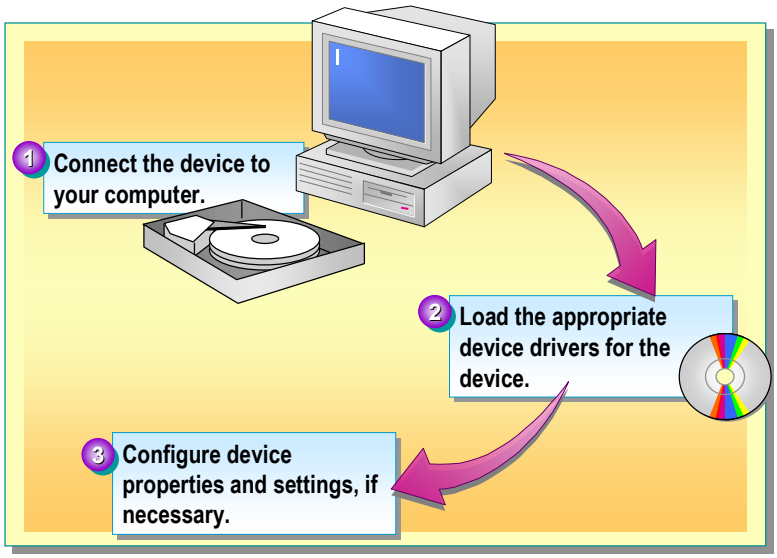
After you install new hardware on your system, you must install and configure the appropriate driver before Windows 2000 can use the device. If the device in question is listed on the Hardware Compatibility List (HCL), Windows 2000 usually includes the correct driver. All device drivers that ship with Windows 2000 have a Microsoft digital signature, which indicates that the driver was tested and works properly with the operating system. Untested device drivers or hardware that is not configured properly can cause computers to crash or force users to restart computers frequently.

Windows 2000 allows you to customize hardware and software settings for particular environments. You use hardware profiles to specify the settings that are used for each device, or the devices that should start when you start your computer. Hardware profiles are useful if you have multiple users on a single computer who may need to use different hardware settings.

Installing Hardware

Topic Objective
To illustrate the process for installing hardware.

Lead-in
Installing a new device typically involves three steps.



**********ILLEGAL FOR NON-TRAINER USE**********

Hardware includes any physical device that is connected to a computer and controlled by the computer's microprocessor. This includes equipment that was connected to the computer when it was manufactured, as well as peripheral equipment that you add later. Modems, disk drives, CD-ROM drives, print devices, network adapters, keyboards, and display adapter cards are all examples of devices.

Installing a new device typically involves three steps:

1. Connect the device to your computer.
2. Load the appropriate device drivers for the device.
3. Configure device properties and settings, if necessary.

Installing a Device

You must be logged on as an administrator or a member of the Administrators group to install a device. To install a device, perform the following steps:

1. Connect the device to the appropriate port, or insert the device into a slot on your computer, according to the device manufacturer's instructions. Follow the instructions listed in the table, depending upon the type of device you are installing.

If the device	Then do this
Needs to be installed into a slot inside your computer, such as a sound card	Shut down Windows and turn off the computer. Remove the computer cover and install the device in the appropriate slot. Replace the computer cover, and then turn on the computer. Note that some computers may have hot-swappable PCI slots.
Is a small computer system interface (SCSI) device	Connect it to the SCSI port on your computer according to the device manufacturer's instructions. Restart or turn on your computer. You need to be sure that the device number for the SCSI device is not used by another SCSI device. To change the device number, see the device manufacturer's instructions.
Is a Universal Serial Bus (USB) or Institute of Electrical and Electronics Engineers, Inc. (IEEE) 1394 device	Plug the device into any USB or IEEE port on your computer. Follow the instructions that appear on your screen. You do not need to shut down or turn off your computer when you install or plug in a USB or IEEE 1394 device.

2. Do one of the following:
   - If prompted, follow the instructions on the screen to choose a destination path to load the appropriate device drivers, and then restart your computer, if necessary.

     -Or-

   - If the device is non-Plug and Play, use **Add/Remove Hardware** in Control Panel to identify type of device that you are installing, and then insert the Windows 2000 compact disc or the manufacturer's disk or compact disc so that Windows 2000 can load the proper device drivers. After you load the device drivers onto your system, Windows 2000 configures the properties and settings for the device.

Key Points
Although you can manually configure device properties and settings, you should let Windows 2000 configure properties and settings automatically.

Examining Device Configuration

When you install a Plug and Play device, Windows 2000 automatically configures the device so that it will work properly with the other devices that are installed on your computer. As part of that configuration process, Windows 2000 assigns a unique set of system resources to the device that you are installing. These resources can include one or more of the following:

- Interrupt request (IRQ) line numbers
- Direct memory access (DMA) channels
- Input/output (I/O) port addresses
- Memory address ranges

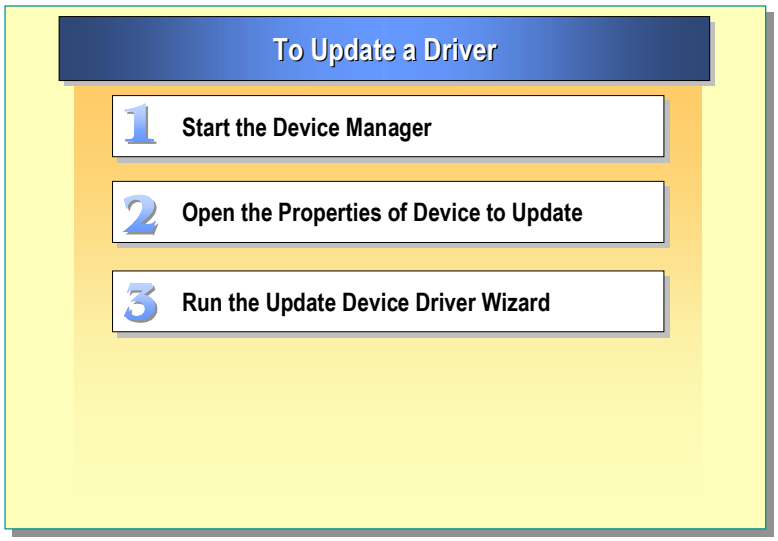
Each resource that is assigned to your device must be unique or the device will not function properly. For Plug and Play devices, Windows 2000 automatically ensures that these resources are configured properly. When you install a non-Plug and Play device, Windows does not automatically configure the resource settings for the device. Depending on the type of device that you are installing, you may have to manually configure these settings in the Device Manager. The settings should be supplied in the documentation that comes with your device.

Generally, you should not manually change resource settings. Doing so causes the settings to become fixed and Windows 2000 will then have less flexibility when allocating resources to other devices. If too many resources become fixed, Windows 2000 may be unable to install additional Plug and Play devices.

Updating Drivers

Topic Objective
To identify the steps for updating drivers.

Lead-in
You need administrative rights to install or update a driver.



**********ILLEGAL FOR NON-TRAINER USE**********

To protect the system from being tampered with, users cannot change drivers without having the appropriate rights. By default, the Administrator account has the rights to perform the following tasks:

- Load and unload drivers
- Copy files to the System32\Drivers folder
- Write settings to the registry

Delivery Tip
Demonstrate the steps for updating device drivers.

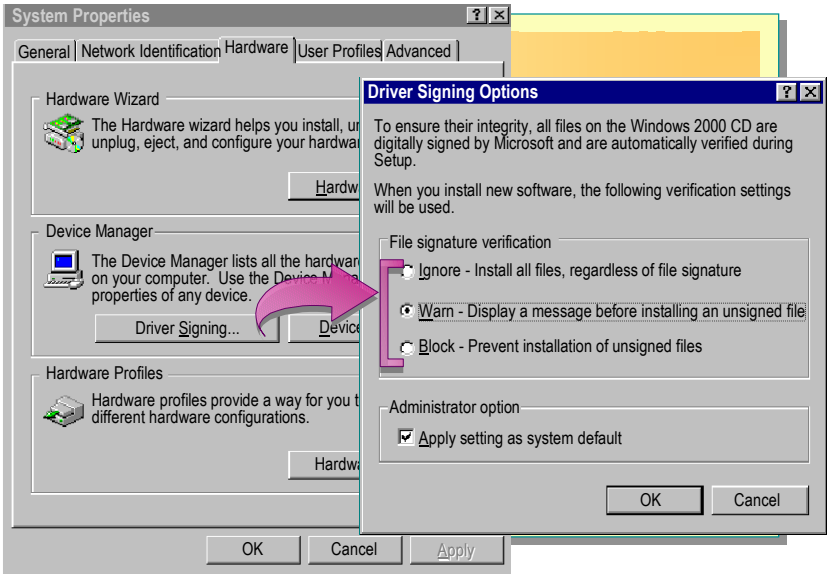
When hardware manufacturers release new device drivers, you should update your driver to use the most current version. To update a device driver, perform the following steps:

1. In Control Panel, double-click **System**, click the **Hardware** tab, and then click **Device Manager**.
2. In Device Manager, right-click the device that you want to update, and then click **Properties**.
3. On the **Driver** tab, click **Update Driver** to open the Update Device Driver wizard, and then follow the wizard instructions.

Managing Driver Signing

Topic Objective
To identify the properties you use to configure digital signing options.

Lead-in
The system files provided with Windows 2000 have a Microsoft digital signature, which ensures that a particular file has met a certain level of testing, and that the file has not been altered or overwritten by another program's installation process.



**********ILLEGAL FOR NON-TRAINER USE**********

Sometimes, when installing new software on your computer, the software installation process overwrites system files with incompatible versions. This can cause system instability.

The system files provided with Windows 2000 have a Microsoft digital signature. These signatures ensure that a particular file has met a certain level of testing, and that the file has not been altered with, or overwritten by, another program's installation process. Digital signatures are required for all vendor-provided drivers that ship with Windows 2000, and for drivers published on the Windows Update Web site.

How Driver Signing Works

Driver signing uses cryptographic technology to store identifying information in a catalog (.cat) file. This information identifies the driver as having passed testing by Windows Hardware Quality Labs (WHQL). No change is made to the binary file of the driver. Instead, a .cat file is created for each driver package and the .cat file is signed with a Microsoft digital signature. The relationship between the driver package and its .cat file is referenced in the driver's .inf file and is maintained by the system after the driver is installed.

Controlling Unsigned Drivers

Use the following procedure to control how Windows 2000 reacts if an installation program attempts to add unsigned drivers to the system. To configure driver signing options, perform the following steps:

1. Right-click **My Computer**, and then click **Properties**.
2. On the **Hardware** tab, click **Driver Signing**, select one of the following options, and then click **OK**:
   - **Ignore**. Installs all device drivers regardless of whether they have a digital signature.
   - **Warn**. Displays a warning when it detects device drivers that are not digitally signed. (This is the default setting.)
   - **Block**. Prevents users from installing device drivers without digital signatures.

Identifying Unsigned Files

Use file signature verification to identify unsigned files on your computer and specify verification options. To use file signature verification, perform the following steps:

1. Click **Start**, click **Run**, type **sigverif** in the **Open** box, and then click **OK**.
2. Click **Start** to identify any files that are not signed.

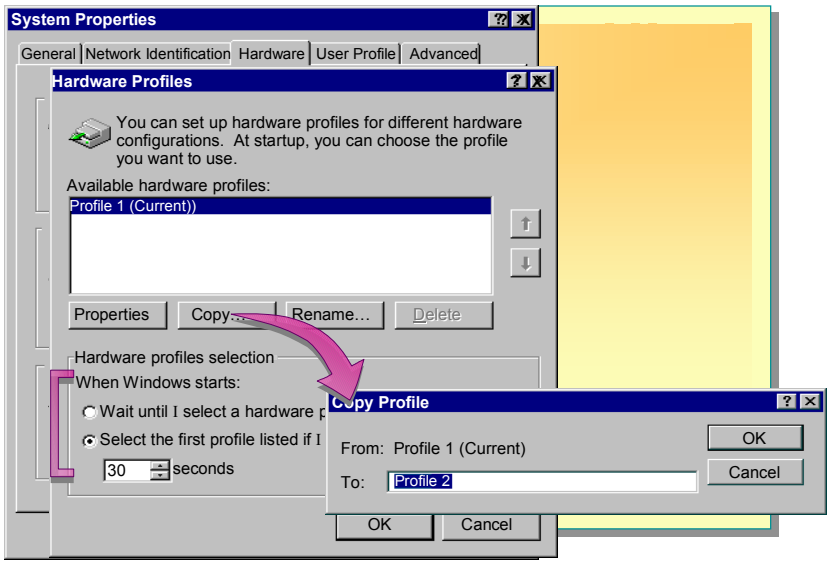
   A list of files that have not been digitally signed appears.
3. If required, click **Advanced** to specify the verification options.

   The **Advanced File Signature Verification Settings** dialog box appears.
4. On the **Search** tab, select one of the following options:
   - **Notify me if any system files are not signed**
   - **Look for other files that are not digitally signed**
5. To view a log file, click **View Log** on the **Logging** tab.

Using Hardware Profiles

Topic Objective
To illustrate the interface for creating a new hardware profile.

Lead-in
To create a new hardware profile, begin by copying the existing profile and then restart your computer using the new profile. Modify the new profile as desired.



**********ILLEGAL FOR NON-TRAINER USE**********

A hardware profile specifies the configuration and characteristics of specific hardware devices and services that load at startup. It also specifies the settings Windows 2000 uses for each device. Hardware profiles enable you to optimize computers for different environments.

Creating a New Hardware Profile

Windows 2000 creates a default profile hardware profile during installation. To create a new profile, you must copy an existing profile, and then modify the configuration settings for the new profile.

To create a new hardware profile, perform the following steps.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. In **Control Panel**, double-click **System**, click the **Hardware** tab, and then click **Hardware Profiles**.
3. In the **Available hardware profiles** list, select the profile that you want to copy, and then click **Copy**.
4. Type a name for the new profile in the **Copy Profile** dialog box, and then click **OK**.
5. Restart the computer and on the **Hardware Profile/Configuration Recovery** menu, select the new profile.
6. Right-click **My Computer**, and then click **Manage**.
7. Expand **Device Manager** to enable or disable devices for the current profile.
8. Expand **Services** under **Services and Applications** to enable or disable services for the current profile, and then click **OK**.

Key Points
Emphasize that the default profile is always first in the list. To change the order, use the arrows to the right to arrange the profiles in the desired order.

Activating a Hardware Profile

If there is more than one profile defined for a computer, at startup Windows 2000 displays the **Hardware Profile/Configuration Recovery** menu.

The default profile is the first profile that appears in the list. To change the order in which the profiles appear on the **Hardware Profile/Configuration Recovery** menu at startup, perform the following steps:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **System**, and then click the **Hardware** tab.
3. In the **Hardware Profiles** dialog box, click the profile that you want to move, and then click the up and down arrows to change the order in which that profile appears.

Configuring Hardware Profile Settings

You can configure the time that the computer waits before automatically starting the default configuration. To adjust this time delay, under **Hardware Profiles**, click **Select the first profile listed if I don't select a profile in**, and then specify the time (in seconds).

Windows 2000 automatically detects whether it should display a particular a hardware profile on the **Hardware Profile/Configuration Recovery** menu. To ensure that a hardware profile displays on the **Hardware Profile/Configuration Recovery** menu, select the hardware profile in the **Hardware Profiles** dialog box, click **Properties**, and then, in the **Hardware Profiles Properties** dialog box, select the **Hardware profiles option** check box.

Lab A: Creating and Using Hardware Profiles

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create a new hardware profile, and modify, test, verify, and remove the profile.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create hardware profiles.
- Modify hardware profiles.
- Delete hardware profiles.

Prerequisites

Before working on this lab, you must have:

- Knowledge of hardware profiles.
- Knowledge of startup and recovery settings.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server.
- A user account named Customer.

Estimated time to complete this lab: 15 minutes

Exercise 1
Creating and Testing Hardware Profiles

Scenario

The Customer Support manager wants you to set up a computer on which customers can view information about upcoming promotions. This computer should be able to act as a stand-alone computer when disconnected from the company network and must also be able to connect to the network if necessary. You suggest setting up hardware profiles on the computer to allow the computer to operate in different roles, both as a stand-alone promotional kiosk and as a network client.

Goal

In this exercise, you will create a hardware profile named Kiosk. You will then disable the CD-ROM drive and network adapter for the Kiosk profile and then test the profile. After successfully testing the Kiosk profile, you will delete the profile.

Tasks	Detailed Steps
1. Log on as administrator with the password of **password** and create a hardware profile called Kiosk. Then, restart the computer and select the Kiosk profile on startup.	**a.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name)
Note: You may need to expand **Options** to verify you are logging into *Server* (where *Server* is your computer name).	
1. *(continued)*	**b.** Click **Start**, point to **Settings**, and then click **Control Panel**. **c.** In Control Panel, double-click **System**. **d.** In the **System Properties** dialog box, on the **Hardware** tab, click **Hardware Profiles**. **e.** In the **Hardware Profiles** dialog box, click **Copy**. **f.** In the **Copy Profile** dialog box, in the **To** text box, type **Kiosk** and then click **OK**. **g.** In the **Hardware Profiles** dialog box, under **Available hardware profiles**, verify that **Kiosk** is selected, and then click the up arrow. **h.** Click **OK** to close the **Hardware Profiles** dialog box. **i.** Click **OK** to close the **System Properties** dialog box. **j.** Close Control Panel. **k.** Click **Start**, click **Shut Down**, click **Restart**, and then click **OK**. *When the computer restarts, the **Hardware Profile/Configuration Recovery** menu appears because the computer has two hardware profiles.* **l.** Press ENTER to select Kiosk.

Tasks	Detailed Steps
Can you modify a hardware profile if it is not the current hardware profile? **No. To modify a hardware profile it must be the current hardware profile.**	
2. Log on as Administrator with the password of **password** and, in Computer Management, set the network adapter and CD-ROM drive as disabled for the Kiosk hardware profile.	**a.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** In Control Panel, double-click **System**. **c.** In the **System Properties** dialog box, on the **Hardware** tab, click **Hardware Profiles**. **d.** Verify that the first profile appears as **Kiosk (Current)**. **e.** In the **Hardware Profiles** dialog box, under **Hardware profiles selection**, in the **Select the first profile listed if I don't select a profile in** box, set the seconds to zero, and then click **OK**. **f.** On the **Hardware** tab, click **Device Manager**.
With the time the hardware profile selection screen displays set to zero, how can the administrator select which hardware profile becomes the default hardware profile? **The Administrator must log on and change the hardware profile listing in hardware profiles and then restart the computer in this new hardware profile. Otherwise, the administrator can log on and change the time the hardware profile screen displays and then restart the computer and select a different hardware profile at start up.**	

Tasks	Detailed Steps
2. *(continued)*	**g.** In Device Manager, expand **Network adapters**, and then double-click *adapter* (where *adapter* is the name of your network adapter. For example, Netelligent 10/100TX PCI Embedded UTP Coax Controller). **h.** In the *adapter* **Properties** dialog box, on the **General** tab, under **Device usage**, click **Do not use this device in the current hardware profile (disable)**, and then click **OK**. *The adapter appears with a red x to indicate that it has been disabled for the current hardware profile, which is Kiosk.* **i.** In Device Manager, expand **DVD/CD-ROM drives**, and then double-click *DVD/CD-ROM* (where *DVD/CD-ROM* is the name of your CD-ROM drive, for example, SONY CD-ROM CDU311-Q). **j.** In the *CD-ROM* **Properties** dialog box, on the **General** tab, under **Device usage**, select **Do not use this device in the current hardware profile (disable)**, and then click **OK**. **k.** Close Device Manager, click **OK** to close the **System Properties** dialog box, and then close Control Panel. **l.** Click **Start**, click **Shut Down**, click **Restart**, and then click **OK**.
When the system restarts does the list of hardware profiles available display? Why or why not? **No. Because the time for the hardware profiles screen to display was set to zero.**	
3. Log on as Customer and verify that the order of the hardware profiles cannot be changed. Then, verify that the network adapter and CD-ROM drive have been disabled.	**a.** Log on using the following information: User name: **Customer** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** In Control Panel, double-click **System**. **c.** In the **System Properties** dialog box, on the **Hardware** tab, click **Hardware Profiles**. **d.** In the **Hardware Profiles** dialog box, verify that the Kiosk hardware profile is current. *Notice that when you are logged on as Customer, you do not have rights to modify the hardware profiles.*
Which user account on the local computer has the rights to configure hardware profiles? **Only members of the local Administrators group (Administrator, by default).**	

Tasks	Detailed Steps
3. (*continued*)	**e.** Click **OK** to close the **Hardware Profiles** dialog box, and then click **OK** to close the **System Properties** dialog box. **f.** Close Control Panel. **g.** Double-click **My Computer**, verify that the CD-ROM drive no longer appears, and then close My Computer. **h.** Click **Start**, and then click **Run**. **i.** In the **Open** box, type **\\london** and then click **OK**. *An error message appears stating that the network path could not be found. This is because the network adapter has been disabled for this hardware profile.* **j.** Click **OK** to close the **\\london** message box, and then click **Cancel** to close the **Run** dialog box. **k.** Click **Start**, click **Shut Down**, click **Log off Customer**, and then click **OK**.
4. Log on as Administrator and change the default hardware profile to the original hardware profile and restart the computer. Log on again as Administrator with the password of **password**, and then delete the Kiosk hardware profile and verify that the network adapter and the CD-ROM drive are enabled.	**a.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** In Control Panel, double-click **System**. **c.** In the **System Properties** dialog box, on the **Hardware** tab, click **Hardware Profiles**. **d.** In the **Hardware Profiles** dialog box, verify that **Kiosk (Current)** is selected, and then click the down arrow. **e.** Click **OK** to close the **Hardware Profiles** dialog box, and then click **OK** to close the **System Properties** dialog box. **f.** Minimize Control Panel. **g.** Restart your computer. **h.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **i.** Restore Control Panel, and then double-click **System**. **j.** In the **System Properties** dialog box, on the **Hardware** tab, click **Hardware Profiles**.

Tasks	Detailed Steps
4. (*continued*)	**k.** In the **Hardware Profiles** dialog box, click **Kiosk**, and then click **Delete**. **l.** In the **Confirm Profile Delete** dialog box, click **Yes**. **m.** Click **OK** to close the **Hardware Profiles** dialog box, and then click **OK** to close the **System Properties** dialog box. **n.** Close Control Panel. **o.** Double-click **My Computer**. **p.** Verify that the CD-ROM drive appears, and then close My Computer. **q.** Click **Start**, and then click **Run**. **r.** In the **Open** box, type **\\london** and then click **OK**. *Notice that you can access the London computer because the network adapter is enabled.* **s.** Close the London window, and then log off.

Configuring Display Options

Topic Objective
To identify the topics related to display options.

Lead-in
You use **Display** in Control Panel to customize your desktop and display settings.

- Configuring the Display
- Multimedia: Introduction to Multiple Monitors
- Configuring Multiple Monitors

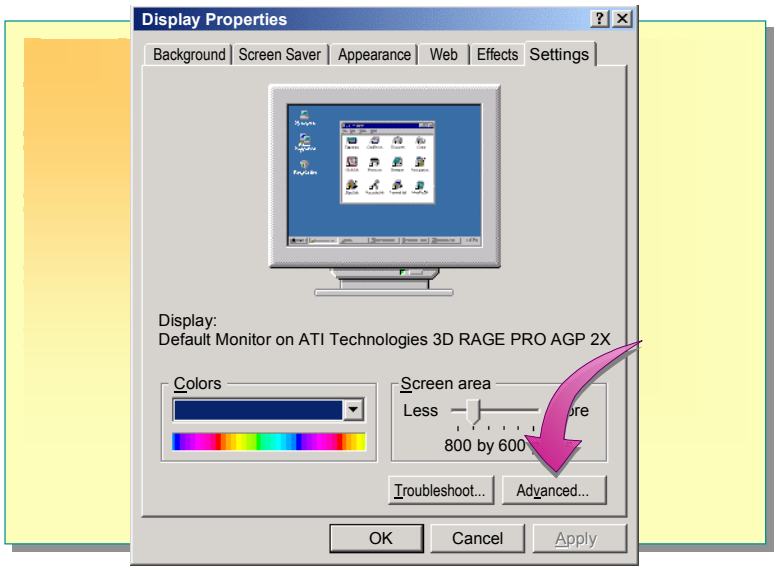
**********ILLEGAL FOR NON-TRAINER USE**********

You use **Display** in Control Panel to configure the computer display, or configure the computer to support multiple displays. It is important that you understand these Control Panel options so that you can effectively take advantage of the display capabilities in Windows 2000.

Configuring the Display

Topic Objective
To illustrate the **Display Properties** dialog box in Control Panel.

Lead-in
You can set the color depth, screen resolution, font size, and refresh frequency in the **Display Properties** dialog box.



**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 allows you to customize your desktop and display settings. These settings control how your desktop looks and how your monitor displays information. For example, you can customize the colors and fonts that are used by Windows 2000, customize the wallpaper image on your desktop, or configure a screen saver with a password in order to protect your work.

Configure display options by using **Display** in Control Panel. Use the **Settings** tab, in the **Display Properties** dialog box, to configure the color depth and the video resolution. Click **Advanced** on the **Settings** tab to configure advanced display options. The following table describes the advanced display options that you can configure.

Delivery Tip
Demonstrate to the students how to access these tabs.

Tab	Option	Description
General	**Display**	Provides small, large, or custom font sizes for the display.
	Compatibility	Determines the action that Windows 2000 should take after you make changes to display settings.
Adapter	**Adapter Type**	Lists the manufacturer, model number, and properties of the installed adapter.
	Properties	Provides configuration details for the display adapter and allows you to modify the configuration.
	List All Modes	Lists all of the combinations of screen resolution, colors, and refresh rates that are available for the display adapter.

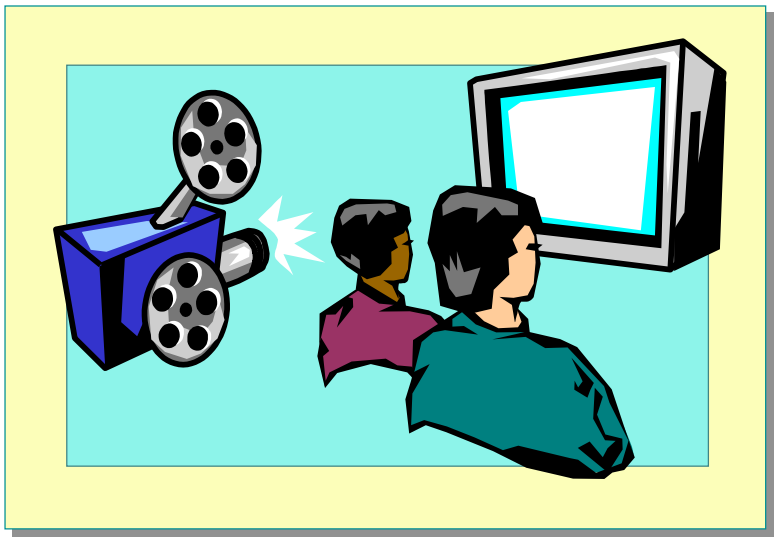
(continued)

Tab	Option	Description
Monitor	**Monitor Type**	Lists the manufacturer, model number, and properties of the monitor that is currently installed. Under the **Properties** tab, you can view and modify the driver configuration and hardware settings.
	Monitor Settings	Configures the screen refresh frequency. This option only applies to high-resolution drivers. Do not select a refresh rate/screen resolution combination that the monitor does not support. If you are unsure, refer to your monitor documentation or select the lowest refresh rate option.
Trouble-shooting	**Hardware Acceleration**	Controls the acceleration level and performance that your graphics hardware supplies. If your hardware supports it, you may choose to alter the acceleration to improve the response time for graphics to redraw on the screen.
Color Management (Optional)		Selects the default color profile for your monitor. Use this if you need to match your screen colors to match publication or graphics needs.

Multimedia: Introduction to Multiple Monitors

Topic Objective
To introduce the multimedia presentation.

Lead-in
With a multiple display configuration, you can configure up to ten monitors to extend the Windows 2000 desktop. This multimedia presentation provides you with an overview of Windows 2000 support for multiple monitors.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Run the multimedia presentation located under Multimedia Presentations on the Web page on the Trainer Materials compact disc, and then discuss the review questions with the students.

The estimated time to complete this multimedia presentation is approximately 5 minutes.

This multimedia presentation provides you with an overview of Windows 2000 support for a multiple monitors. With a multiple display configuration, you can configure up to ten monitors to extend the Windows 2000 desktop.

Note This presentation is available under Multimedia Presentations on the Web page on the Student Materials compact disc.

As you view the presentation, try to answer the following questions:

1. A user calls and says that she has two ISA video adapters and wants to know if she can use these for multiple monitor?

   Windows 2000 multiple monitor only supports PCI and AGP video adapters.

2. A user asks for help to configure multiple monitors. The user has two monitors aligned side by side on her desktop. The primary monitor is on the right and the secondary monitor is on the left. When she tries to drag an icon from the right monitor to the left monitor she is unable to move it. Without rearranging the monitors on her desktop, how can she solve this problem?

   To arrange multiple monitors, double-click Display in Control Panel. On the Settings tab, click Identify to display an identification number that corresponds to each of the monitor icons. Drag the monitor icons to arrange them, and then click OK.

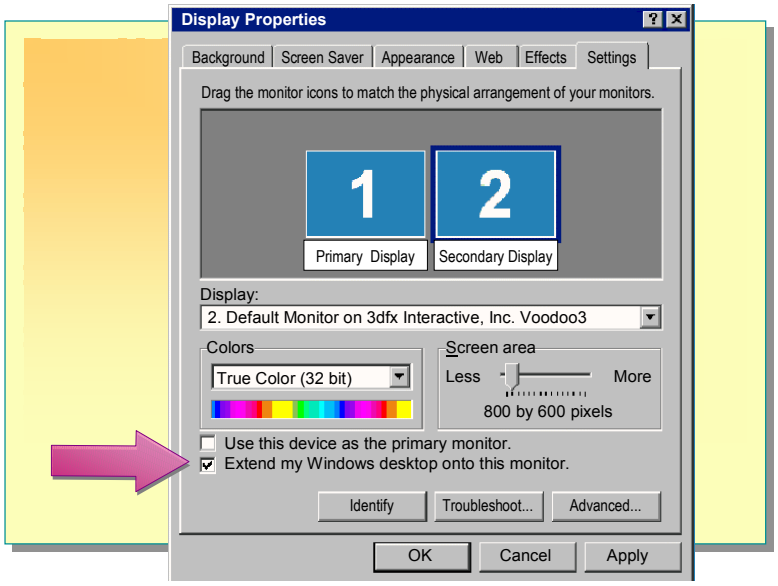
3. A user calls with a question about his computer configured to use multiple monitors. He has two monitors running on his Windows 2000 Professional computer. When he executes an application from the **Start** menu it displays on the secondary monitor. What is happening, and how can he configure his monitors such that the programs display on the primary monitor where the **Start** menu appears?

   To change the primary monitor, open Display in Control Panel. On the Settings tab, click the monitor icon that represents the monitor you want to designate as primary. Select the Use this device as the primary monitor check box. Note that this check box is unavailable when you select the monitor icon that is currently set as your primary monitor.

Configuring Multiple Monitors

Topic Objective
To illustrate the interface for configuring multiple monitors.

Lead-in
Selecting the **Extend my Windows desktop onto this monitor** check box allows you to drag items across your screen onto alternate monitors.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
To be compatible with multiple monitor support, the display adapter must be PCI or AGP.

When using multiple monitors, you will have a primary display or monitor followed by a secondary display, and then the rest in sequential order. To use the multiple monitor feature, you need to use either a Peripheral Component Interconnect (PCI) or Accelerated Graphics Port (AGP) cards or adapters.

Installing Additional Monitors

To install additional monitors, perform the following steps.

1. Turn off your computer.
2. Insert your additional PCI or AGP video adapter into an available slot.
3. Plug your additional monitor into the card.
4. Turn on your computer. Windows 2000 will detect the new video adapter and install the appropriate drivers.
5. Double-click **Display** in Control Panel.
6. On the **Settings** tab, click the monitor icon that represents the monitor you want to use in addition to your primary monitor.
7. Select the **Extend my Windows desktop onto this monitor** check box, and then click **Apply**.
8. Select the color depth and resolution for the secondary display.
9. Repeat steps 6 through 8 for each additional display, and then click **OK** to close the **Display Properties** dialog box.

Changing the Primary Monitor

When you start the computer, the primary monitor serves as the central focus for all activity. By default, any logon screen appears on the primary monitor. When you open a program, the opening windows also appear on the primary monitor until you move them.

To change the primary monitor, perform the following steps:

Double-click **Display** in Control Panel. On the **Settings** tab, click the monitor icon that represents the monitor you want to designate as primary. Select the **Use this device as the primary monitor** check box and then click **OK**. Note that this check box is unavailable when you select the monitor icon that is currently set as your primary monitor.

Arranging Multiple Monitors

You can arrange the position of multiple monitors in the **Display Properties** dialog box to represent their physical arrangement. This simplifies your ability to move items around from one monitor to another.

To arrange multiple monitors, perform the following steps:

Double-click **Display** in Control Panel. On the **Settings** tab, click **Identify** to display an identification number that corresponds to each of the monitor icons. Drag the monitor icons to arrange them, and then click **OK**.

The icon positions determine how you move items from one monitor to another. For example, if you are using two monitors and you want to move items from one monitor to the other by dragging left and right, place the icons side by side. To move items between monitors by dragging up and down, place the icons one above the other.

◆ Configuring System Settings

Topic Objective
To identify the topics associated with configuring system settings.

Lead-in
You can use Control Panel to configure system settings such as performance options, the paging file, environment variables, and startup and recovery settings.

- **Modifying Environment Variables**
- **Modifying Startup and Recovery Options**

**********ILLEGAL FOR NON-TRAINER USE**********

System performance can vary over time due to changes in workload and resource usage. Windows 2000 contains several configuration options that allow you to optimize system performance.

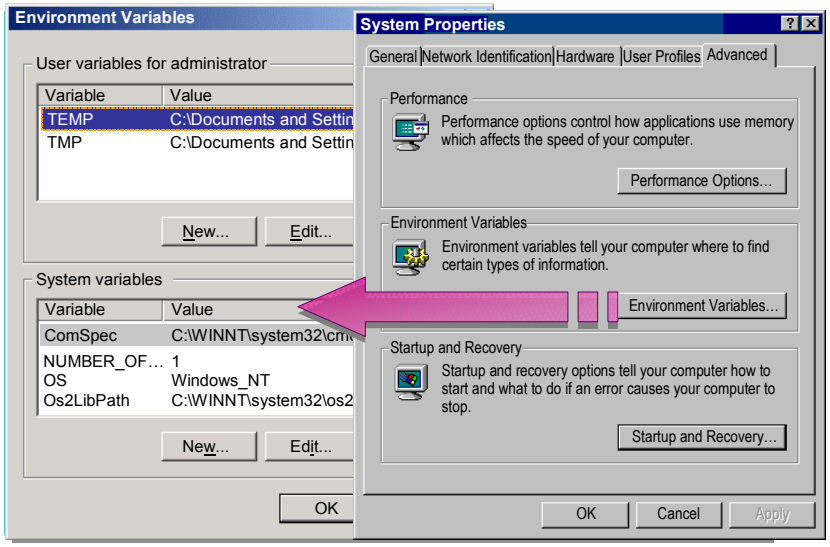
When you configure operating system settings, they apply to all users who log on to the computer; you do not need to reconfigure the settings for each user. In Control Panel, you can configure the following operating system settings:

- *Environment Variables*. The settings found under the **Advanced** tab under **System** in Control Panel, allow you to alter user and system variables. For example, you can change the location of the system's temporary files to optimize space.
- *Startup and Recovery*. The settings found under the **Advanced** tab under **System** in Control Panel, allow you to configure startup and recovery procedures. For example, you can set the counter to zero to minimize the restart time.

Modifying Environment Variables

Topic Objective
To illustrate the interface for setting environment variables.

Lead-in
Environment variables define the system and user environment information.



**********ILLEGAL FOR NON-TRAINER USE**********

The **Environment Variables** dialog box lists specific configuration information, such as the location of temporary files that are used by the operating system or specific applications. The environment variables available under the **Advanced** tab of the **System Properties** dialog box has two areas, one for user variables pertaining to the user logged on at the time, and one for system variables pertaining to the particular computer. Each area has buttons for creating new variables, or editing and deleting existing ones. Windows 2000 uses this information to control various applications. For example, the TEMP environment variable specifies where an application places its temporary files.

Delivery Tip
Open the **Environment Variables** dialog box, and describe the configuration options that are available.

Students will not configure environment variables in a lab.

To display or edit the user and system environment variables that are currently in effect in the **Environment Variables** dialog box, open the **System Properties** dialog box, click the **Advanced** tab, and then click **Environment Variables**.

Configuring User Environment Variables

The user environment variables differ for each user of a particular computer and are stored as part of the user's profile. The user environment variables include any user-defined settings (such as the Temp folder) and any variables that the applications define (such as the path to the location of the application files). Users can add, modify, or remove their user environment variables in the **Environment Variables** dialog box.

Configuring System Environment Variables

System environment variables apply to the entire system. Consequently, these variables affect all system users. During installation, Setup configures the default system environment variables, including the path to the Windows 2000 files. Only an administrator can add, modify, or remove a system environment variable.

Setting Default Environment Variables

During startup, Windows 2000 searches the startup files and sets any environment variables. Windows 2000 sets environment variables in the following order:

1. Autoexec.bat variables
2. System environment variables
3. User environment variables

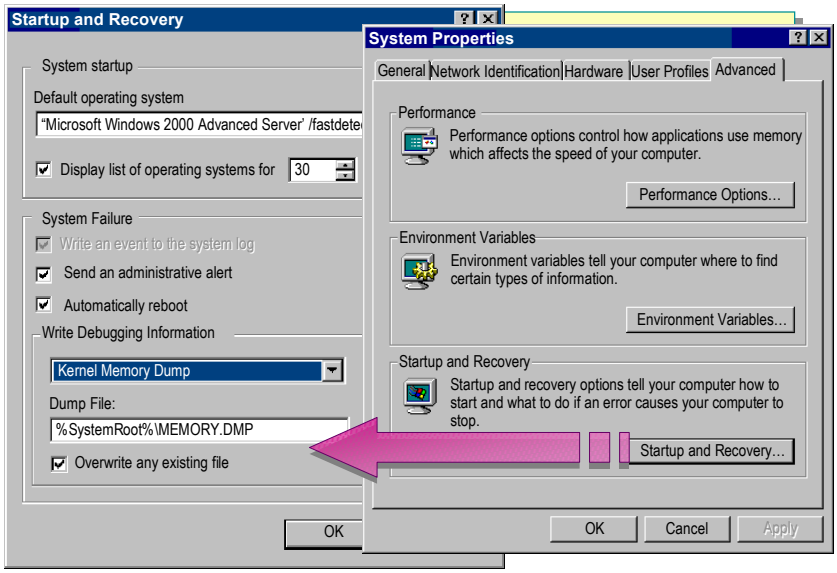
For example, if you add the line **SET TMP=C:** to Autoexec.bat, a startup file, and a TMP=X:\TEMP user variable is set, the user environment variable setting (X:\TEMP) overrides the prior setting (C:\).

The ability to configure the environment variables can be a useful administrative task. For example, suppose several users share a computer. You install a new program and it requires each user to add a path to the user's variables. As an administrator, you can add the variable to the system variables and this modification would allow all users of the computer to run the new program without having to make the changes individually.

Modifying Startup and Recovery Options

Topic Objective
To illustrate the interface for changing system settings.

Lead-in
Startup and recovery options specify the default operating system and determine how the system will recover in the event that it stops unexpectedly.



**********ILLEGAL FOR NON-TRAINER USE**********

You can configure startup and recovery options to indicate which operating system your computer uses when it starts and what actions it performs if the system stops unexpectedly.

Delivery Tip
Open the **Startup and Recovery** dialog box and describe the configuration options.

Students will not configure startup and recovery options in a lab.

To configure startup and recovery options, open the **System Properties** dialog box, click the **Advanced** tab, and then click **Startup and Recovery**.

Modifying System Startup

When you first turn on the computer, the system displays a menu that lists the available operating systems. By default, the system chooses one of the operating systems and displays a countdown timer. If you do not choose another operating system, the system starts the pre-selected operating system when the countdown timer reaches zero or when you press ENTER.

Use the options in the **System startup** area to designate which operating system starts by default. Select the appropriate operating system from the drop-down menu. Adjust the countdown timer value to control how long the system waits to automatically start the default operating system.

Configuring Recovery Settings

Use the options in the **System Failure** area to determine the actions that are automatically performed in the event of a *Stop error*. A Stop error is a severe error that causes the operating system to stop all processes.

You can configure recovery settings to indicate what actions your computer performs if the operating system generates a Stop error.

The following options are available for recovery settings:

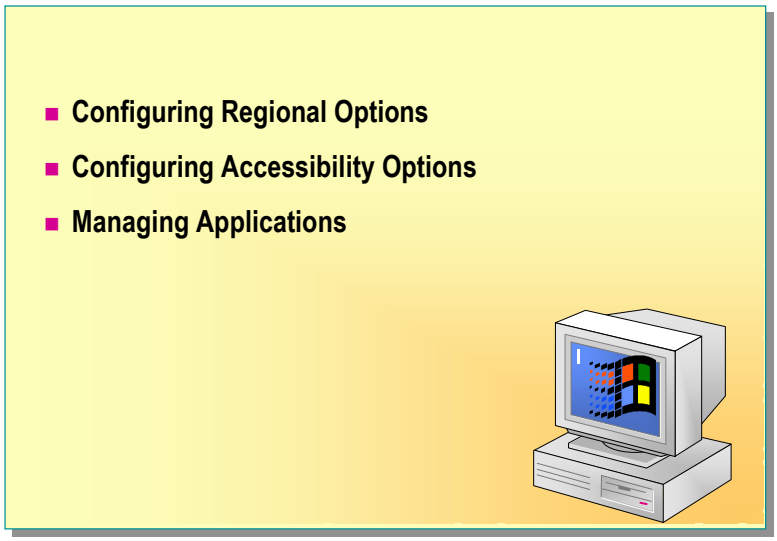
- Write an event to the system log.
- Alert administrators.
- Send system memory contents to a file that support engineers can use for debugging. This option has the following requirements:
  - The paging file must be on the same partition as the systemroot folder.
  - The paging file must be 1 megabyte (MB) larger than the amount of physical RAM in your computer.
  - You must have enough free disk space for the specified file. To overwrite a file created by a previous Stop error, select the **Overwrite any existing file** check box.
- Automatically restart the computer as part of the recovery process.

Note For more information on performance optimization and modifying the paging file, see module 8, "Monitoring and Optimizing Performance in Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Configuring the Desktop Environment

Topic Objective
To identify the topics related to configuring the desktop environment.

Lead-in
You can use the programs in Control Panel to change the appearance and functionality of Windows 2000 to meet the needs of users in your organization.



**********ILLEGAL FOR NON-TRAINER USE**********

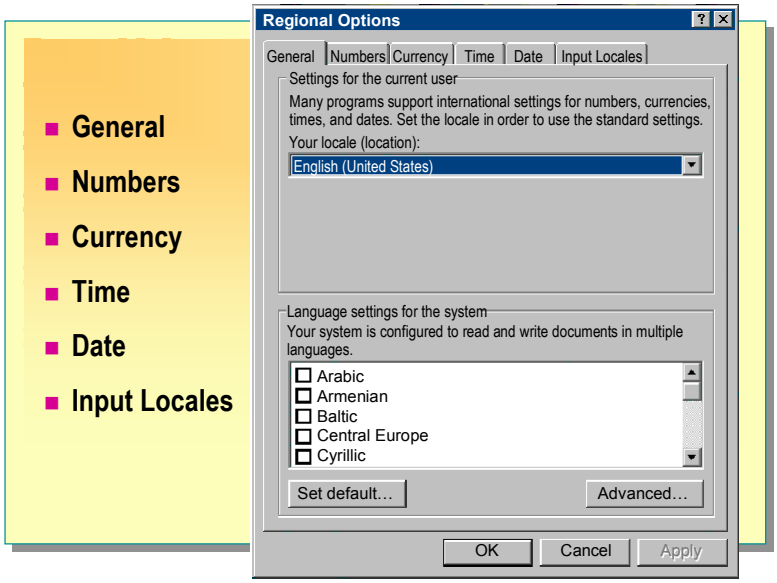
You can use Control Panel to change the appearance and functionality of Windows 2000 to meet the needs of users in your organization. For example, you can change regional options to control the way Windows 2000 displays numerical data. You can also adjust the interface for users who have difficulties with their vision or hearing, or for users who have other physical disabilities. In addition, you use Control Panel to install, remove, change, and repair applications.

A thorough understanding of the use of Control Panel and how it enables you to configure and customize Windows 2000 will help you provide desktop environments to users that maximize their productivity.

Configuring Regional Options

Topic Objective
To introduce the options that you can configure using **Regional Options** in Control Panel.

Lead-in
You use **Regional Options** in Control Panel to change the way Windows 2000 displays dates, times, currency amounts, large numbers, and numbers with decimal fractions.



**********ILLEGAL FOR NON-TRAINER USE**********

You use **Regional Options** in Control Panel to change the way Windows 2000 displays dates, times, currency amounts, large numbers, and numbers with decimal fractions. You can also choose the metric or U.S. system of measurement.

Selecting Regional Options

The following table describes the tabs available for configuration under **Regional Options**.

Tab	Function
General	Sets default display languages and standard settings for input, based on locale.
Numbers	Configures the default appearance for numbers.
Currency	Configures the default appearance for currency.
Time	Configures the default appearance for the time.
Date	Configures the default appearance for the date.
Input Locales	Installs keyboard layouts for alternative languages and sets keyboard sequences for keyboard shortcuts.

Configuring Input Locales

In addition, you can specify one of several input locales. *Input locales* are geographical location designations, such the **English (Ireland)** or **English (United States)** options, that specify which geographical region a user is in. When you switch to another input locale, some programs offer special features, such as font characters or spell checkers designed for different languages.

If you work in more than one language or communicate with speakers of other languages, you might want to install additional language groups. Each language group you install allows you to type and display documents composed in languages of that group, such as Western Europe and United States, Central Europe, Baltic, in the correct font.

Each language has a default keyboard layout, but many languages have alternate layouts. Even if you work mainly with one language, you may want to try other layouts. In English, for example, typing letters with accents might be simpler with the United States-International layout.

Configuring Accessibility Options

Topic Objective
To illustrate the interface for configuring accessibility options.

Lead-in
Accessibility Options and the Accessibility wizard enable you to configure computers for users with disabilities.

**********ILLEGAL FOR NON-TRAINER USE**********

You can adjust the appearance and behavior of Windows 2000 to enhance accessibility for users with disabilities or other special needs without requiring additional software or hardware.

Important The accessibility tools included in Windows 2000 provide a minimum level of functionality for users with special needs. To support efficient daily use, many users with disabilities will need utility programs with higher functionality. For a list of Windows-based accessibility utilities, see Microsoft Accessibility at the Microsoft Web site (http://www.microsoft.com/enable).

Running Accessibility Programs

The following table shows the programs included in Windows 2000 to enhance accessibility, together with the function of each program. To view these programs, click **Start**, point to **Programs**, point to **Accessories**, point to **Accessibility**, and then click the menu entry for the desired program.

Program	Function
Magnifier	Enlarges a portion of the screen for easier viewing.
Narrator	Uses text-to-speech technology to read the contents of the screen aloud. This is useful for people who are blind or who have low vision.
On-Screen Keyboard	Provides users, with limited mobility, the ability to type on-screen using a pointing device.
Utility Manager	Enables users, with administrator-level access, to check an accessibility program's status, start or stop an accessibility program, and specify that the program starts when Windows 2000 starts.

Selecting Accessibility Options

Use **Accessibility Options** in Control Panel to specify how to use your keyboard, display, and mouse functions. The following table shows the accessibility tools available in **Accessibility Options** and their functions.

Tool	Function
StickyKeys	Enables simultaneous keystrokes while pressing one key at a time.
FilterKeys	Adjusts the response of your keyboard.
ToggleKeys	Emits sounds when certain locking keys are pressed.
SoundSentry	Provides visual warnings for system sounds.
ShowSounds	Instructs programs to display captions for program speech and sounds.
High Contrast	Improves screen contrast with alternative colors and font sizes.
MouseKeys	Enables the keyboard to perform mouse functions.
Support SerialKeys	Allows the use of input devices other than a keyboard and mouse.

Using the Accessibility Wizard

Delivery Tip
Start the Accessibility wizard and demonstrate the types of settings that users can configure with this wizard.

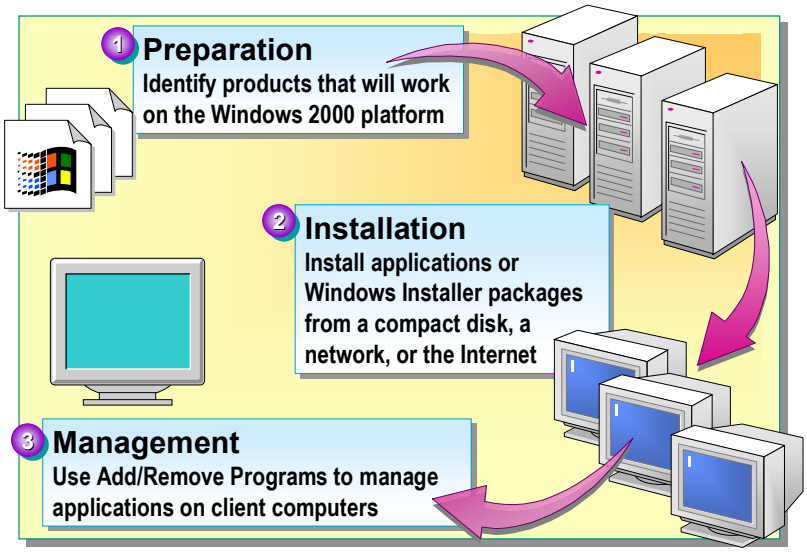
Use the Accessibility wizard to help you set up the options and programs for your individual needs. The Accessibility wizard automates configuration through dialog boxes that explain the available options. With the Accessibility wizard, you can save the configuration in a file, and then transfer it to other computers.

To start the Accessibility Wizard, click **Start**, point to **Programs**, point to **Accessories**, point to **Accessibility**, and then click **Accessibility Wizard**.

Managing Applications

Topic Objective
To illustrate the process of managing applications.

Lead-in
Windows 2000 provides several options that you can use to help manage applications more efficiently.



**********ILLEGAL FOR NON-TRAINER USE**********

Total cost of ownership (TCO) of personal computers is an important issue facing organizations today. One way to reduce TCO is to make deploying and managing applications as easy as possible. Windows 2000 provides a number of options that allow you to manage applications more efficiently.

Identifying Products for Windows 2000

You can use the online Directory of Windows 2000 Applications to identify products that will work with Windows 2000. The directory classifies applications at one of three levels, according to the level of testing they have passed:

- *Certified.* These applications meet all standards in the Application Specification for Windows 2000, and have passed all Windows 2000 compliance testing by both ISV and VeriTest, two independent testing organizations. This is the highest level ranking for Windows 2000-compatible applications.
- *Ready*. ISV has tested the application for Windows 2000 compatibility and provides Windows 2000-related product support.
- *Planned*. ISV committed to delivering a Windows 2000 compatible version of this application in the future, and has indicated that the application will be at the Ready or Certified levels.

Note For more information about Windows 2000 product compatibility, see http://www.microsoft.com/windows/professional/deploy/compatible/default.asp or http://www.microsoft.com/windows/server/deploy/compatible/default.asp for client or server, respectively.

Installing Applications Using Add/Remove Programs

Install applications directly from a compact disc, a network, or the Internet by using **Add/Remove Programs** in Control Panel. **Add/Remove Programs** uses Windows Installer to make installing, removing, changing, and repairing applications easier and more efficient. Windows Installer is a client-side operating system service for managing installed applications. For example, when a user removes an application, Windows Installer removes all of the applications files, including .dll files that may be distributed throughout the computer's hard drive.

Explain that you must be in an Active Directory environment and use Group Policy in order to publish applications.

Note Applications that appear in the **Add Programs from your network** section of **Add/Remove Programs** have a corresponding .msi file and have been published in the Active Directory™ directory service. After an application is published, computer users who are members of the domain can install it. Some software vendors include .msi files with their programs so they can be published in Active Directory.

Windows 2000 server products include WinInstall LE, used to create Windows Installer packages for software that does not include natively authored .msi files. You can then deploy Windows Installer packages using **Add/Remove Programs**, Microsoft Windows Explorer, or a command prompt.

Managing Applications Using Add/Remove Programs

Delivery Tip
Open **Add/Remove Programs** and point out each option as you describe it.

Use **Add/Remove Programs** to manage applications on client computers. Published applications in **Add New Programs** only display the **Categories** option. Using the **Categories** option makes it easier for users to find a published application under **Add New Programs**. For example, you could define categories such as Sales Applications or Accounting Applications.

Applications currently installed appear in **Change or Remove Programs** and display the following options:

- *Name*. For example under **Change or Remove Programs**, installed applications appear in user friendly names such as, Microsoft Office 97 rather than \\Server1\Msofc97\Setup.exe.
- *Frequency of use*. Lists programs by frequency of use so that those that are used infrequently can be removed to free up disk space.
- *Size*. Lists programs by size so that they are identified by the amount of disk space used. This can be helpful in determining which programs use the most disk space.
- *Date Last Used*. Sorts programs by the last date they were used. This can be helpful in determining which programs are no longer used and can be removed.

When you open Control Panel and double-click **Add/Remove Programs**, the currently installed programs appear in the list. If you click **Add New Programs**, programs that have been published in Active Directory appear in the list. You can then click **CD or Floppy** to install an application from compact disc or a floppy disk, click **Windows Update** to install an application from the Web, or click a published application. After you select your installation option, click **Add** to install the software.

Lab B: Modifying Startup and Recovery Options

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will modify startup and recovery options.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to modify startup and recovery options.

Prerequisites

Before working on this lab, you must have knowledge of startup and recovery settings.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server.

Estimated time to complete this lab: 15 minutes

Exercise 1
Disable the Display List of Operating Systems

Scenario

You have several users that are currently using computers running Windows 98. You will be upgrading their computers to Windows 2000. The users want their computers configured to run both Windows 98 and Windows 2000 for one month. You have decided that for one month, users will have 30 seconds to select an operating system at startup. For the next month, users will not have the option to select an operating system at startup. At the end of the two-month period, you will remove the Windows 98 operating system. You must present your manager with the detailed steps you will take to accomplish this task.

Goal

In this exercise, you will verify that the changes you make to the display list of operating system settings are correctly configured in the Boot.ini file.

Tasks	Detailed Steps
1. Log on to *Server* (where S*erver* is your assigned computer name) as Administrator with a password of **password** and configure Windows Explorer to show all files, including system files, hidden files, and known file extensions.	**a.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** Click **Start**, point to **Programs**, point to **Accessories**, and then click **Windows Explorer**. **c.** On the **Tools** menu, click **Folder Options**. **d.** In the **Folder Options** dialog box, on the **View** tab, under **Advanced settings**, click **Show hidden files and folders**. **e.** Clear the **Hide file extensions for known file types** and **Hide protected operating system files (Recommended)** check boxes. *A warning box appears, indicating that you have chosen to display protected operating system files in Windows Explorer.* **f.** Click **Yes** to close the **Warning** message box. **g.** Click **OK** to close the **Folder Options** dialog box.
2. Use Notepad to view the Boot.ini file.	**a.** In the Windows Explorer console tree, under My Computer, click Local Disk (C:). **b.** In the **Windows Explorer** details pane, right-click **Boot.ini**, and then click **Open With**. **c.** In the **Open With** dialog box, click **Notepad**, and then click **OK**. *A Notepad window appears, displaying the contents of Boot.ini.*

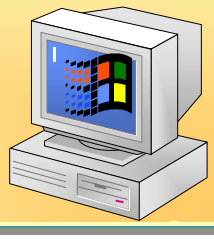
Tasks	Detailed Steps
What is the timeout value? **30.**	
2. *(continued)*	**d.** Close Notepad without saving changes to the file, and then minimize Windows Explorer.
3. View the current System startup settings configured in the **System Properties** dialog box and compare it with the setting contained in the Boot.ini file.	**a.** In Control Panel, double-click **System**. **b.** In the **System Properties** dialog box, on the **Advanced** tab, click **Startup and Recovery**. **c.** In the **Startup and Recovery** dialog box, under **System startup**, verify that the **Display list of operating systems for 30 seconds check** box is selected.
Is the time listed under **System startup** in **Startup and Recovery** the same as that listed in the Boot.ini file? **Yes.**	
4. Configure the Startup and Recovery settings so that the list of operating systems will not appear for a dual boot configuration.	**a.** In the Startup and Recovery dialog box, under System startup, clear the Display list of operating systems for 30 seconds check box. *The number of seconds resets to zero and is grayed out, indicating that the setting cannot be changed.* **b.** Click **OK** to close the **Startup and Recovery** dialog box, and then click **OK** to close the **System Properties** dialog box.
5. Verify that the settings in the Boot.ini file match those set in Startup and Recovery.	**a.** Restore Windows Explorer. **b.** Open the Boot.ini file with Notepad.
Were the changes made to Startup and Recovery settings also made in the Boot.ini file? **Yes.**	
5. *(continued)*	**c.** Close any open windows, and then log off.

Configuring Internet Options for Client Computers

Topic Objective
To illustrate how to access Internet Explorer 5 configuration options.

Lead-in
Configuration options in Internet Explorer 5 are located on the **Tools** menu under **Internet Options**.

- Changing the Home Page
- Caching Temporary Internet Files
- Configuring Proxy Server Settings
- Setting Security Levels for Web Content Zones



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to access the **Internet Options** dialog box in Control Panel for students. Have them follow along on their computers.

You can use **Internet Options** in Control Panel to configure basic settings for Internet access. The settings that you typically configure for client computers include:

- The browser's home page.
- The total disk space used for temporary Internet files.
- Proxy server between the local area network (LAN) and the Internet.
- Security levels.

To configure Internet options, double-click **Internet Options** in Control Panel. You can also access **Internet Options** within Internet Explorer from the **Tools** menu.

Changing the Home Page

The home page is the page that Internet Explorer 5 displays every time a user opens the browser. You can configure the home page to one that users need to view frequently, such as your organization's home page.

To configure the browser's home page, display the Web page that you want to appear when you first start Internet Explorer. Then, in **Internet Options**, click the **General** tab, and then click **Use Current** under **Home Page**.

Caching Temporary Internet Files

Internet Explorer stores, or caches, files on the local hard disk when a user accesses Web files. This improves browser performance when the user subsequently accesses the same Web sites. You can configure the amount of disk space allocated to the cache.

To configure cache disk space, in **Internet Options**, click the **General** tab, and then click **Settings** under **Temporary Internet Files**. Use the slider or the **MB** box to adjust the amount of disk space that is used.

Configuring Proxy Server Settings

Some networks use a proxy server to access resources on the Internet. A proxy server can improve performance for users by caching and directly supplying frequently requested data. Proxy servers can also act as a firewall by filtering and discarding requests that are not appropriate, such as requests for unauthorized access to proprietary files.

To configure Internet Explorer to use a proxy server, click the **Connections** tab in **Internet Options**, and then click **LAN Settings**. Under **Proxy server**, select the **Use a proxy server** check box. Type the address of the proxy server in the **Address** box and the port number in the **Port** box, and then click **OK**.

Note To improve performance for intranet Web sites, select the **Bypass proxy server for local addresses** check box.

Setting Security Levels for Web Content Zones

Windows 2000 allows you to configure security levels in **Internet Options** for each of the four Web content zones: Internet, Local intranet, Trusted sites, and Restricted sites. This allows you to configure security settings in each Web content zone to prevent users from browsing potentially harmful Web sites.

The following table summarizes the four zones.

Web content zone	Description
Internet	By default, all zones that have not been placed in a different zone.
Local intranet	All Web sites and Universal Naming Convention (UNC) paths from your local intranet.
Trusted sites	Web sites that you choose to trust not to damage your computer or data.
Restricted sites	Sites that could potentially damage your computer or data.

On the **Security** tab of **Internet Options**, define the level of security to implement for different zones accessed via Internet Explorer. The **Security** tab features four content zones. Each zone allows you to set the level of security from high to low using a slider bar on the menu.

The security level slider has four different levels of security:

- *High*. This level disables *cookies* and many other features. Some Web sites will not function correctly. Cookies are small text files placed on your hard drive by a Web server.
- *Medium*. This level prompts the user before downloading potentially unsafe content. Internet Explorer will not download unsigned Microsoft ActiveX® controls. Most Web sites function correctly. This is the most common security setting.
- *Medium-low*. Most content is enabled without prompts before downloading. It will not download unsigned ActiveX controls.
- *Low*. Most content is downloaded. Appropriate for trusted Web sites. All active content can run without prompting the user.

Under the **Custom Level** area, customize the details of each zone security setting, allowing or disallowing specific Web-related features. On the **Sites** tab, add specific Web sites to add or remove from a particular Web content zone. By default, Internet Explorer is configured to operate with a standard recommended security setting. You alter each zone to suit your particular environment as needed.

Lab C: Configuring Internet Options

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will configure Internet options.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure the Internet Connection wizard.
- Configure a home page.
- Configure the amount of space used for temporary Internet files.
- Configure proxy settings.
- Configure security levels for zones.

Prerequisites

Before working on this lab, you must have knowledge of **Internet Options** in Control Panel.

Lab Setup

To complete this lab, you need a computer running Microsoft Windows 2000.

Estimated time to complete this lab: 10 minutes

Exercise 1
Configure Internet Options

Scenario

As network administrator, you have configured **Internet Options** on all computers. A new computer was just purchased and Windows 2000 was installed. This computer is going to be used by a new administrator for the purpose of doing research on the company Web site. The IT manager wants you to configure **Internet Options** for the administrator.

Goal

In this exercise, you will configure **Internet Options** on the new administrator's computer. You will configure the following options:

- Configure the Internet Connection wizard.
- Set the default Web page to www.microsoft.com.
- Set the space for temporary Internet files at 100 megabytes (MB).
- Set the Internet zone for high security.
- Configure the local area network (LAN) proxy settings.

Tasks	Detailed Steps
1. Log on as Administrator with a password of **password** and complete the configuration of the Internet Connection wizard.	**a.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** On the desktop, double-click **Connect to the Internet**. **c.** On the **Welcome to the Internet Connection Wizard** page, click **I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)**, and then click **Next**. **d.** On the **Setting up your Internet Connection** page, click **I connect through a local area network (LAN)**, and then click **Next**. **e.** On the **Local area network Internet configuration** page, click **Next** to accept the default settings. **f.** On the **Set Up Your Internet Mail Account** page, click **No**, and then click **Next**. **g.** On the **Completing the Internet Connection Wizard** page, clear the **To connect to the Internet immediately, select this box and then click Finish** check box, and then click **Finish**.
2. Open **Internet Options** in Control Panel. On the **General** tab, set the home page to www.microsoft.com.	**a.** Click **Start**, click **Settings**, and then click **Control Panel**. **b.** Double-click **Internet Options**. **c.** On the **General** tab, under **Home page**, in the **Address** box, type **www.microsoft.com** and then click **Apply**.

Tasks	Detailed Steps
How does this affect what will display when Internet Explorer is opened? **When Internet Explorer is opened, the Web page for www.microsoft.com will appear.**	
3. Set the disk space used for temporary Internet files at 100 MB.	**a.** On the General tab, under Temporary Internet files, click Settings. **b.** In the **Settings** dialog box, under **Temporary Internet files** folder, in the **Amount of disk space to use** box, type **100** and then click **OK**.
4. Set the Internet zone to high security.	**a.** On the Security tab, under Select a Web content zone to specify its security settings, verify that Internet is selected, and then under Security level for this zone, move the slider bar to High.
5. Set the local area network to use the following proxy server settings: PROXYSRV and Port 80.	**a.** On the Connections tab, click LAN Settings. **b.** In the **Local Area Network (LAN) Settings** dialog box, clear the **Automatically detect settings** check box. **c.** In the **Local Area Network (LAN) Settings** dialog box, select the **Use a proxy server** check box, enter the following information, and then click **OK**. Address: **http://proxysrv** Port: **80**
Note: Substitute any instructor supplied information if necessary for this step.	
5. *(continued)*	**d.** Click **OK** to close the **Internet Properties** dialog box. **e.** Close Control Panel, and then log off.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Configuring and Managing Hardware
- Configuring Display Options
- Configuring System Settings
- Configuring the Desktop Environment
- Configuring Internet Options for Client Computers

**********ILLEGAL FOR NON-TRAINER USE**********

1. An administrator copies Profile 1 (current) and names the new profile Network Disabled. The user immediately restarts the computer and selects the hardware profile named **Network Disabled**. The user can still access the network resources. The administrator asks you to troubleshoot the profile. What would you check?

   You would check to see if the administrator configured the network adapter to be disabled with this hardware profile.

2. A user installs a video adapter that supports multiple monitors. On the first startup after installation of the video adapter, the user clicks the **Settings** tab under **Display Properties**, and extends the Windows desktop onto the new monitor. However, the physical location of the monitors does not match the display on the **Settings** tab under **Display Properties**. The user wants to have the **Settings** tab display the monitors so that they reflect the physical position. How can the user accomplish this?

   The user should click Identify on the Settings tab to indicate monitor 1 and monitor 2, and then click and drag the displays in the Settings tab to reflect the physical position of the monitors.

3. A user tells you that they want to change the TEMP folder location under the **System Variables** area of the **Environment Variables** dialog box for their computer, but that the commands display as disabled. Why can't the user change the TEMP folder location?

   The user is not a member of the local administrators group.

4. A new employee is hired to write a company newsletter. The company newsletter must be in both Spanish and English. The employee must have the ability to switch the keyboard between an English layout and a Spanish layout. Where can the employee configure this option?

   In Control Panel open Regional Options. On the Input Locales tab of the Regional Options dialog box, add the Spanish input locale needed and then install the appropriate keyboard layout.

5. A manager wants to increase the amount of disk space used by temporary Internet files. What steps must the manager take to accomplish this?

   In Internet Options, click the General tab, and then click Settings under Temporary Internet Files. Use the slider or the MB box to adjust the amount of disk space that is used.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 3: Connecting Windows 2000–based Clients to Networks

Contents

Overview	1
Windows 2000 Connectivity	2
Connecting to a Microsoft Network	4
Lab A: Configuring and Testing IP Addresses	13
Connecting to a Novell NetWare Network	23
Lab B: Installing and Configuring Gateway (and Client) Services for NetWare	31
Review	32

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware.

Instructor Notes

Presentation:
60 Minutes

Labs:
45 Minutes

This module provides students with the knowledge and skills necessary to connect client computers running Microsoft® Windows® 2000 to networks on which Windows 2000–based servers or Novell NetWare-based servers reside. Students will learn to install and configure Transmission Control Protocol/Internet Protocol (TCP/IP) and NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, in addition to the required services.

At the end of this module, students will be able to:

- Describe the components connectivity in a Windows 2000 environment.
- Connect to a Microsoft network.
- Connect to a Novell NetWare network.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_03.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the white paper, *Microsoft Windows 2000 Professional Operating System in a Novell NetWare Environment*, located under **Additional Reading** on the Student Materials compact disc.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for a lab.

Lab A: Configuring and Testing IP Addresses

► **To prepare for the lab**

1. Instructor computer must be configured as a Dynamic Host Configuration Protocol (DHCP) server for the classroom. See the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.
2. Students must have the classroom organizational chart stating the student number and the static IP address to use for the lab. See the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab B: Installing and Configuring Gateway (and Client) Services for NetWare

► **To prepare for the lab**

- Students must have completed module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Module Strategy

Use the following strategy to present this module:

- Windows 2000 Connectivity

  In this topic, provide a brief overview of the components of connectivity in a network running both Windows 2000 and Novell NetWare. These components include protocols, services, network interface cards, and bindings. When presenting this information, describe each component and explain its role in the connection process.

- Connecting to a Microsoft Network

  In this topic, provide information about connecting to a network running Windows 2000 or Microsoft Windows NT® version 4.0. First, explain how to install TCP/IP. Next, explain how to configure TCP/IP for automatic IP addressing: first through a DHCP server, and then through Automatic Private IP Addressing. (Note that the slide for this topic is animated. Click the build icon, or press the SPACEBAR to advance.)

  Next, present the information on configuring a static IP address. Demonstrate configuring the different components, but do not apply the changes. Next, demonstrate how to use the **ipconfig** and **ping** commands to verify and test the TCP/IP configuration. (Note that the slide for this topic is animated.) Finally, present the different ways that a user at a computer running Windows 2000 can connect to another computer running Windows 2000.

- Connecting to a Novell NetWare Network

  In this topic, provide information about configuring connectivity to a network running Novell NetWare. First, present information on the components that facilitate connectivity between Microsoft Windows 2000-based computers and Novell NetWare-based computers. (Note that the slide for this topic is animated.) Next, demonstrate how to install and configure NWLink. Next, demonstrate the procedures for installing Gateway (and Client) Services for NetWare. Finally, present the different ways that a user at a client computer running Windows 2000 can connect to a Novell NetWare-based server.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

There are no lab setup requirements that affect replication or customization. The following information describes the setup requirements for the labs in this module.

Setup Requirement for Lab A

The first lab in this module requires completion of the following:

- Install and configure the instructor computer according to the guidelines outlined in the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.
- Complete lab A, "Installing Windows 2000," in module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Setup Requirement for Lab B

The second lab in this module is a simulation and therefore can run on any computer running Windows 2000, Microsoft Windows 95, Microsoft Windows 98, and Windows NT versions 3.51 and 4.0.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

- Performing the labs in this module introduces no configuration changes.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about connecting client computers running Windows 2000 to both Microsoft and Novell networks.

- **Windows 2000 Connectivity**
- **Connecting to a Microsoft Network**
- **Connecting to a Novell NetWare Network**

**********ILLEGAL FOR NON-TRAINER USE**********

A network consists of multiple computers that communicate with each other. In order for multiple computers to communicate, common rules and methods for communicating—called protocols—must be applied to the computers. In a network that has resources that exist on both Microsoft® Windows® 2000–based servers and Novell NetWare-based servers, you must ensure that users can gain access to these resources.

You can configure client computers running Windows 2000 with a variety of communications protocols to ensure proper connectivity to both Microsoft networks and Novell NetWare networks.

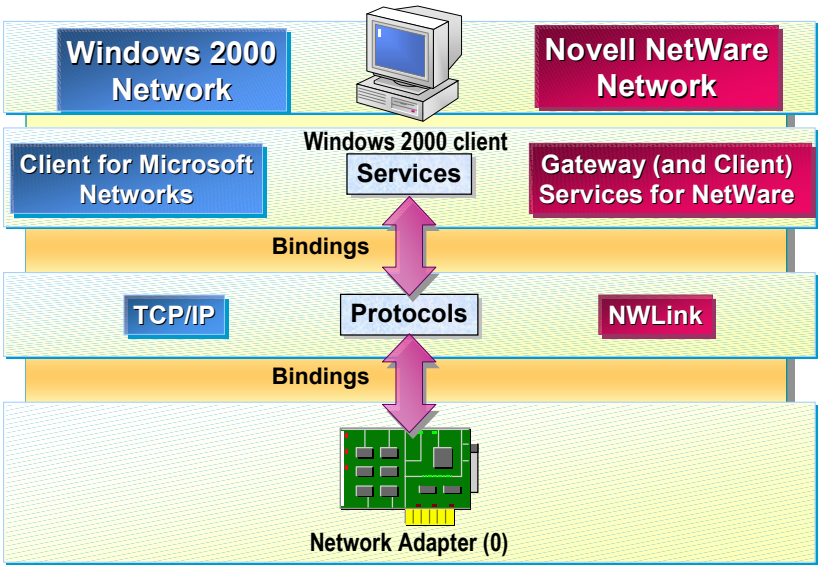
At the end of this module, you will be able to:

- Describe the components of connectivity in a Windows 2000 environment.
- Connect to a Microsoft network.
- Connect to a Novell NetWare network.

Windows 2000 Connectivity

Topic Objective
To illustrate the function of the four main components involved in connectivity.

Lead-in
There are four components that enable a connection between a computer running Windows 2000 and a Windows 2000 network, or a Novell NetWare network.



**********ILLEGAL FOR NON-TRAINER USE**********

Computers running Windows 2000 use four components to support connectivity to a Windows 2000 or NetWare network:

- Protocols
- Network services
- Network adapters
- Bindings

In order to effectively configure network connectivity, you need to understand how the components interact to make that connection occur.

Protocols

A protocol is a set of rules and conventions for sending information over a network. These rules govern the content, format, timing, sequencing, and error control of data exchanged among network devices. Protocols makes it possible for networks to move data, so different computers can share information.

Windows 2000 automatically installs Transmission Control Protocol/Internet Protocol (TCP/IP). You must manually install NWLink IPX/SPX/NetBIOS Compatible Transport Protocol.

Network Services

Network services allow computers running the same network protocols to connect to shared folders and other resources. Network Services provide a network function to applications, such as the ability to gain access to shared folders and printers on other computers. These services consist of software that is part of Windows 2000, or is supplied by a third party.

Microsoft Windows 2000 automatically installs Client for Microsoft Networks. If necessary, you can manually install Gateway (and Client) Services for NetWare.

Network Adapters

A network adapter is a hardware component that allows a computer to connect to a network cable or other network medium. Network adapters provide the physical interface (connector) and the hardware (circuitry) to let a computer access a network.

Bindings

Bindings are a method of linking network components. A binding enables communication between the various network components, such as between TCP/IP and a network adapter. By changing the order of protocols bound to those providers, you can improve performance. For example, assume your local area network (LAN) connection is enabled to access NetWare using IPX, and Microsoft Windows networks using TCP/IP. However, you primarily use your computer to connect is to a Microsoft Windows network that uses TCP/IP.

In this example, in order to improve performance, you want to configure TCP/IP as your primary protocol. To configure TCP/IP as your primary protocol, perform the following tasks:

1. Move Microsoft Windows Network to the top of the Network providers list on the **Provider Order** tab.
2. Move Internet Protocol (TCP/IP) to the top of the **File and Printer Sharing for Microsoft Networks** binding on the **Adapters and Bindings** tab.

Note For more information about protocols, see module 4, "Examining the Network," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

For a description of other protocols supported by Windows 2000, see appendix A, "Protocols Supported by Windows 2000," on the Student Materials Web page on the Student Materials compact disc. To view appendix A, click **Appendices**, and then click the title of the appendix.

◆ Connecting to a Microsoft Network

Topic Objective
To identify the topics related to connecting to a Microsoft network.

Lead-in
Microsoft networks rely on TCP/IP for the logon process, file and print services, replication of information between domain controllers, and other common functions.

- **Installing TCP/IP for Connectivity Within a Microsoft Network**
- **Configuring TCP/IP to Obtain an IP Address Automatically**
- **Configuring TCP/IP to Use a Static IP Address**
- **Verifying and Testing a TCP/IP Configuration**
- **Connecting to a Windows 2000 Network Resource**

**********ILLEGAL FOR NON-TRAINER USE**********

To connect to a Microsoft network, you must first install and configure the appropriate protocol, then install and configure the service, and finally configure the bindings, if required. The process of configuring the computer to connect to a Microsoft network is greatly simplified in Windows 2000. During installation, Windows 2000 automatically installs the following services and protocol needed to connect to a Microsoft network:

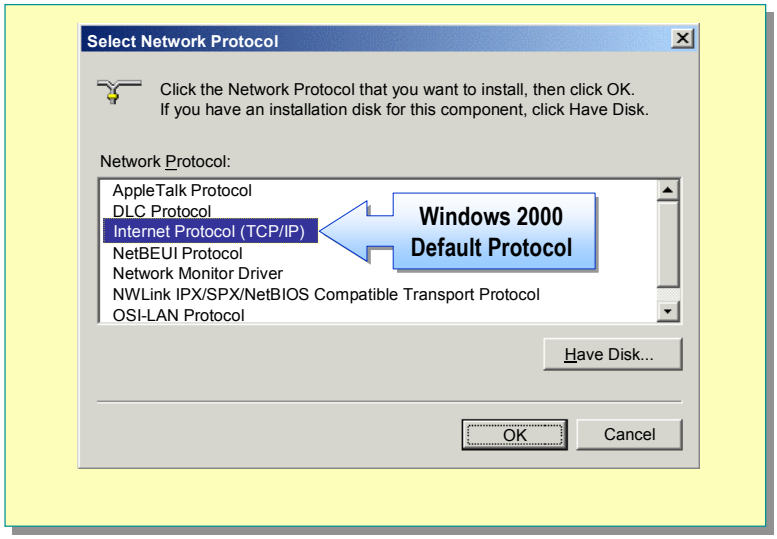
- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- TCP/IP

Networks running Windows 2000 and using TCP/IP can take advantage of such network services as the Domain Name System (DNS) Server service, the Dynamic Host Configuration Protocol (DHCP) Server service, and the Active Directory™ directory service. Understanding how to enable TCP/IP connectivity for a client computer running Windows 2000 allows you to take advantage of these and other network services.

Installing TCP/IP for Connectivity Within a Microsoft Network

Topic Objective
To illustrate the interface used to install TCP/IP.

Lead-in
TCP/IP is the default protocol that is installed during Windows 2000 Setup. In order to connect to a Windows 2000 network, you must install TCP/IP.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate this procedure for students. Students should not perform this procedure for installing TCP/IP now, however, as it is already installed on their computers.

Windows 2000 automatically installs TCP/IP as the default protocol during installation (if a network adapter is detected). However, if TCP/IP was not installed during installation, you can install it manually.

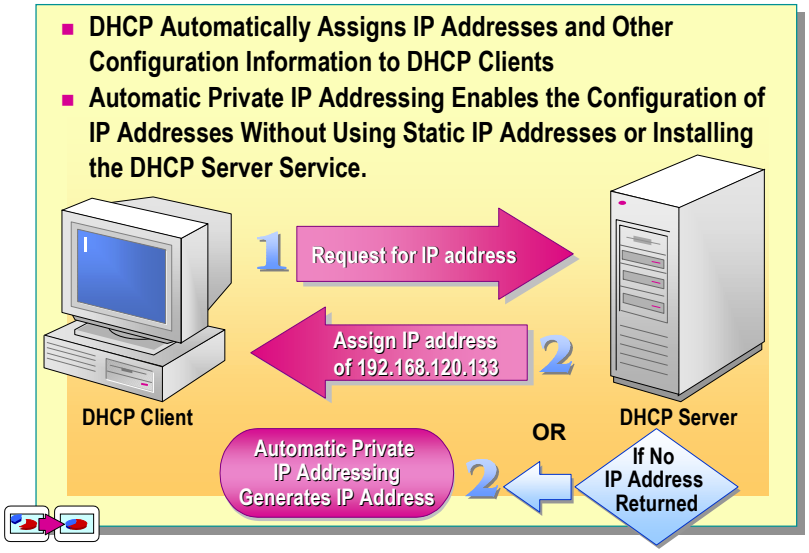
To install TCP/IP, perform the following steps:

1. Right-click **My Network Places**, and then click **Properties**.
2. In the Network and Dial-up Connections window, right-click the icon that represents the local area connection that you want to configure, and then click **Properties**.
3. Verify that Internet Protocol (TCP/IP) is not on the list of installed components.
4. Click **Install**.
5. Click **Protocol**, and then click **Add**.
6. In the **Select Network Protocol** dialog box, click **Internet Protocol (TCP/IP)**, and then click **OK**.
7. Verify that the **Internet Protocol (TCP/IP)** check box is selected, and then click **OK**.

Configuring TCP/IP to Obtain an IP Address Automatically

Topic Objective
To illustrate how client computers obtain IP addressing information automatically.

Lead-in
By default, client computers running Windows 2000 are automatically configured to obtain TCP/IP configuration information from a DHCP server.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon or press the SPACEBAR to advance the animation.

After installing TCP/IP, the client computer obtains an IP address in one of two ways if TCP/IP has been configured to obtain an IP address automatically:

- From a DHCP server
- Through Automatic Private IP Addressing

DHCP Addressing

A DHCP server automatically provides an IP address and other TCP/IP configuration information, such as the IP address of the DNS server, the WINS server, and default gateway. The process a DHCP server uses to automatically provide the IP address is as follows:

1. The client computer requests an IP address from the DHCP server.
2. The DHCP server provides the IP address to the client computers.

You must ensure that TCP/IP settings are configured in order for a client computer to obtain an IP address automatically from a DHCP server. By default, Windows 2000 automatically configures these TCP/IP settings. If for some reason the client computer is not configured to obtain an IP address automatically, you can configure TCP/IP manually.

To configure TCP/IP to obtain an IP address through DHCP, perform the following steps:

1. Right-click **My Network Places**, and then click **Properties**.
2. In the Network and Dial-up Connections window, right-click the icon that represents the network connection that you want to configure, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically**, and then click **Apply**.

Automatic Private IP Addressing

Automatic Private IP Addressing enables the configuration of an IP address in the event that the client computer cannot receive an IP address from a DHCP server. Automatic Private IP Addressing only provides an IP address and a subnet mask, not additional configuration information such as a default gateway. This limits the connectivity to the LAN of the client computer. The client computer cannot connect to other networks or the Internet.

When a computer without an IP address starts, the following occurs:

1. The client computer attempts to locate a DHCP server and obtain IP configuration information from it.
2. If a DHCP server cannot be found, the client computer automatically configures its IP address and subnet mask using a selected address from the Microsoft-reserved, class B network, 169.254.0.0, with the subnet mask, 255.255.0.0.

Make sure that students understand what a Microsoft-reserved, class B network is.

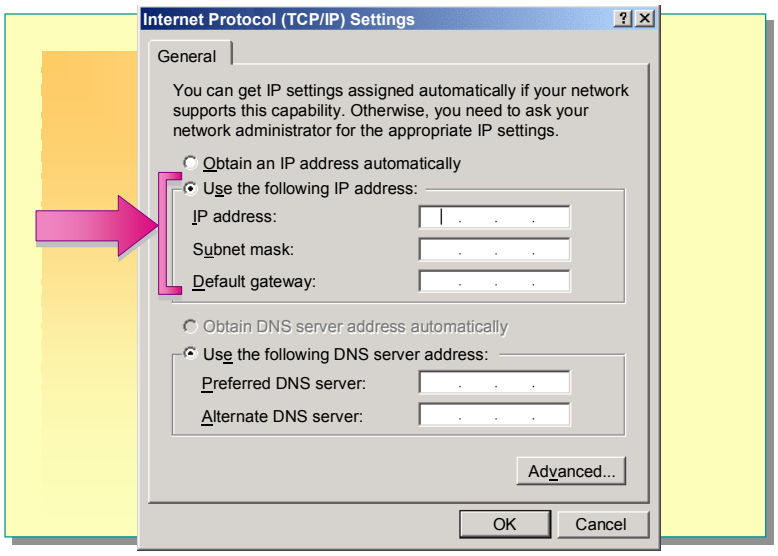
Note For more information about the DHCP Server service, see module 2, "Automating IP Address Assignment," in course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

For more information about Automatic Private IP Addressing, see appendix B, "Automatic Private IP Addressing," on the Student Materials Web page on the Student Materials compact disc. To view appendix B, click **Appendices**, and then click the title of the appendix.

Configuring TCP/IP to Use a Static IP Address

Topic Objective
To illustrate the interface for configuring TCP/IP to use a static IP address.

Lead-in
Even in a network running the DHCP Server service, there are times when you may want to manually assign IP addressing information to selected network computers.



**********ILLEGAL FOR NON-TRAINER USE**********

In a network running the DHCP Server service, there are times when you may want to manually configure static IP addresses for network computers. For example, a computer that is running the DHCP Server service cannot be a configured to receive an automatic IP address. In addition, a mail server or a Web server might need to keep the same IP address; therefore, you must configure these computers with a static IP address.

Static IP Address Settings

When you configure a static IP address, you must configure the subnet mask and default gateway for each network adapter in a computer on a network using the TCP/IP protocol. The following table describes the TCP/IP configuration settings.

Configuration setting	Description
IP address	A 32-bit address that identifies a TCP/IP host. Each network adapter in a computer running TCP/IP requires a unique IP address, which is normally shown in decimal format, such as 192.168.0.108. Each address has two parts: a network ID, which identifies all hosts on the same network, and a host ID, which identifies a specific host on the network. In this example, the network ID is 192.168.0 and the host ID is 108, based on a default subnet mask.
Subnet mask	A number that is used to determine which subnet the computer is on. Subnets divide a large intranet network into multiple networks that are connected with routers. A subnet mask indicates which part of a host's IP address is the network ID and which part is the host ID. When hosts try to communicate, they use their subnet mask to determine whether the destination host is on a local or remote network.

(*continued*)

Configuration setting	Description
Default gateway	The router that a host will send all IP packets for remote networks to when it does not have a specific route for that network. A default gateway is generally configured with routing information that allows it to forward packets to the destination network or to other intermediate routers. To communicate with a host on another network, configure an IP address for the default gateway.

Ideally, your organization's Information Technology (IT) team would be responsible for providing individual administrators with the static IP information for their individual sites. This should prevent the use of incorrect IP addresses.

Caution If two or more computers running Windows 2000 have the same IP address, Windows 2000 displays a warning message on both computers and disables TCP/IP on the computer with the duplicate IP address. The warning message appears when you start the computer and continues to appear at startup until you change the IP address or you remove the computer with the duplicate IP address. Computers that run other operating systems may not provide the same mechanism for detecting IP address conflicts. For more information about IP addressing, see module 6, "Examining TCP/IP," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Configuring a Static IP Address

Delivery Tip
Demonstrate the procedure for the students, but do not apply the changes.

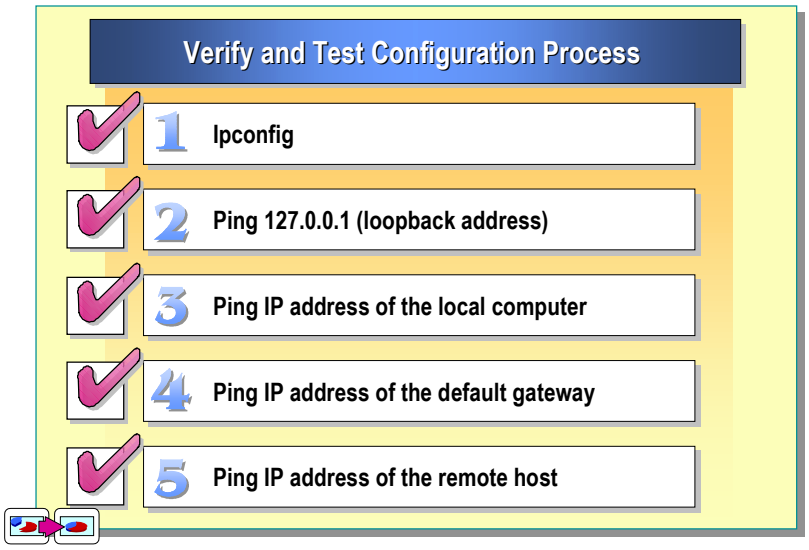
To configure TCP/IP to use a static IP address, perform the following steps:

1. Right-click **My Network Places**, and then click **Properties**.
2. In the Network and Dial-up Connections window, right-click the icon that represents the local area connection that you want to configure, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Use the following IP address**.
5. Type the IP address, subnet mask, and default gateway (if required), and then click **OK**.

Verifying and Testing a TCP/IP Configuration

Topic Objective
To identify the procedure for using the **ipconfig** and **ping** commands to verify and test a TCP/IP configuration.

Lead-in
After configuring TCP/IP, you should verify and test the configuration by using the **ipconfig** and **ping** commands.



**********ILLEGAL FOR NON-TRAINER USE**********

After configuring TCP/IP, use the **ipconfig** and **ping** commands to test the configuration of the local computer, and to ensure that the computer can communicate using TCP/IP across a network using TCP/IP.

Delivery Tip
The slide combines the **ipconfig** and the **ping** commands. Do not build the slide until you reach the section on the overall testing process.

Ipconfig

The **ipconfig** command displays TCP/IP configuration information on the computer on which it is run and determines whether the computer is TCP/IP initialized. You can then view the displayed information to verify if it is correct.

Key Point
By combining the **ipconfig** and **ping** commands, an administrator can ensure that the user can connect from their client computers running Windows 2000 to Windows 2000-based servers.

Ping

The **ping** command is a diagnostic tool that you can use to test TCP/IP configurations between two computers and diagnose connection failures. Run the **ping** command to determine whether you can communicate with another TCP/IP host.

Verifying and Testing TCP/IP

By combining the **ipconfig** and **ping** commands, you can test the local computer's IP configuration and the IP connection between two computers on the network. The following steps outline the procedure for using the **ipconfig** and **ping** commands in combination:

1. At a command prompt, type **ipconfig**

   The result of the **ipconfig** command is as follows:

   - If TCP/IP has initialized, the **ipconfig** command displays the IP address and subnet mask for each network adapter in your computer. Ipconfig also displays other configuration settings, such as the default gateway.
   - If a duplicate IP address exists, the **ipconfig** command indicates that the IP address is configured; however, the subnet mask is 0.0.0.0., which indicates that the computer's IP address is in use on the network.

     An Automatic Private IP Address always has a network ID of 169.254.0.0. If you show a network ID beginning with 169.254.*x.x*., then you are not receiving an IP address from a DHCP server and are instead receiving an address through Automatic Private IP Addressing.

   Note For a list of all switches for the **ipconfig** command, type **ipconfig /?**

Delivery Tip
Demonstrate the result of successful and unsuccessful **ping** commands by typing the following commands: **ping 127.0.0.1** (which is successful) and **ping 192.168.0.108** (which is not successful).

2. Run the **ping** command with the loopback address (**ping 127.0.0.1**) to verify that TCP/IP is correctly installed. A *loopback address* is an address that your computer uses to identify itself.

   Note The syntax for the **ping** command is **ping** *IP_address*, where *IP_address* is the address for another TCP/IP host or computer.

3. Run the **ping** command with the IP address of the local computer to verify that your IP address is configured correctly.
4. Run the **ping** command with the IP address of the default gateway to verify that your computer can communicate with the local network. Although you can **ping** any computer on the local network to verify that your computer can connect to the local network, the default gateway is most commonly used because it is usually never shut down or turned off.
5. Run the **ping** command with the IP address of a remote host to verify that the computer can communicate through a router.

By default, the following message appears four times after a successful **ping** command:

```
Reply from IP_address
```

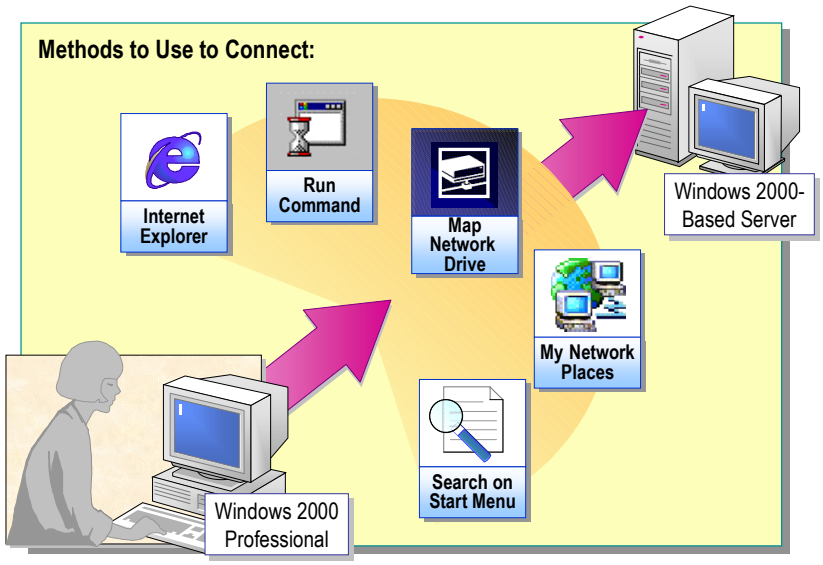
Followed by statistical information:

```
Ping Statistics for IP_address
Packets:  Sent = #, Received = #, Lost = # (#% lost)
Approximate round trip times in milliseconds:
Minimum = #ms, Maximim = #ms, Average = #ms
```

Connecting to a Windows 2000 Network Resource

Topic Objective
To identify the different methods a user can employ to connect to a Windows 2000-based server.

Lead-in
After you have set up and verified connectivity for your network computers, users can connect to any Windows 2000-based server on your organization's network.



**********ILLEGAL FOR NON-TRAINER USE**********

Emphasize that there are several methods to connect to a Windows 2000 network resource.

After you set up a computer running Windows 2000 and verify connectivity to a Microsoft network, you can use a variety a methods to connect to network resources such as shared folders and shared printers.

To connect to a network resource from a Windows 2000-based computer you can:

- Use Internet Explorer. Start Internet Explorer, browse for the network resource, and then connect to it.
- Use the **Run** command. On the **Start** menu, click **Run**, and then type the path to the network resource in the **Open** box.
- Use **Map Network Drive**. Right-click **My Computer** or **My Network Places**, and then click **Map Network Drive**. Type the path to the network resource in the **Path** box.
- Use **My Network Places**. Start **My Network Places**, expand the network tree, browse for the network resource, and then connect to it.
- Use Search. Click **Start**, point to **Search**, and then select the appropriate category. Enter the information to locate the network resource, and then connect to it.

Lab A: Configuring and Testing IP Addresses

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will configure IP addresses. You will then verify that TCP/IP is correctly installed and test to ensure that it operates properly.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure Microsoft Windows 2000 to use a dynamic IP address.
- Configure Windows 2000 to use a static IP address.

Prerequisites

Before working on this lab, you must have:

- Knowledge about dynamic and static IP addressing.
- Knowledge about the function of protocol bindings.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- A user account in the domain named Admin*x* (where *x* is your assigned student number).
- The IP address of the instructor computer, which you should record below:

_____

Estimated time to complete this lab: 30 minutes

Exercise 1
Verifying TCP/IP Configuration and Functionality

Scenario

Your company has just received a new range of IP addresses they will use on client computers to access the Internet, so you will be changing your server's TCP/IP configuration in the near future. Before you make any changes, you need to confirm the existing configuration so that you can revert to it if necessary.

Goal

In this exercise, you will log on as a user without administrative rights on the local computer and then attempt to change the TCP/IP properties. You will then log on with a user account that has administrative rights on the local computer and verify the existing TCP/IP properties.

Tasks	Detailed Steps
1. Log on to the nwtraders domain as Student*x* (where *x* is your assigned student number) with a password of **domain** and attempt to modify the TCP/IP properties.	**a.** Log on using the following information: User name: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** (Hint: Click **Options** to display the **Log on to** area of the dialog box.) **b.** Click **Start**, point to **Settings**, and then click **Control Panel**. **c.** In Control Panel, double-click **Network and Dial-up Connections**. **d.** In the **Network and Dial-up Connections** dialog box, right-click **Local Area Connection**, and then click **Properties**. *A message appears, indicating that you do not have sufficient privileges to access the TCP/IP properties.*
What privileges does the user account need to have to modify TCP/IP properties? **The user account must have administrative privileges for the computer on which you are configuring the TCP/IP setting.**	
1. (*continued*)	**e.** Click **OK** to close the **Local Network** message box. **f.** Click **Close** to close the **Local Area Connection Properties** dialog box. **g.** Close Network and Dial-up Connections, and then log off.

Tasks	Detailed Steps
2. Log on to the nwtraders domain as Admin*x* (where *x* is your assigned student number) with a password of **domain**. Verify the existing TCP/IP properties by using the **ipconfig** and **ping** commands.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In the Configure Your Server wizard, clear the **Show this screen at startup** check box, and then close the wizard. **c.** Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**. **d.** At the command prompt, type **ipconfig /all | more** and then press ENTER. *The Ipconfig utility displays the TCP/IP properties of the physical and logical adapters that are configured on your computer.*

Use the information displayed on the screen about your local area connection to complete as much of the following table as possible. Press the SPACEBAR to display additional information, as necessary.

Answers will vary.

Setting	Value
Host Name	
Description	
Physical Address	
DHCP Enabled	
IP Address	
Subnet Mask	
DNS Servers	

2. (*continued*)	**e.** Verify that TCP/IP is working and is bound to your adapter by typing **ping** *ip_address* (where *ip_address* is the IP address of your computer), and then press ENTER. *Four **Reply from** **ip_address** responses indicate that TCP/IP has been configured and bound to the local adapter.* **f.** Test TCP/IP connectivity with the instructor computer by typing **ping** *instructor_ip_address* (where *instructor_ip_address* is the IP address of the instructor computer), and then press ENTER. **g.** Minimize the command prompt.

By successfully pinging the IP address of the local computer and the instructor computer what conclusion can you draw about the above computers TCP/IP configuration?

That TCP/IP is installed and configured properly on the above computers and because of this you have established basic communications on these computers.

Exercise 2
Configuring TCP/IP to Obtain an IP Address Automatically

Scenario

Your organization is implementing DHCP to provide IP addresses to all of the client computers on the network. You need to configure all client computers to have their IP addresses and TCP/IP configuration settings assigned by a DHCP server.

Goal

In this exercise, you will configure your computer as a DHCP client and compare the configuration with the configuration you recorded in exercise 1.

Tasks	Detailed Steps
1. Configure TCP/IP to obtain an IP address automatically.	**a.** In Control Panel, double-click **Network and Dial-Up Connections**. **b.** Open the **Properties** dialog box for Local Area Connection. **c.** Click **Internet Protocol (TCP/IP)**, verify that the check box to the left of the entry is selected, and then click **Properties**. **d.** In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically**. **e.** Click **Obtain DNS server address automatically**. **f.** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box, and then click **OK** to close the **Local Area Connection Properties** dialog box. **g.** Minimize Network and Dial-up Connections.
2. Test the automatic IP configuration by using the Ipconfig and Ping utilities.	**a.** Restore the command prompt, type **ipconfig /all | more** and then press ENTER.

Use the information about your local area connection that is displayed on the screen to complete as much of the following table as possible. Press the SPACEBAR to display additional information, as necessary.

Answers will vary.

Setting	Value
DHCP Enabled	
IP Address	
Subnet Mask	
DNS Servers	
Lease Obtained	
Lease Expires	

Tasks	Detailed Steps
What is different about your TCP/IP properties? **You have a different IP address and it is leased.**	
2. (*continued*)	**b.** At the command prompt, type **ping** *ip_address* (where *ip_address* is the IP address of your computer), and then press ENTER. **c.** Type **ping** *instructor_ip_address* (where *instructor_ip_address* is the IP address of the instructor computer), and then press ENTER.

Exercise 3
Obtaining an IP Address by Using Automatic Private IP Addressing

Scenario

You need to configure all client computers in a branch office one day before a DHCP server is to be installed. Users in that branch office do not need access to resources outside the office, but they do need to access shared files on each other's computers. You want to make sure that all computers can communicate with each other during the transition.

Goal

In this exercise, you will test Automatic Private IP Addressing.

Tasks	Detailed Steps
Do not begin this procedure until your instructor tells you that the DHCP Server service on the instructor computer has stopped.	
1. Release and then attempt to renew your IP address.	**a.** At the command prompt, type **ipconfig /release** and then press ENTER. **b.** At the command prompt, type **ipconfig /renew** and then press ENTER. *There is a pause while Windows 2000 attempts to locate a DHCP server on the network.*
What message appears and what does it indicate? Would you expect to have an assigned IP address? If so, what would the first two octets of the IP address be? **An error occurred when renewing the local adapter Local Area Connection: DHCP Server unreachable. With DHCP stopped on the Instructor computer you would not expect to have a DHCP assigned IP address. This error message indicates that Automatic Private IP Addressing generated the IP address. The IP address your computer generated would start with the first two octets of 169.254.**	
2. Review and test the TCP/IP configuration.	**a.** At the command prompt, type **ipconfig /all | more** and then press ENTER.

Tasks	Detailed Steps
	Use the information displayed on the screen about your local area connection to complete as much of the following table as possible. Press the SPACEBAR to display additional information, as necessary. **The IP address will be 169.254.*x.y*, with a subnet mask of 255.255.0.0 and no default gateway.** **Setting** **Value** **DHCP Enabled** **Autoconfiguration Enabled** **Autoconfiguration IP Address** **Subnet Mask** **DNS Servers**
	Is this the same IP address that was assigned to your computer in exercise 2? Why or why not? **No, the IP address is not the same as the one that was assigned in exercise 2. In this exercise, the Automatic Private IP Addressing feature of Windows 2000 assigned the IP address because a DHCP server was not available. In exercise 2, the DHCP Server service assigned an IP address.**
2. *(continued)*	**b.** At the command prompt, type **ping** *ip_address* (where *ip_address* is the IP address of your computer), and then press ENTER. **c.** Type **ping** *instructor_ip_address* (where *instructor_ip_address* is the IP address of the instructor computer), and then press ENTER.
	Can you communicate with the instructor computer? Why or why not? **No. The instructor computer is configured with a static IP address in another network, and there is no default gateway configured on your computer.**
	Before continuing, ensure that your partner's computer has an IP address that was assigned by Automatic Private IP Addressing.
2. *(continued)*	**d.** Test TCP/IP connectivity with your partner's computer by typing **ping** *partner_ip_address* (where *partner_ip_address* is the IP address of your partner's computer), and then press ENTER.

(*continued*)

Tasks	Detailed Steps
Make sure to use the IP address that was issued to your partner's computer by Automatic Private IP Addressing, not the address used at the beginning of this lab.	
Can you communicate with your partner's computer? Why or why not? **Yes. Your partner's computer is also configured with an IP address that was assigned by Automatic Private IP Addressing. Because your partner's computer is on the same network, a default gateway is unnecessary.**	
2. *(continued)*	**e.** Minimize the command prompt.

Exercise 4
Configuring TCP/IP to use a Static IP Address

Scenario

Because of some difficulties with the DHCP server, your organization has decided to postpone using a DHCP server to provide IP addresses to all of the client computers on your network. You need all of the client computers on your network to return to the static IP addresses they were originally using.

Goal

In this exercise, you will configure TCP/IP to use a static IP address in order to return your computer to its original configuration. In addition, you will test the configuration to confirm that the configuration is correct and that you can communicate with the instructor computer.

Tasks	Detailed Steps
Before continuing, ensure that your partner has completed exercise 3.	
1. Configure TCP/IP to use a static IP address.	**a.** Restore Network and Dial-up Connections. **b.** Open the **Properties** dialog box for Local Area Connection. **c.** Click **Internet Protocol (TCP/IP)**, verify that the check box to the left of the entry is selected, and then click **Properties**. **d.** Click **Use the following IP address**. **e.** In the **IP address** box, type the value that you recorded in exercise 1, and then press TAB. *The subnet mask setting is automatically entered.*
Be careful when entering IP configuration settings manually, especially numeric addresses. The most frequent cause of TCP/IP connection problems is incorrectly entered IP address information.	
1. (*continued)*	**f.** Verify that **Use the following DNS server addresses** is selected, and then in the **Preferred DNS Server** box, type the value that you recorded in exercise 1. **g.** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box, and then click **OK** to close the **Local Area Connection Properties** dialog box. **h.** Close Network and Dial-up Connections.
2. Test the static TCP/IP configuration.	**a.** Restore the command prompt, type **ipconfig /all | more** and then press ENTER.

(*continued*)

Tasks	Detailed Steps
Use the information about your local area connection that is displayed on the screen to complete as much of the following table as possible. Press the SPACEBAR to display additional information, as necessary. **Answers will vary.** **Setting** — **Value** **DHCP Enabled** **IP Address** **Subnet Mask** **DNS Servers**	
2. (*continued*)	**b.** Type **ping** *ip_address* (where *ip_address* is the IP address of your computer), and then press ENTER. **c.** Type **ping** *instructor_ip_address* (where *instructor_ip_address* is the IP address of the instructor computer), and then press ENTER. **d.** After ensuring that your partner has configured TCP/IP, ping your partner's computer to test TCP/IP connectivity. **e.** Close the command prompt, and then log off.

◆ Connecting to a Novell NetWare Network

Topic Objective
To identify the topics related to connecting to a Novell NetWare network.

Lead-in
Connectivity of a computer running Windows 2000 Advanced Server within a Novell NetWare network involves the implementation of NWLink and Gateway (and Client) Services for NetWare.

- **Connectivity Within a Novell NetWare Network**
- **Installing NWLink**
- **Configuring NWLink**
- **Installing and Configuring Gateway (and Client) Services for NetWare**
- **Connecting to a Shared Resource on a NetWare-based Server**

**********ILLEGAL FOR NON-TRAINER USE**********

In order to connect a computer running Windows 2000 Professional to a Novell NetWare network, you need to install the NWLink protocol and Client Service for NetWare. If you are running Windows 2000 Advanced Server, you need to install the NWLink protocol and Gateway (and Client) Services for NetWare. When you install Client Service for NetWare or Gateway (and Client) Services for NetWare, the NWLink protocol is installed automatically.

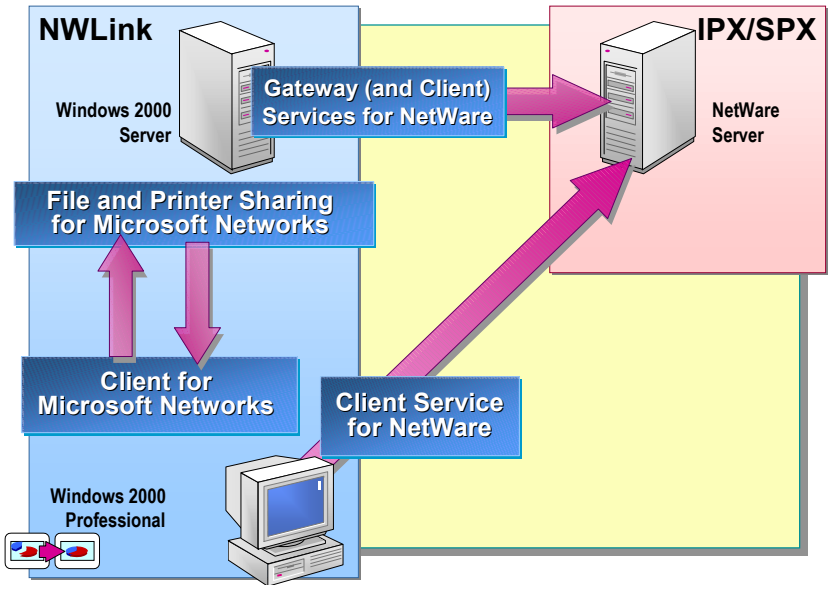
In networking environments that use the Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocol, computers running Windows 2000 and using the NWLink protocol can communicate with other computers or network devices that are using IPX/SPX.

Computers running NWLink can also gain access to applications that are running on network devices that are using IPX/SPX.

Connectivity Within a Novell NetWare Network

Topic Objective
To illustrate the various relationships between Microsoft Windows 2000 and Novell NetWare.

Lead-in
NWLink is the protocol that provides client computers running Windows 2000 access to NetWare-based servers. NWLink is used in conjunction with Client Service for NetWare to provide full connectivity.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

Have the students look at the properties of their **Local Area Connection Properties** dialog box to see that the File and Printer Sharing for Microsoft Networks and the Client for Microsoft Networks features are installed on their computers.

Computers running Windows 2000 can use NWLink, Client Service for NetWare, and Gateway (and Client) Services for NetWare to connect a Novell NetWare-based server using IPX/SPX.

- The NWLink protocol allows computers running Windows 2000 to gain access to applications running on Novell NetWare-based server.
- Client Service for NetWare is the service that allows client computers running Windows 2000 Professional and NWLink to connect to network resources such as file and print resources on a Novell NetWare-based server.
- Gateway Service, a component of Gateway (and Client) Services for NetWare, allows client computers running Windows 2000 to connect to a shared folder on a Novell NetWare-based server by connecting through the Windows 2000-based server running Gateway (and Client) Services for NetWare. As a result, client computers do not need to use Client Service for NetWare.

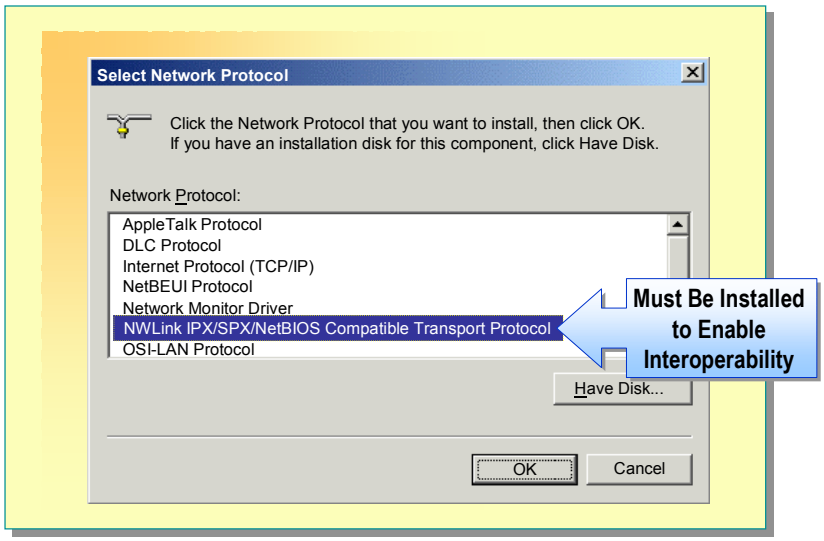
Note For additional information on the requirements for a server running Novell NetWare, see the white paper, *Microsoft Windows 2000 Professional Operating System in a Novell NetWare Environment*, located under **Additional Reading** on the Student Materials compact disc.

Key Points
NWLink is automatically installed when Gateway (and Client) Services for NetWare or Client Service for NetWare is installed.

Installing NWLink

Topic Objective
To illustrate the interface for Installing NWLink.

Lead-in
The procedure for installing NWLink is the same procedure that you use to install any network protocol in Windows 2000.



**********ILLEGAL FOR NON-TRAINER USE**********

You must install the NWLink protocol in order to enable interoperability between a Microsoft Windows 2000-based computer and network devices running IPX/SPX. The procedure for installing NWLink is the same procedure that you use to install any network protocol in Windows 2000.

Delivery Tip
Demonstrate installing NWLink.

Key Point
The procedure to install NWLink is the same as that for installing any network protocol.

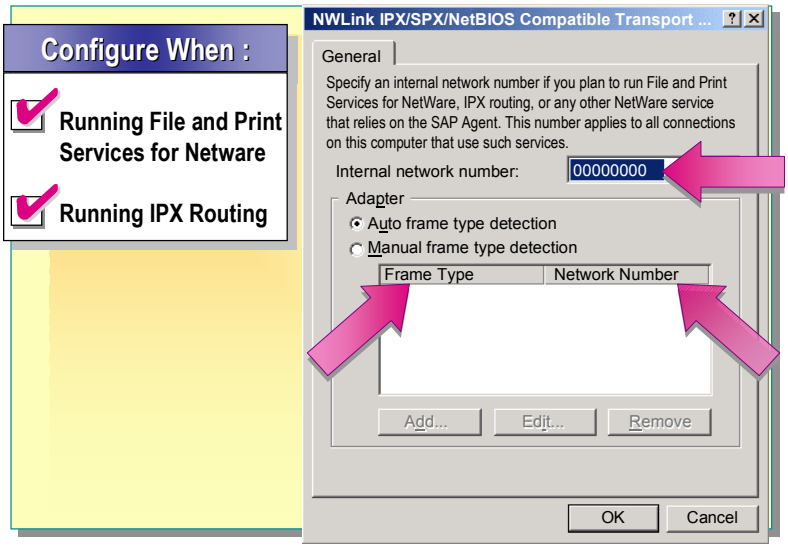
To install NWLink, perform the following steps:

1. Right-click **My Network Places**, and then click **Properties**.
2. In the Network and Dial-up Connections window, right-click the icon that represents the local area connection that you want to configure, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
5. In the **Select Network Protocol** dialog box, in the **Network Protocol** list, click **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, and then click **OK**.
6. In the **Local Area Connection Properties** dialog box, click **Close**.

Configuring NWLink

Topic Objective
To illustrate the interface for configuring NWLink.

Lead-in
Although Windows 2000 automatically detects frame type, network number, and internal network number, there are instances when you may need to configure these settings manually.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
If a network requires it, you can manually configure an internal network number. You can also manually configure the network number and frame type if your network uses more than one network number and frame type.

By default, Windows 2000 automatically detects the frame type and the network number when you install NWLink. If required, you can manually configure the network number, for example, if you are running File and Print Services for NetWare. To configure NWLink manually, you must define three components:

- Network number
- Frame type
- Internal network number

Assigning an Internal Network Number

An internal network number uniquely identifies a server on an IPX internetwork and is similar to the host portion of an IP address in a TCP/IP configuration. This eight-digit hexadecimal number, or virtual network number, is set to 00000000 by default. You must manually assign a unique network number for any of the following situations:

- File and Print Services for NetWare is installed and there are multiple frame types on a single adapter.
- File and Print Services for NetWare is installed and NWLink is bound to multiple adapters in the computer.
- An application is using the NetWare Service Advertising Protocol (SAP). SQL Server and SNA Server are examples of applications that can use SAP.
- An internal network number needs to be unique on the IPX internetwork. If you find it necessary to manually assign a network number for any reason, consult an administrator who administers IPX address assignments in your organization. Incorrectly configuring this information can cause connectivity problems.

Key Point
An administrator configures a frame type and a network number when the network is using two different frame types and network numbers.

Configuring a Frame Type

Windows 2000 supports all of the frame types that are associated with the IPX/SPX protocol. A frame type is the format in which IPX sends packets over a network. A computer only recognizes the IPX frame types for which it is configured. All computers on a network must use the same frame type to communicate or an IPX router must exist that converts frame types.

To ensure proper communication between a computer running Windows 2000 and a NetWare-based server, the NWLink frame type must match the frame type on the NetWare-based server.

When you install NWLink, Windows 2000 automatically determines which frame type is in use on the network and sets the NWLink frame type accordingly. If Windows 2000 detects more than one frame type, NWLink uses the 802.2 frame type by default. Windows 2000 can detect and support the following frame types: Ethernet II, Ethernet 802.3, 802.2, Subnetwork Access Protocol (SNAP), and Attached Resource Computer network (ARCnet). If a second frame type is in use on the network, you must manually configure all required frame types and network numbers.

The process you use to configure the frame type may vary:

- On a computer running Windows 2000, at a command prompt, run the **ipxroute config** command to display the network number, frame type, and devices that are in use. If you need to configure the network number on a particular computer, consult an administrator who administers IPX address assignments in your organization.
- If a computer has multiple network adapters that are bound to NWLink, and if you want each one to use a different frame type, configure each network adapter to use the Manual Frame Type Detection option. You must also specify a frame type, network number, and internal network number for the computer.

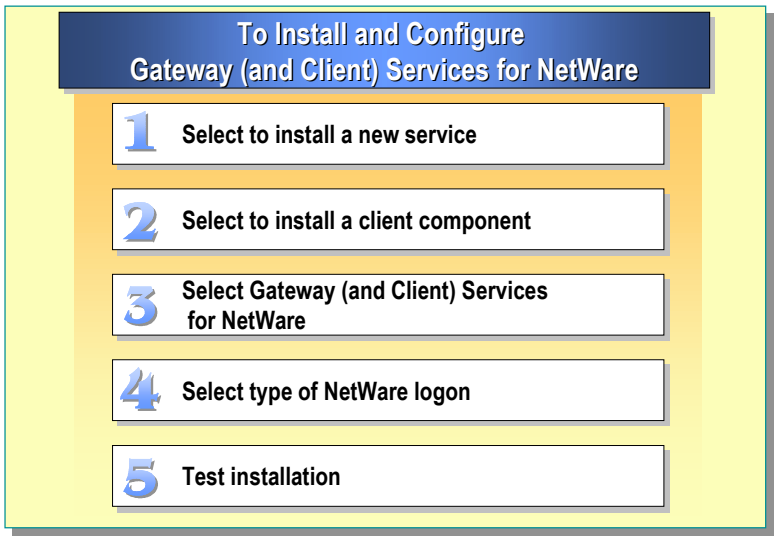
Configuring a Network Number

The network number is similar to the subnet number in TCP/IP configuration. Each frame type that is configured on a network adapter requires a network number that must be unique for each network segment. All computers on a segment that use the same frame type must use the same network number to communicate with one another. If you configure the frame type you must configure the network number.

Installing and Configuring Gateway (and Client) Services for NetWare

Topic Objective
To illustrate the installation of Gateway (and Client) Services for NetWare.

Lead-in
Install Client Service for NetWare to enable computers running Windows 2000 to make direct connections to file and print resources on NetWare-based servers.



**********ILLEGAL FOR NON-TRAINER USE**********

You install and configure Gateway (and Client) Services for NetWare to enable computers running Windows 2000 Advanced Server to make direct connections to file and print resources on NetWare-based servers.

Note NWLink is installed automatically when you install Gateway (and Client) Services for NetWare.

Delivery Tip
Demonstrate this process to students as you describe the procedure.

To install Gateway (and Client) Services for NetWare, perform the following steps:

1. Select to install a new service. To install a new service, perform the following steps:
   a. Double-click **Network and Dial-up Connections** in Control Panel, right-click the appropriate local area connection, and then click **Properties**.
   b. On the **General** tab, click **Install**.
2. In the **Select Network Component Type** dialog box, click **Client**, and then click **Add**.
3. In the **Select Network Client** dialog box, click **Gateway (and Client) Services for NetWare**, and then click **OK**.
4. In the **Select NetWare Logon** dialog box, click **Preferred Server** and then in the **Select Preferred Server** list, select a server from the list of NetWare-based servers. Click **OK**, and then, in the **Local Network** dialog box, click **Yes** to restart your computer.
5. Test that Gateway (and Client) Services for NetWare is initialized properly. To test, carry out the **net view/network:nw** command. You should see a list of available Novell NetWare-based servers.

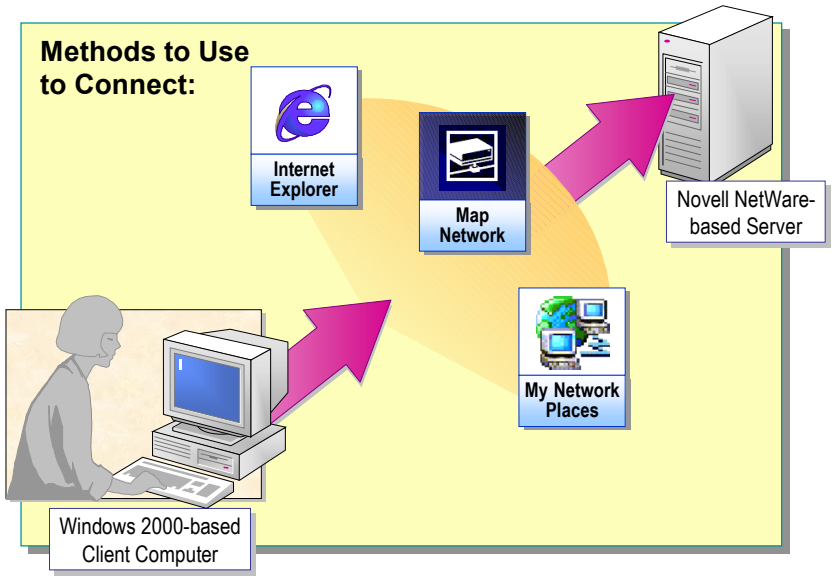
When you install Gateway (and Client) Services for NetWare, it is installed for all connections. If you do not want Client Service for NetWare installed for a certain connection, view the properties of that connection, and then clear the **Client Service for NetWare** check box.

Note You can also gain access to the Gateway (and Client) Services for NetWare dialog box by double-clicking **Gateway (and Client) Services for NetWare** in Control Panel. For more information about Gateway (and Client) Services for NetWare, see the white paper, Microsoft Windows 2000 Professional Operating System in a Novell NetWare Environment, located under **Additional Reading** on the Student Materials compact disc.

Connecting to a Shared Resource on NetWare-based Server

Topic Objective
To illustrate the different methods a user can employ to connect to a Novell NetWare-based server.

Lead-in
You have a variety of ways to connect to a Novell NetWare-based server. However, in all cases you will need three essential pieces of information.



**********ILLEGAL FOR NON-TRAINER USE**********

Mention that although there are more ways to connect to a Windows 2000-based resource, there are still several ways to connect to a NetWare-based resource.

After you install Client Service for Netware and Gateway (and Client) Services for NetWare, users can connect to a NetWare network resource by using some of the same methods they use to connect to a Windows 2000 network resource.

To connect to a NetWare network resource you can:

- Use Internet Explorer. Start Internet Explorer, browse for the network resource, and then connect to it.
- Use Map Network Drive. Right-click **My Computer** or **My Network Places**, and then click **Map Network Drive**. Type the path to the NetWare network resource in the **Path** box.
- Use My Network Places. Open My Network Places, expand the network tree, and then double-click the appropriate NetWare network resource.

Lab B: Installing and Configuring Gateway (and Client) Services for NetWare

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will install and configure Gateway (and Client) Services for NetWare.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install Gateway (and Client) Services for NetWare.
- Access a file located on a NetWare server.
- Configure Gateway (and Client) Services for NetWare.
- Uninstall Gateway (and Client) Services for NetWare.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Windows 2000, Windows NT version 4.0, Windows 98, or Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors.

► **To start the lab**

1. Insert the Student Materials compact disc into your CD-ROM drive.
2. At the root of the compact disc, double-click **Default.htm**.
3. On the Student Materials Web page, click **Lab Simulation**.
4. Click **Installing and Configuring Gateway (and Client) Services for NetWare**.
5. Read the introduction information, and then click the link to start the lab.

Estimated time to complete this lab: 15 minutes

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Windows 2000 Connectivity
- Connecting to a Microsoft Network
- Connecting to a Novell NetWare Network

**********ILLEGAL FOR NON-TRAINER USE**********

1. Your computer has two network adapters and you have installed both the TCP/IP and NWLink protocols. What must you configure if you want NWLink to run on only one adapter?

   Configure the bindings by selecting the adapter that you do not want NWLink to run on and disabling NWLink on that adapter.

2. List the five tasks you must perform to verify and test a TCP/IP configuration.

   1) Ipconfig

   2) Ping 127.0.0.1 (loopback address).

   3) Ping IP address of the local computer.

   4) Ping IP address of the default gateway.

   5) Ping IP address of the remote host.

3. Your computer has TCP/IP installed. You attempt to connect to a computer running Windows 2000 on a remote network using the **Run** command and a universal naming convention (UNC), but you cannot connect. In addition, when you type **ipconfig** the IP address of the local computer displays as 169.254.2.100. Where would you begin troubleshooting?

   First, the IP address 169.254.*x.x* is an automatically assigned IP address. This means the local computer is configured to receive an IP address automatically. This also means that the DHCP server has not leased an IP address. Start by checking the DHCP server. If necessary, you may need to manually assign an IP address to work in the environment.

4. Your computer has NWLink installed and you have just installed Gateway (and Client) Services for NetWare. You can connect to some but not all of the NetWare-based servers on the network. You suspect the frame type is incorrect. What is the default frame type that is automatically detected by Windows 2000? What command can you type to view the frame type?

   The frame type is 802.2

   Type: ipxroute config

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 4: Creating and Managing User Accounts

Contents

Overview	1
Introduction to User Accounts	2
Guidelines for New User Accounts	3
Creating Local User Accounts	7
Lab A: Creating Local User Accounts	9
Creating and Configuring Domain User Accounts	14
Setting Properties for Domain User Accounts	20
Customizing User Settings with User Profiles	29
Lab B: Creating and Modifying Domain User Accounts	33
Best Practices	39
Review	40

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

Labs:
75 Minutes

This module provides students with the skills and knowledge to set up, configure, and administer user accounts in a Microsoft® Windows® 2000 workgroup and in a Windows 2000 domain. This includes creating local and domain user accounts.

At the end of this module, students will be able to:

- Describe the role and purpose of user accounts.
- Identify the guidelines for new user accounts.
- Create local user accounts.
- Create and configure domain user accounts.
- Set properties for domain user accounts.
- Customize user settings with user profiles.
- Identify best practices for creating and configuring user accounts.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_04.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Introduction to User Accounts

  Present the different types of Windows 2000 user accounts. Emphasize the differences between local user accounts and domain user accounts including where the different accounts reside. Mention the two built-in user accounts: Administrator and Guest.

- Guidelines for New User Accounts

  First, present information on naming conventions, including the guidelines to follow when developing the conventions. Emphasize that, for a user logon name, Windows 2000 recognizes only the first 20 characters. Then, present the password guidelines information. Emphasize that if security is important, all users should have complex passwords. Finally, present the important user account options that an administrator can set for new user accounts.

- Creating Local User Accounts

  Present information on creating local user accounts. Demonstrate creating an account. Emphasize that local user accounts reside in the Security Account Manager (SAM) of the computer they are created on and not in the Active Directory™ directory service.

- Creating and Configuring Domain User Accounts

  First, present information on the Windows 2000 Administration Tools package and demonstrate how to install the package. Mention that when it is installed on a client computer or member server, an administrator can manage the network from that computer. Next, present information on creating domain user accounts. Demonstrate the process. Mention that an administrator can only create them on domain controllers. Then, present information on setting the password requirements while demonstrating the process. Emphasize that all user accounts should have passwords to maintain security. Finally, present information on how to use home folders to manage users data. Demonstrate the process.

- Setting Properties for Domain User Accounts

  First, present information on setting personal properties for a user account. Open a user's **Properties** dialog box to show the properties. Emphasize that it is good to provide as many of the values for personal properties as possible, as users can use search Active Directory for these properties. Then, provide more details on the account properties that can be set, including user account expiration. Next, present information on logon options, including logon hours and controlling which computers a user can log on to. Mention that if a user is connected to the network when his or her logon hours are over, the connection is not broken.

  Next, present information on copying domain user accounts. Mention that when an administrator copies an account, the new account does not have the permissions and rights of the original account. Finally, present information on creating user account templates. Emphasize that it is important for the template account to be disabled.

- Customizing User Settings with User Profiles

  Begin by presenting information on the different types of user profiles. Have the students open the **System Properties** dialog box and view the user profiles on the **User Profile** tab. Then, present the procedures for creating roaming user profiles and mandatory roaming user profiles. Mention that to make a user profile mandatory, an administrator changes the .dat extension on the Ntuser file to a .man extension.

- Best Practices

  Present the best practices for creating and configuring user accounts.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server.*

Lab Setup

The labs in this module require that each student computer be configured as a member server in the nwtraders.msft domain. Each computer must also be configured for the classroom environment. To prepare student computers to meet these requirements, perform the following action:

- Complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- The following local accounts are created on the student computer (where *x* is the assigned student number):
  - LocalUser*x*
  - Manager*x*
- The following domain accounts are created in the *Server*OU (where *Server* is the assigned computer name):
  - *Server*T1
  - *Server*T2

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn how to set up and configure user accounts to provide users with access to resources.

- **Introduction to User Accounts**
- **Guidelines for New User Accounts**
- **Creating Local User Accounts**
- **Creating and Configuring Domain User Accounts**
- **Setting Properties for Domain User Accounts**
- **Customizing User Settings with User Profiles**
- **Best Practices**

**********ILLEGAL FOR NON-TRAINER USE**********

As an administrator, you need to provide the users in your organization with access to the various network resources that they require. User accounts enable users to log on and gain access to local or domain resources. In this module, you will learn how to create local and domain user accounts and set properties for them.

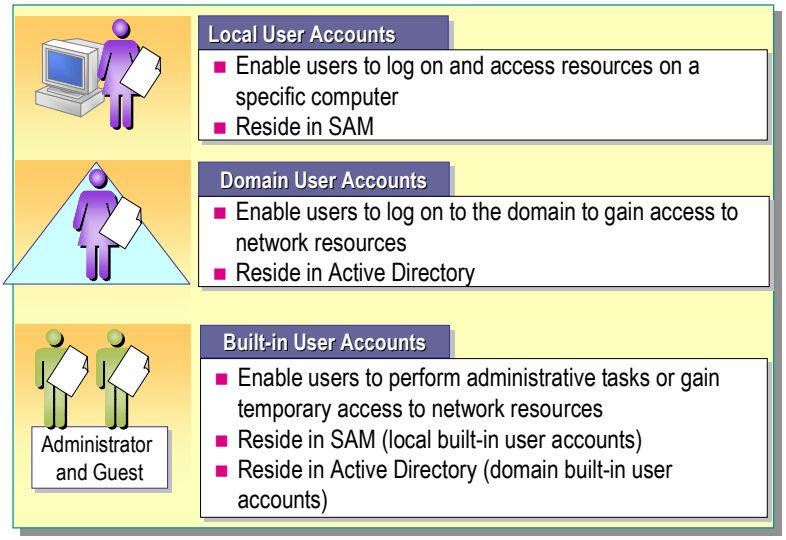
At the end of this module, you will be able to:

- Describe the role and purpose of user accounts.
- Identify the guidelines for new user accounts.
- Create local user accounts.
- Create and configure domain user accounts.
- Set properties for domain user accounts.
- Customize user settings with user profiles.
- Identify best practices for creating and configuring user accounts.

Introduction to User Accounts

Topic Objective
To list the types of user accounts.

Lead-in
The types of user accounts that you can create are domain user accounts and local user accounts. Windows 2000 also provides built-in user accounts to assist with administrative tasks or to allow users to gain temporary access to resources.



**********ILLEGAL FOR NON-TRAINER USE**********

Make sure that students understand the difference between domain user accounts and domain computer accounts.

A *user account* contains a user's unique credentials and enables a user to log on to the domain to gain access to network resources or to log on to a specific computer to access resources on that computer. Each person who regularly uses the network should have a user account.

The following table describes the types of user accounts that Microsoft® Windows® 2000 provides.

Key Point
Local user accounts reside in SAM, which is the local security account database on a computer. Domain user accounts reside in Active Directory.

User account type	Description
Local user account	Enables a user to log on to a specific computer to gain access to resources on that computer. Users can gain access to resources on another computer if they have a separate account on the other computer. These user accounts reside in the Security Accounts Manager (SAM) of the computer.
Domain user account	Enables a user to log on to the domain to gain access to network resources. The user can gain access to network resources from any computer on the network with a single user account and password. These user accounts reside in the Active Directory™ directory service.
Built-in user account	Enables a user to perform administrative tasks or to gain temporary access to network resources. There are two built-in user accounts, which that cannot be deleted: Administrator and Guest. The local Administrator and Guest user accounts reside in SAM and the domain Administrator and Guest user accounts reside in Active Directory. Built-in user accounts are automatically created during Windows 2000 installation and the installation of Active Directory.

Guidelines for New User Accounts

Topic Objective
To list the topics that are relevant to creating new user accounts.

Lead-in
Before you create new user accounts, you need to determine the conventions that have been defined for the network.

- **Naming Conventions**
- **Password Guidelines**
- **Account Options**

**********ILLEGAL FOR NON-TRAINER USE**********

A user account enables a user to log on to computers and domains with an identity that can be authenticated and authorized for access to domain resources.

To make the process of creating user accounts more efficient, you need to familiarize yourself with the conventions and guidelines already in use on the network. Following the conventions and guidelines makes it easier for you to manage the user accounts after they are created.

Naming Conventions

Topic Objective
To list the guidelines for naming user accounts.

Lead-in
One of the important requirements for creating a new user account is to follow an established naming convention.

- **User Logon Names and Full Names Must Be Unique**
- **User Logon Names:**
  - Can contain up to 20 characters
  - Can include a combination of special alphanumeric characters
- **A Naming Convention Should:**
  - Accommodates duplicate employee names
  - Identifies temporary employees

**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Using the **User logon name** option for creating a domain user account, you can enter more than 20 characters, but Windows 2000 recognizes only the first 20 characters.

The naming convention establishes how user accounts are identified in the domain. A consistent naming convention makes it easier to remember user logon names and locate them in lists. It is a good practice to adhere to the naming convention already in use in an existing network that supports a large number of users.

Consider the following guidelines for naming conventions:

- User logon names for domain user accounts must be unique in Active Directory. Domain user account full names must be unique within the domain in which you create the user account. Local user account names must be unique on the computer on which you create the local user account.
- User logon names can contain up to 20 uppercase and lowercase characters (the field accepts more than 20 characters, but Windows 2000 recognizes only 20), except for the following:

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

  You can use a combination of special and alphanumeric characters to help uniquely identify user accounts.
- If you have a large number of users, your naming convention for logon names should accommodate employees with duplicate names. The following are some suggestions for handling duplicate names:
  - Use the first name and the last initial, and then add additional letters from the last name to accommodate duplicate names. For example, for two users named Judy Lew, one user account logon name could be Judyl and the other Judyle.
  - In some organizations, it is useful to identify temporary employees by their user accounts. To do so, you can prefix the user account name with a T and a dash. For example, T-Judyl.

Password Guidelines

Topic Objective
To list the guidelines for assigning passwords to user accounts.

Lead-in
To protect a user account from unauthorized access, you must secure it by assigning a password.

- **Assign a Password for the Administrator Account**
- **Determine Who Has Control over Passwords**
- **Educate Users on How to Use Passwords**
  - Avoid obvious associations, such as a family name
  - Use long passwords
  - Use a combination of uppercase and lowercase characters

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Give an example of a password that is difficult to guess.

To protect access to the domain or a computer, every user account should have a complex password. This helps to prevent unauthorized individuals from logging on to your domain. Consider the following guidelines for assigning passwords to user accounts:

- Always assign a password for the Administrator account to prevent unauthorized access to the account.
- Determine whether you or the users will control passwords. You can assign unique passwords for the user accounts and prevent users from changing them, or you can allow users to enter their own passwords the first time that they log on. In most cases, users should control their own passwords.

Key Point
If security is important, all users should have complex passwords that are difficult to determine.

- Educate users about the importance of using complex passwords that are hard to guess:
  - Avoid using passwords with an obvious association, such as a family member's name.
  - Use long passwords because they are harder to guess. Passwords can be up to 128 characters. A minimum length of eight characters is recommended.
  - Use a combination of uppercase and lowercase letters and non-alphanumeric characters.

Account Options

Topic Objective
To list the important settings to configure on new user accounts.

Lead-in
Before you activate a new user account, you can set restrictions on its usage.

- **Set Logon Hours to Match Users' Work Hours**
- **Specify the Computers from Which a User Can Log On**
  - Domain users can log on at any computer in the domain, by default
  - Domain users can be restricted to specific computers to increase security
- **Specify When a User Account Expires**

**********ILLEGAL FOR NON-TRAINER USE**********

Mention to the students that these are the core account options.

User account options control how a user accesses the domain or a computer. For example, you can limit the hours during which a user can log on to the domain and the computers from which the user can log on. You can also specify when a user account expires. This enables you to maintain the security required by your network.

Logon Hours

You can set logon hours for users who require access only at specific times. For example, you can set logon hours for night shift workers to enable them to log on only during their working hours.

Key Point
By default, a domain user can log on to any computer in the domain. If security is critical, an administrator can restrict the computers to which a user can log on.

Computers from Which Users Can Log On

Users can log on to the domain by using any computer in the domain by default. You can configure account options to specify the computers from which users can log on. For example, you can enable users, such as temporary workers, to log on to the domain only from their computer. This prevents these users from logging in to other computers and gaining access to sensitive information that is stored on other computers.

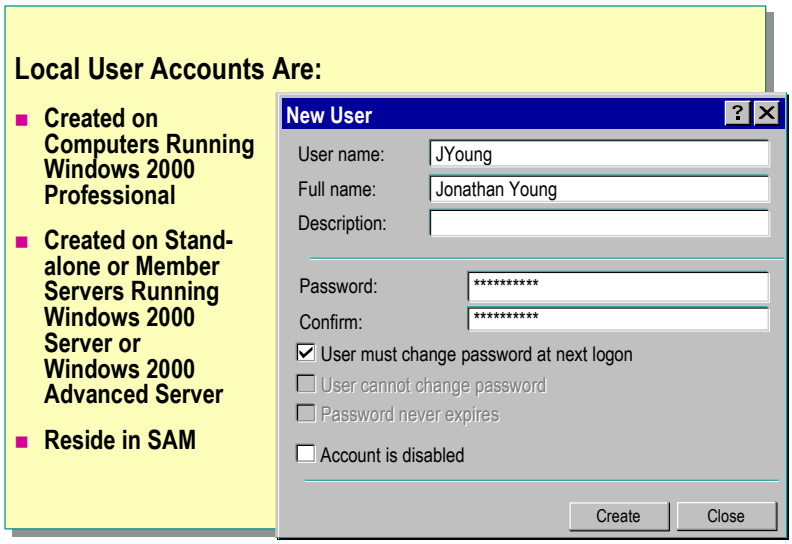
Account Expiration

You can set an expiration date on a user account to ensure that the account is disabled when the user no longer requires access to the network. For example, as a good security practice, you can set user accounts for temporary workers to expire on the date when their contracts end.

Creating Local User Accounts

Topic Objective
To illustrate the user interface for creating a local user account.

Lead-in
Use Computer Management to create a local user account.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the procedure for creating a local user account by using Computer Management and selecting a student's member server as the computer to administer remotely.

Key Points
When you create a local user account, there are fewer options because of reduced functionality.

Local user accounts do not reside in the Active Directory database on the domain controllers, but rather, they reside in the SAM database of the computer. They are available only on the computer on which you create them.

Therefore, it is best to use local user accounts only on computers that are not part of a domain.

Use Computer Management to create a local user account. You can create local user accounts only on computers running Windows 2000 Professional and on stand-alone or member servers running Windows 2000 Server or Windows 2000 Advanced Server.

Characteristics of Local User Account

A local user account is used only in a smaller network environment, such as a workgroup, or on stand-alone computers that are not networked. Do not create local user accounts on computers that are part of a domain because the domain does not recognize local user accounts and as a result, the user account would only be able to gain access to resources that are on the computer.

Local user accounts reside in the SAM database, which is the local security account database of the computer on which you created the account. They are not stored in Active Directory for the domain. In addition, local user accounts have fewer properties than domain accounts.

Creating Local User Accounts

To create a local user account, perform the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Computer Management**.
2. In **Computer Management**, expand **Local Users and Groups**.
3. Right-click the **Users** folder, and then click **New User**.

   The following table describes the user information you provide for a local user account.

Option	Description
User name	The user's unique logon name, based on your naming convention.
Full name	The user's complete name. Use this to determine to which person the local user account belongs.
Description	A description that you can use to identify the user by job title, department, or office location. This field is optional.

4. In the **Password** and **Confirm Password** boxes, type the user's password.
5. Select the appropriate check box or check boxes to set the password restrictions.
6. Click **Create** to create the user account.

When you create a local user account, Windows 2000 does not replicate the local user account information to *domain controllers*. A domain controller is a Windows 2000-based server that is running Active Directory. This is why you cannot use local user accounts to gain access to resources on other computers.

After the local user account is created, the computer uses its SAM to authenticate the local user account, which allows the user to log on to that computer. The user can then gain access to resources that are available only on the local computer.

Lab A: Creating Local User Accounts

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create local user accounts.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objective.

Objective

After completing this lab, you will be able to create local user accounts.

Prerequisites

Before working on this lab, you must have:

- Knowledge about creating local user accounts.
- Experience logging on and off a computer running Microsoft Windows 2000.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server.

Estimated time to complete this lab: 45 minutes

Exercise 1
Creating Local User Accounts

Scenario

You have just installed and configured a computer running Windows 2000 Advanced Server for the Accounts Receivable department. The Accounts Receivable manager needs to be able to log on to the computer. The stand-alone Windows 2000 Advanced Server is going to be shared by two interns. The Accounts Receivable manager will manage it. He will be able to reset passwords and perform other administrative tasks. The manager expects you to be the only administrator of the server. The manager has asked you to create one user account for him and another account named LocalUser.

Goal

In this exercise, you will create two local user accounts. You will create the LocalUser*x* account while you are logged on as Administrator. For the other account, you will be logged on as LocalUser*x*. Because the LocalUser*x* account does not have the right to create local user accounts, you will need to use the **Run as** command to start Computer Management as Administrator, and then create the other account.

Tasks	Detailed Steps
1. Attempt to log on to *Server* (where *Server* is your computer name) as LocalUser*x* (where *x* is your student number) with the password of **password**.	**a.** Attempt to log on using the following information: User name: **LocalUser***x* (where *x* is your student number) Password: **password** Log on to: *Server* (where *Server* is your assigned computer name)
Can a user account that does not exist in the local computers Security Account Manager log on to a local computer? **No. The account must exist in the local computer's Security Account Manager to be authenticated.**	
2. Log on to *Server* (where *server* is your computer name) as Administrator with the password of **password** and create a local user account using the following information: User name: **LocalUser***x* (where *x* is your assigned student number). Password: **password** Description: **My user account**	**a.** Click **OK** to close the message. **b.** Log on using the following information: User name: **Administrator** Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **c.** Open Computer Management from the **Administrative Tools** menu. **d.** In the console tree, under **System Tools**, expand **Local Users and Groups**, and then click **Users**.

Tasks	Detailed Steps
In the list of user accounts, why does the Guest account appear with a red x? **The Guest account on a local computer, as well as on the domain controller, is disabled by default.**	
2. (*continued*)	**e.** Right-click **Users**, and then click **New User**. **f.** Enter the following information in the **New User** dialog box: User name: **LocalUser***x* (where *x* is your assigned student number) Description: **My user account** Password: **password** Confirm password: **password** **g.** Clear the **User must change password at next logon** check box, and then click **Create**. **h.** Click **Close** to close the **New User** dialog box. **i.** Close Computer Management, and then log off.
3. Log on to the LocalUser*x* account you created in task 1. Using the **Run as** command, create the Manager account with the following information: User name: **Manager***x* (where *x* is your assigned student number) Password: **password** Description: **AR Manager**	**a.** Log on using the following information: User name: **LocalUser***x* (where *x* is your assigned student number) Password: **password** Log on to: *Server* (where *Server* is your assigned computer name) **b.** Open Computer Management from the **Administrative Tools** menu. **c.** In the console pane, under **System Tools**, expand **Local Users and Groups**, right-click **Users**, and then click **New User**. **d.** In the **New User** dialog box, in the **User name** box, type **Manager***x* (where *x* is your student number) and then click **Create**. *An access denied message displays in the **Local Users and Groups** dialog box.*
Why does the LocalUser*x* account receive an error message when attempting to create a user account? **The LocalUser*x* account does not have the proper right to create a user account. Only members of the Administrators group or the Account Operators group have the right to create user accounts.**	

Tasks	Detailed Steps
3. (*continued*)	**e.** Click **OK** to close the error message. **f.** Click **Close** to close the **New User** dialog box, and then close Computer Management. **g.** Click **Start**, point to **Programs**, point to **Administrative Tools**, right-click **Computer Management**, and then click **Run as**. **h.** In the **Run As Other User** dialog box, verify that the user name is Administrator and that the domain is *Server*. **i.** In the **Password** box, type **password** and then click **OK**. **j.** In the console tree, under **System Tools**, expand **Local Users and Groups**, right-click **Users**, and then click **New User**. **k.** Enter the following information in the **New User** dialog box: User name: **Manager***x* (where *x* is your student number) Description: **AR Manager** Password: **password** Confirm password: **password** **l.** Clear the **User must change password at next logon** check box, and then click **Create**. **m.** Click **Close** to close the **New User** dialog box, and then close Computer Management.
4. While logged on as LocalUser*x*, test the local account's ability to connect to a domain resource by attempting to access the London domain controller. In the **Enter Network** Password dialog box, type **Admin***x* (where *x* is your assigned student number) with the password of **domain**.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\london** and then click **OK**. *The **Enter Network Password** dialog box appears, which indicates that the local account LocalUser**x** does not have the rights to access the London computer.* **c.** In the **Enter Network Password** dialog box, in the **Connect As** box, type **Admin***x* (where *x* is your assigned student number). **d.** In the **Password** box, type **domain** and then click **OK**.

Why was the LocalUser*x* account not able to connect to the domain controller? Why was the Admin*x* account able to connect to the domain controller?

The LocalUser*x* account is a local account, and therefore can only access resources on the local computer. The Admin*x* account is a domain account, and can therefore access domain resources.

4. (*continued*)	**e.** Close the **London** window, and then log off.
5. Attempt to log on to the domain with the LocalUser*x* account.	**a.** Attempt to log on to the domain using the following information: User name: **LocalUser***x* (where *x* is your assigned student number) Password: **password** Log on to: **nwtraders**

Tasks	Detailed Steps
Why can't the LocalUser*x* account log on to the nwtraders domain? Where does the LocalUser*x* account reside? Where must the account reside to log on to the nwtraders domain? **The LocalUser*x* account is not a domain account, and therefore cannot log on to the nwtraders domain. The LocalUser*x* account resides on the local computer. In order to log on to the nwtraders domain, the account must reside on a domain controller in the domain.**	
5. (*continued*)	**b.** Click **OK** to close the message. **c.** Log on using the following information: User name: **LocalUser*x*** (where *x* is your assigned student number) Password: **password** Log on to: *Server* (where *Server* is your assigned computer name)
Why was the LocalUser*x* account able to log on to the *Server* (where *Server* is your assigned computer name)? **The LocalUser*x* account is a local account and has the right to log on to server.**	
5. (*continued*)	**d.** Log off.

◆ Creating and Configuring Domain User Accounts

Topic Objective
To list the topics related to creating and configuring domain user accounts.

Lead-in
Create domain user accounts on a domain controller.

- **Installing Windows 2000 Administration Tools**
- **Creating a Domain User Account**
- **Setting Password Requirements**
- **Managing User Data by Creating Home Folders**

**********ILLEGAL FOR NON-TRAINER USE**********

Domain user accounts allow users to log on to a domain and gain access to resources anywhere on the network. You create a domain user account on a domain controller.

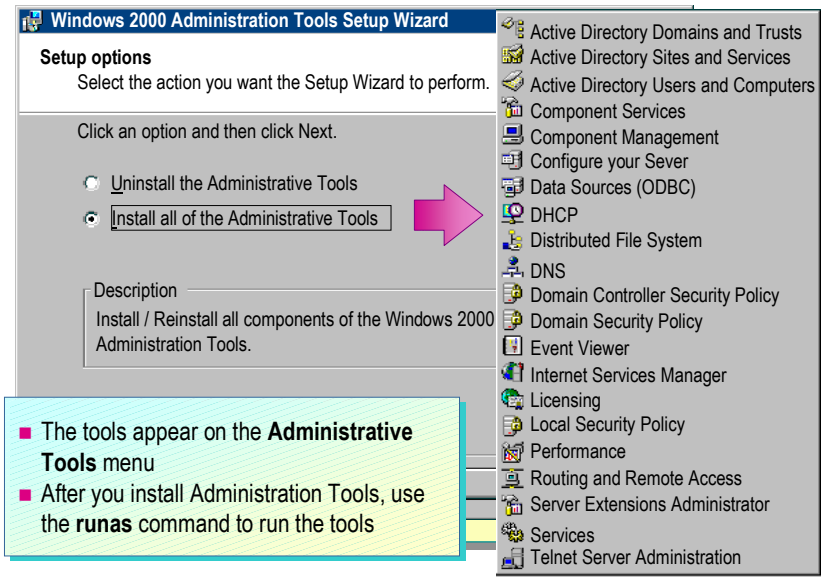
Windows 2000 provides administrative tools to help you create and administer user accounts. Windows 2000 Administration Tools are installed on a domain controller by default. However, you can remotely manage a domain and its user accounts by manually installing the Windows 2000 Administration Tools on a member server or a computer running Windows 2000 Professional.

Use Active Directory Users and Computers to create the domain user account and to configure domain user accounts, such as setting password requirements (whether the users must change their passwords the next time they log on). In addition, you can create a home folder to provide users with a central location in which they can store their data.

Installing Windows 2000 Administration Tools

Topic Objective
To illustrate the user interface for installing Windows 2000 Administration Tools and the tools that are added to the **Administrative Tools** menu during the installation.

Lead-in
You must install Windows 2000 Administration Tools to be able to manage remote servers.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the procedure for installing Windows 2000 Administration Tools. After that, demonstrate using the **runas** command.

Install Windows 2000 Administration Tools to remotely manage domain controller from any computer (client computers and member servers) that is running Windows 2000. Windows 2000 Administration Tools is included on the Windows 2000 Server and Windows 2000 Advanced Server compact discs.

Note You must have administrative rights on the domain controller to manage the domain remotely.

Mention to the students that they should only install Windows 2000 Administration Tools selectively on computers that they are going to use for remote administration because they allow access to domain controllers.

Install Windows 2000 Administration Tools on a computer running Windows 2000 Professional or on a stand-alone or member server running Windows 2000 Server or Windows 2000 Advanced Server. To install Windows 2000 Administration Tools, open the I386 folder on the applicable Windows 2000 Server compact disc, and then double-click **Adminpak.msi**. The Windows 2000 Administration Tools Setup wizard guides you through the process of installing Windows 2000 Administration Tools. After Windows 2000 Administration Tools is installed, you can gain access to the administrative tools by clicking **Start**, pointing to **Programs**, and then pointing to **Administrative Tools**.

Key Point
The **runas** command enables you to use administrative tools with administrative rights and permissions while you are logged on as a normal user.

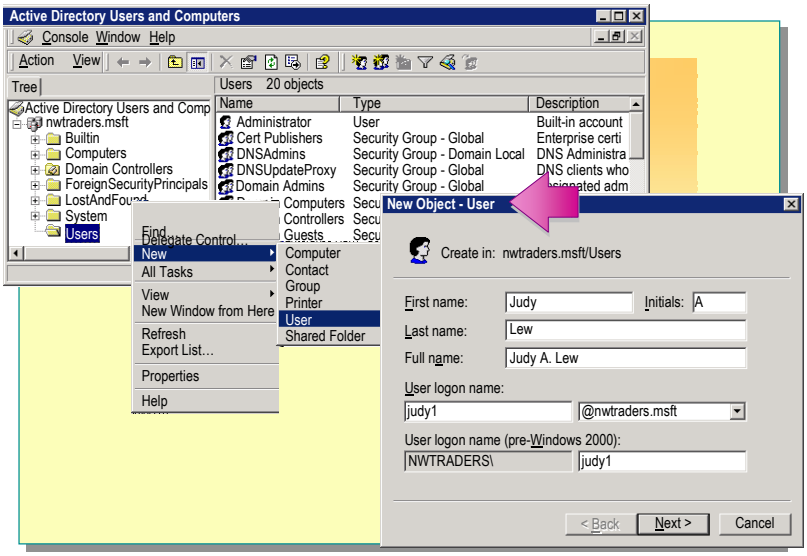
For security purposes, do not log on to the domain with administrative privileges. Instead, log on as a normal user and use the **runas** command when performing administrative tasks. The **runas** command enables you to use administrative tools with administrative rights and permissions while you are logged on as a normal user.

To use the **runas** command, on the **Administrative Tools** menu, hold the SHIFT key, right-click **Active Directory Users and Computers**, and then click **Run as**. In the **Run As Other User** dialog box, verify that **Run the program as the following user** is selected. Type the user name and password for your administrator account, type the domain, and then click **OK**.

Creating a Domain User Account

Topic Objective
To illustrate the user interface for creating a domain user account.

Lead-in
You create a domain user account on a domain controller. The user account is automatically replicated to all other domain controllers.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Point out the various objects in Active Directory, such as users and computers.

Demonstrate how to create a domain user account by using Active Directory Users and Computers.

A domain user account resides on a domain controller and is automatically replicated to all other domain controllers. Create the domain user account in the default Users folder or in a separate folder that you have created to hold domain user accounts. To create a domain user account, perform the following steps:

1. Open Active Directory Users and Computers from the **Administrative Tools** menu, and then expand the domain in which you want to add the user account.
2. Right-click the folder that will contain the user account, point to **New**, and then click **User**.

   The following table describes the options that you can configure.

Option	Description
First name	The user's first name.
Initials	The user's middle initials. This is not a required entry.
Last name	The user's last name.
Full name	The user's complete name. This name must be unique within the folder in which you create the account. Windows 2000 completes this option if you enter information in the **First name** or **Last name** box, and then displays this name in the folder where the user account is located in Active Directory.
User logon name	The user's unique logon name, based on the naming conventions. This is required and must be unique within Active Directory.
User logon name (pre-Windows 2000)	The user's unique logon name that is used to log on from previous versions of Microsoft Windows. This is a required entry and must be unique within the domain.

Setting Password Requirements

Topic Objective
To illustrate the user interface for setting password requirements for a domain user account.

Lead-in
After entering the account name information, click **Next** to set the password requirements for the domain user account.

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to set the password requirements for a domain user account.

The following table describes the password requirements that you can configure when you assign a password to a domain user account.

Option	Description
Password	Provide the password that is used to authenticate the user. For greater security, you should *always* assign a password. The password is not visible when you type it. Instead, it is represented as a series of asterisks (*).
Confirm password	Confirm the password by typing it a second time to ensure that it has been entered correctly. This is a required entry.
User must change password at next logon	Select this check box if you want the user to change his or her password the first time that he or she logs on. This ensures that the user is the only person who knows the password.
User cannot change password	Select this check box if you have more than one person using the same domain user account (such as Guest) or to maintain control over user account passwords. This allows only administrators to control passwords.
Password never expires	Select this check box if you never want the password to change—for example, for a domain user account that will be used by an application or a service in Windows 2000.
Account is disabled	Select this check box to prevent use of this user account—for example, for a new employee who has not yet started.

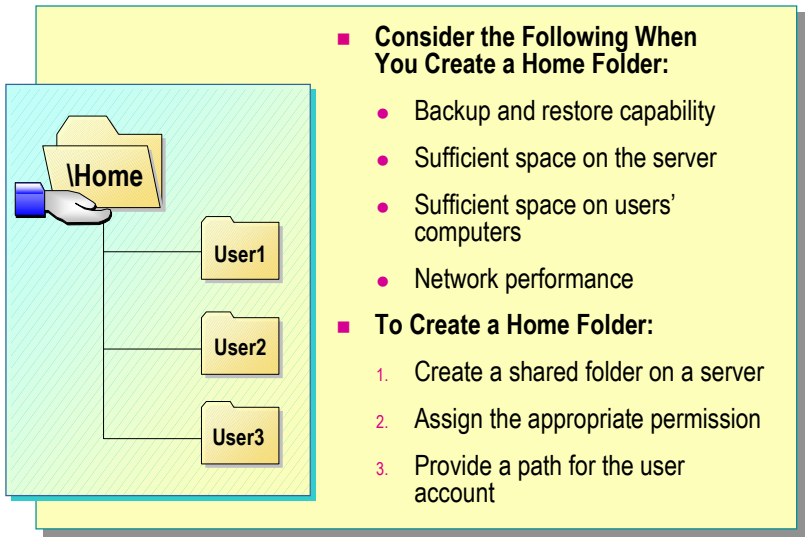
Key Point
Always assign passwords to user accounts and require users to change them the first time that they log on.

Note The **User must change password at next logon** option overrides the **Password never expires** option.

Managing User Data by Creating Home Folders

Topic Objective
To list the characteristics of home folders when they are stored on a server or on a user's computer and how to create a home folder.

Lead-in
Home folders provide a central location in which users can store their documents.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate setting up a home folder for one of your students on the Instructor computer.

You can provide a centralized network location for users to store their documents. This additional location is the user's home folder. Home folders are not part of a user profile, so they do not affect the logon process. You can locate all users' home folders in a central location on a network server.

Consider the following points when determining the home folder location:

- Back up and restore capability

  Preventing the loss of data is your primary responsibility. It is much easier to ensure that 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 will need to perform regular backups on each computer.

- Sufficient space on the server

  It is important that there is enough room on the server to allow users to store their data. Windows 2000 provides more precise control of network-based storage with disk quotas, which enable you to monitor and limit the amount of hard disk space used by each user.

- Sufficient space on users' computers

  If users are working on computers with very little disk space or no hard disks, home folders should be located on a network server.

- Network Performance

  There is less network traffic if the home folder is located on the user's local computer.

To create a home folder, perform the following tasks:

1. Create and share a folder on a server.
2. Grant the appropriate permission for the folder.
3. Provide a path for the user account to the folder.

Setting Properties for Domain User Accounts

Topic Objective
To list the options for setting properties for domain user accounts.

Lead-in
After you have created a user account, you may need to make changes to the default properties for the domain user account.

**********ILLEGAL FOR NON-TRAINER USE**********

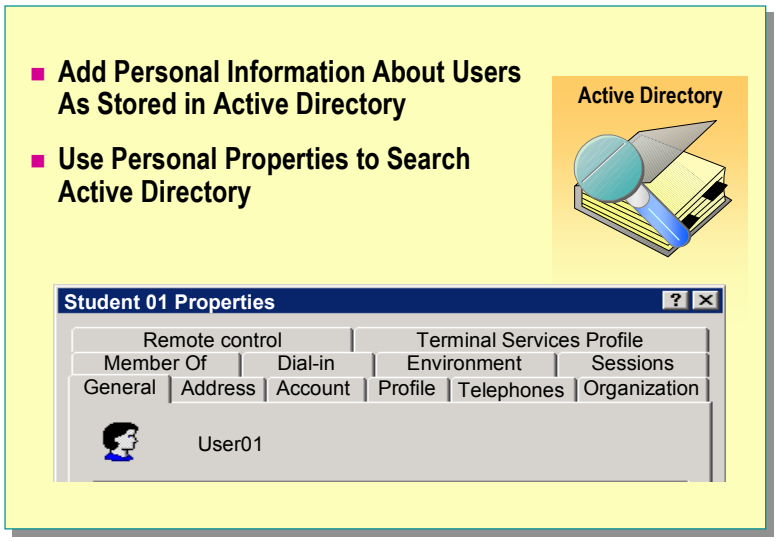
A set of default properties is associated with each domain user account that you create. After you create a domain user account, you can configure personal and account properties, logon options, and dial-up settings.

You can use the properties that you define for a domain user account to search for users in Active Directory. For example, you can search for a person by a telephone number, office location, manager's name, or last name. For this reason, you should provide detailed property definitions for each domain user account that you create.

Setting Personal Properties

Topic Objective
To illustrate the tabs that are available for setting personal property options.

Lead-in
You need to complete as many of the personal property options as possible to facilitate locating user accounts in Active Directory.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tips
Demonstrate opening the **Properties** dialog box by using Active Directory Users and Computers.

Do not spend a lot of time demonstrating how to enter the properties in this dialog box. Ask students how they would use the different properties in their organizations and how the properties would benefit them.

The **Properties** dialog box contains information about each user account. This information is stored in Active Directory. The more complete the information, the easier it is to search for users in Active Directory. For example, if all of the properties on the **Address** tab are complete, you can locate the user by using the street address as the search criteria.

To set personal properties, perform the following steps:

1. Open Active Directory Users and Computers from the **Administrative Tools** menu, select the domain, and then click the appropriate folder to view available domain user accounts.
2. Right-click the appropriate domain user account, and then click **Properties**.
3. On the **Properties** dialog box, choose the appropriate tab for the personal properties that you want to enter or change, and then enter values for each property.

Key Point
An administrator needs to provide as many of the values for personal properties as possible so that users and administrators can search Active Directory on these properties to easily locate user accounts. For example, if a postal number is provided, users can search for other users who live in a particular geographic location.

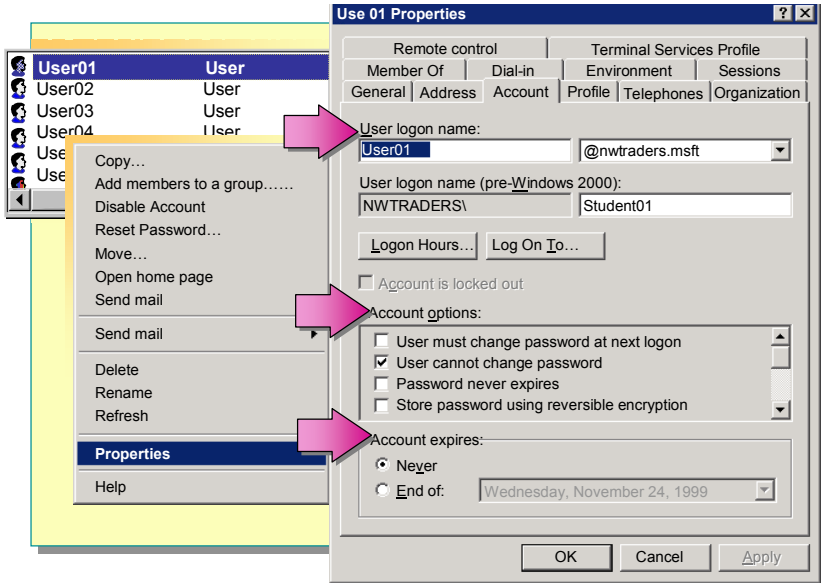
The following table describes the tabs in the user **Properties** dialog box.

Tab	Purpose
General	Documents the user's name, description, office location, telephone number, e-mail alias, and home page information.
Address	Documents the user's street address, post office box, city, state or province, postal zip code, and country.
Account	Assigns the user's logon name, set account options, and specify account expiration.
Profile	Assigns the user's profile path and home folder.
Telephones	Documents the user's home, pager, mobile, fax, and Internet Protocol (IP) telephone numbers, and allows you to type notes that contain descriptive information about the user.
Organization	Documents the user's title, department, company manager, and direct reports.
Member Of	Specifies the groups to which the user belongs.
Dial-in	Sets remote access permissions, callback options, and static IP address and routes.
Environment	Specifies one or more applications to start up and the devices to connect to when the user logs on.
Sessions	Specifies Terminal Services settings.
Remote control	Specifies Terminal Services remote control settings.
Terminal Services Profile	Sets the user's Terminal Services profile.

Setting Account Properties

Topic Objective
To illustrate the user interface for setting account properties for domain user accounts.

Lead-in
Let's look in greater detail what you can do on the **Account** tab. You can set account properties for domain user accounts.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to set properties for domain user accounts.

Point out the domain user account options that are the same for the **Account** tab and the **Create New Object – (User)** dialog box.

Key Point
On the **Account** tab, an administrator can set an expiration date for a user account.

On the **Account** tab of the **Properties** dialog box, you can configure settings that were specified when you created a domain user account, such as the user logon name and logon options. You can modify the password requirements by clearing or selecting the appropriate check box under **Account options**.

In addition, you can use the **Account** tab to set an expiration date for a user account. This is the date on which Windows 2000 will automatically disable the user account. By default, a user account never expires.

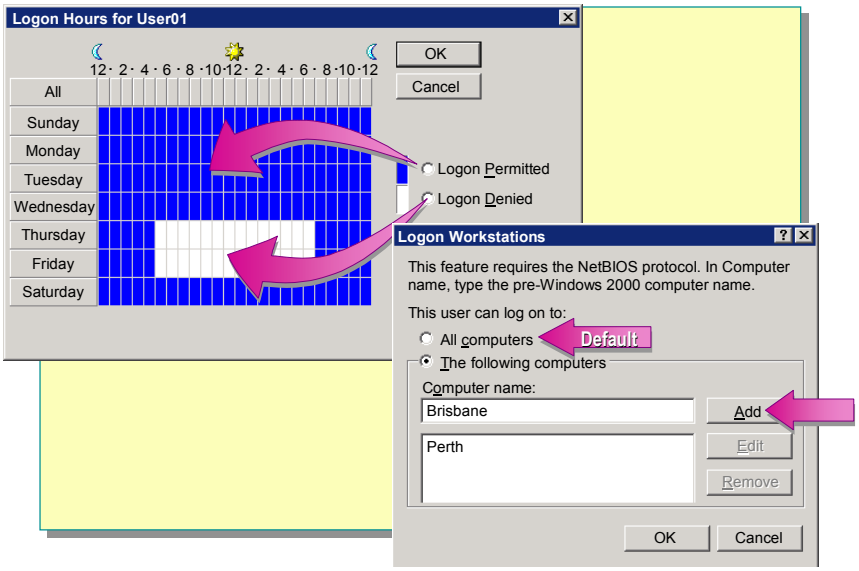
To set an account expiration date, perform the following steps:

1. Open the **Properties** dialog box for the appropriate user account.
2. On the **Account** tab, under **Account Expires**, click **End of**. Select an expiration date from the list, and then click **OK**.

Specifying Logon Options

Topic Objective
To illustrate the user interface for restricting logon hours and logon workstations for a domain user account.

Lead-in
Another task you can perform on the **Account** tab, is controlling the hours during which a user can log on to the domain by setting logon hours. You can also control the computers from which a user can log on to the domain by setting logon workstations.



**********ILLEGAL FOR NON-TRAINER USE**********

Setting logon options for a domain user account allows you to control the hours during which a user can log on to the domain, in addition to the computers from which a user can log on to the domain. These are settings you gain access to from the **Account** tab.

Setting Logon Hours

Delivery Tip
Demonstrate how to change logon hours for a domain user account.

By default, users can connect to a server 24 hours a day, 7 days a week. In a high-security network, you may want to 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. You can enable night shift workers to log on only during their working hours.

Key Point
Connections to network resources on the domain are not disconnected when the user's logon hours expire. However, the user will not be able to make any new connections.

To set logon hours, perform the following steps:

1. Open the **Properties** dialog box for the user account. On the **Account** tab, click **Logon Hours**.

   A blue box indicates that the user can log on during the hour. A white box indicates that the user cannot log on.

2. To allow or deny access, do one of the following, and then click **OK**:

   - Select the boxes on the days and hours that you want to *deny* access by clicking the start time, dragging to the end time, and then clicking **Logon Denied**.
   - Select the rectangles on the days and hours that you want to *allow* access by clicking the start time, dragging to the end time, and then clicking **Logon Permitted**.

Important Connections to network resources on the domain are not terminated when the user's logon hours expire. However, the user will not be able to make new connections to other computers in the domain.

Setting the Computers from Which Users Can Log On

Key Point
You can specify the computers from which a user can log on. You cannot specify the computers from which a user cannot log on.

By default, any user with a valid account can log on to the network from any computer running Windows 2000. In a high-security network where sensitive data is stored on the local computer, restrict the computers from which users can log on to the network. For example, User1 can only log on from the computer named Computer1. You cannot specify the computer from which a user cannot log on.

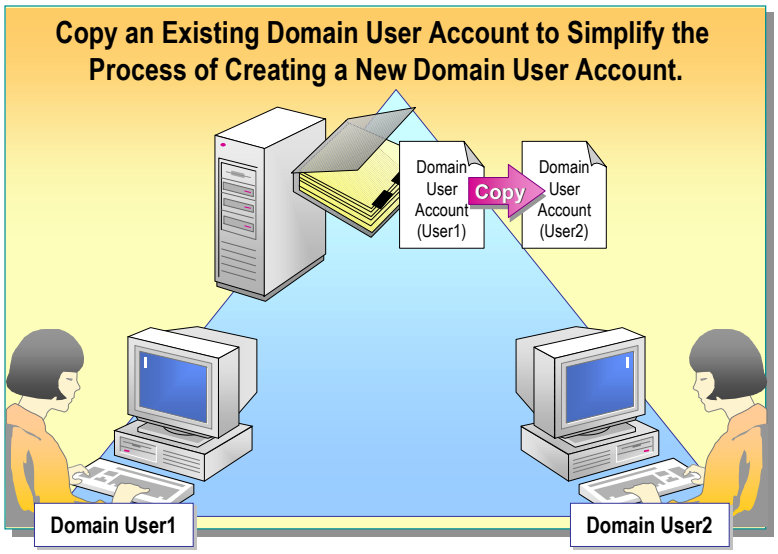
To specify the computers from which a user can log on, perform the following steps:

1. Open the **Properties** dialog box for the user account, and then, on the **Account** tab, click **Log On To**.
2. Click **The following computers**. Add the computers from which a user can log on by typing the name of the computer in the **Computer name** box, and then click **Add**. When you are finished adding computers, click **OK**.

Copying Domain User Accounts

Topic Objective
To illustrate the concept of copying a domain user account.

Lead-in
You can simplify the process of creating domain user accounts by copying an existing user account.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Copying domain user accounts to create a new domain user account eliminates the need to configure all the properties for the new domain user account.

You can copy an existing domain user account to simplify the process of creating a new domain user account. When you copy an existing user account, many of the account properties are copied to the new user account. This eliminates the need to configure all of the properties for the new user account.

Note You cannot copy user accounts on a computer that is running Windows 2000 Professional or on a Windows 2000 member server. You can only copy user accounts on a domain controller.

Properties Copied to the New User Account

The user properties are copied from the existing domain user account to the new domain user account as described in the following table.

Tab	Properties copied to new domain user account
General	None.
Address	All, except **Street Address**.
Account	All, except **Logon Name**, which is copied from the **Copy Object – User** dialog box.
Profile	All, except the **Profile path** and **Home folder** entries, which are modified to reflect the new user's logon name.
Telephones	None.
Organization	All, except **Title**.
Member Of	All.

(continued)

Tab	Properties copied to new domain user account
Dial-in	None. Default settings apply to new user account.
Environment	None. Default settings apply to new user account.
Sessions	None. Default settings apply to new user account.
Remote control	None. Default settings apply to new user account.
Terminal Services Profile	None. Default settings apply to new user account.

Key Point
The rights and permissions of an individual user account do not copy to the new user account.

Important Rights and permissions that are granted to an individual user account are not copied to the new user account.

Copying an Existing User Account

To create a new user account by copying an existing user account, perform the following steps:

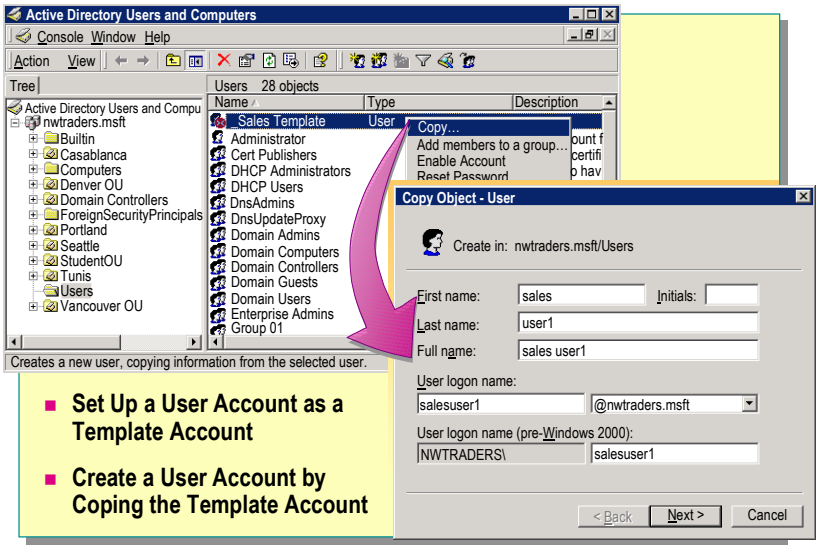
Delivery Tip
Demonstrate the procedure for copying a domain user account.

1. Open **Active Directory Users and Computers**, and then click the **Users** folder in the console tree.
2. In the details pane, right-click the user account that you want to copy, and then click **Copy**.
3. In the **Copy Object - User** dialog box, type the user name and user logon name information for the new user account, and then click **Next**.
4. Type and confirm the password, set the password requirements (clear the **Account is disabled** check box, if appropriate), and then click **Next**.
5. Verify that the new user account information is correct, and then click **Finish**.

Creating User Account Templates

Topic Objective
To illustrate the user interface for creating and copying a user account template.

Lead-in
You can create templates to further simplify the process of creating new user accounts for users who will have common account properties.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate creating a template.

A user account template is a standard user account that you can create to contain the properties that apply to users with common needs. For example, if all sales personnel require membership in the Sales group, you can create a template that includes membership to that group.

Key Point
It is important that the template user account you create is disabled. It is never to be used to log on to the domain.

Creating a User Account Template

To create a template, create a new domain user account, or copy an existing domain user account. Assign a unique account name, and remember to select the **Account is disabled** check box when setting the password requirements.

Guidelines to consider when creating templates are:

- 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.

Tip If you begin each template name with a nonalphabetic character, such as the underscore character (_), the template will always appear at the top of the list in the details pane of the Active Directory Users and Computers window.

Creating a New User Account by Using a Template

To use a template to create a new user account, copy the template account, assign a user name and password for the new user, and change the user account properties as necessary. Remember to clear the **Account is disabled** check box.

Customizing User Settings with User Profiles

Topic Objective
To list the topics related to customizing user settings with user profiles.

Lead-in
User profiles define a user's work environment.

- **User Profile Types**
- **Creating Roaming and Mandatory Roaming User Profiles**

**********ILLEGAL FOR NON-TRAINER USE**********

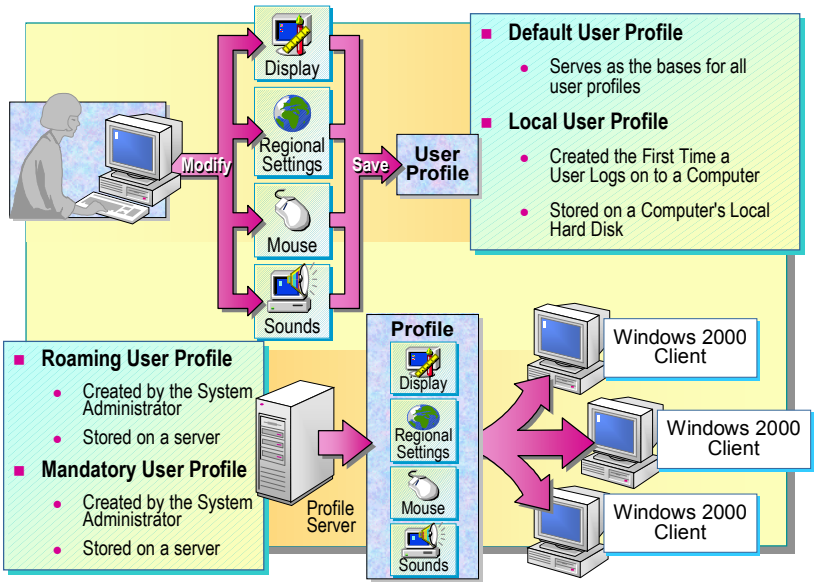
In Windows 2000, a user's computing environment is determined primarily by the user profile. For security purposes, Windows 2000 requires a user profile for each user account that has access to the system.

The user profile contains all of the settings that the user can define for the work environment of a computer running Windows 2000, including display, regional, mouse, and sounds settings, in addition to network and printer connections. You can set up user profiles so that a profile follows a user to each computer that the user logs on to.

User Profile Types

Topic Objective
To list the different types of user profiles.

Lead-in
Windows 2000 creates a user profile the first time a user logs on to a computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Have the students open the **System Properties** dialog box and view the user profiles on the **User Profile** tab. To open the **System Proprieties** dialog box, in Control Panel double-click the **System** icon.

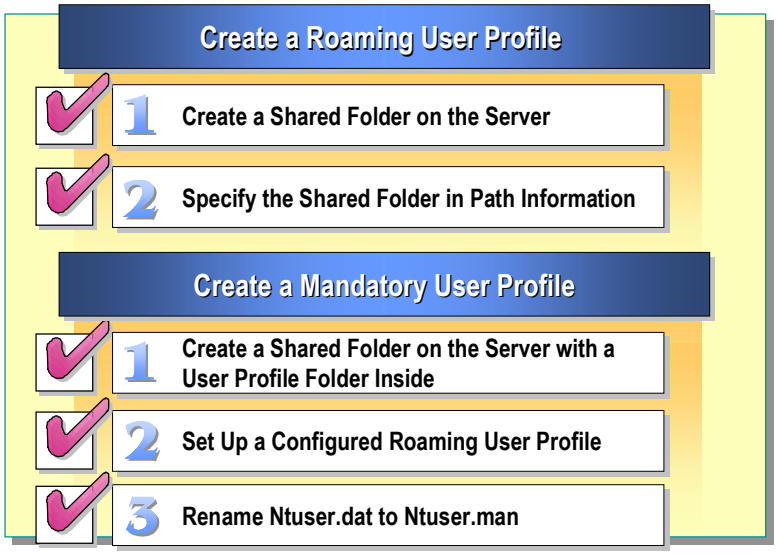
A user profile is created when a user logs on to a computer for the first time. All user-specific settings are automatically saved in the user's folder within the Documents and Settings folder (C:\Documents and Settings*User name*). When the user logs off, the user's profile is updated on the computer at which the user was logged on. Thus, the user profile maintains the desktop settings for each user's work environment on the local computer. Only system administrators can make changes to mandatory user profiles. Types of user profiles include:

- *Default user profile*. Serves as the basis for all user profiles. Every user profile begins as a copy of the default user profile, which is stored on each computer running Windows 2000 Professional or Windows 2000 Server.
- *Local user profile*. Created the first time a user logs on to a computer and is stored on the local computer. Any changes made to the local user profile are specific to the computer on which the changes were made. Multiple local user profiles can exist on one computer.
- *Roaming user profile*. Created by the system administrator and stored on a server. This profile is available every time a user logs on to any computer on the network. If a user makes changes to his or her desktop settings, the user profile is updated on the server when the user logs off.
- *Mandatory user profile*. Created by the administrator to specify particular settings for a user or users and it can be local or roaming. A mandatory user profile does not enable users to save any changes to their desktop settings. Users can modify the desktop settings of the computer while they are logged on, but these changes are not saved when they log off.

Creating Roaming and Mandatory Roaming User Profiles

Topic Objective
To illustrate the concept of roaming and mandatory user profiles.

Lead-in
Roaming and mandatory user profiles are stored on a server in order to provide users with the same working environment on any computer.



**********ILLEGAL FOR NON-TRAINER USE**********

You can store user profiles on a server so that they are available every time a user logs on to any computer on the network. Roaming and mandatory user profiles are stored centrally on a server in order to provide users with the same working environment regardless of which computer they log on to.

Delivery Tip
Demonstrate creating a roaming user profile.

Creating a Roaming User Profile

To set up a roaming user profile, perform the following tasks:

1. Create a shared folder on a server and provide users with the Full Control permission to the folder.
2. Provide the path to the shared folder. Open Active Directory Users and Computers. In the details pane, right-click the applicable user account, and then click **Properties**. On the **Profile** tab, under **User profile**, type the path information to specify the shared folder in the **Profile path** box.

   The path information should appear as follows:

   \\server_name\shared_folder_name\user_name

   You can use the variable **%user_name%** instead of typing in the user name. Windows 2000 automatically replaces %user_name% with the user account name for the roaming user profile.

Key Point
Only an administrator can modify a roaming user profile.

After a roaming user profile is created, only an administrator can modify it.

Note The Ntuser.dat file contains the section of the registry that applies to the user account and contains the user profile settings. This file is located in the user's profile folder.

Creating a Mandatory Roaming User Profile

Delivery Tip
Demonstrate the procedure for creating a mandatory user profile. After the profile is created, point out the .man extension to the students.

Typically you use a mandatory profile when a group of users needs the same desktop settings and you do not want them to modify their desktops.

To create a mandatory roaming user profile, perform the following tasks:

1. Create a shared folder on a server with a profile folder for the user profile you will create inside. Provide users with the Full Control permission to the profile folder. For example, create a folder called Profiles, and then create a folder called User1 in the Profiles folder.
2. Set up a configured roaming user profile. In Active Directory Users and Computers, create a new user, specify the user's profile folder for the path information, and then configure the profile.

   For example, create a user called User1 and specify the profile path of *server_name*\Profiles\User1. To configure the profile, log on to the domain as User1, modify the desktop settings as necessary, and then log off.

Key Point
To make a user profile mandatory, an administrator changes the .dat extension on Ntuser to .man.

3. Rename the profile file Ntuser.dat to Ntuser.man. This makes the profile read-only and therefore mandatory. To rename the profile, log on as Administrator, open Windows Explorer, and, in the user's profile folder, rename the Ntuser.dat file to Ntuser.man.

Note The Ntuser.dat file in the user's profile folder will be hidden. To view the file in Windows Explorer, click **Tools**, and then click **Folder Options**. On the **View** tab of the **Folder Options** dialog box, under **Advanced settings**, click **Show hidden files and folders**. Clear the **Hide file extensions for known file types** check box, and then click **OK**.

Lab B: Creating and Modifying Domain User Accounts

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create and then modify a domain user account.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create domain user accounts.
- Modify domain user accounts.

Prerequisites

Before working on this lab, you must have:

- Knowledge about creating domain user accounts.
- Knowledge about modifying domain user accounts.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- An account named Admin*x* (where *x* is your assigned student number) with administrative rights for the Student*x* OU.
- An organizational unit named *Server*OU (where *Server* is your assigned computer name).
- A partner with a similarly configured computer to test the account properties.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating Domain User Accounts

Scenario

Two new temporary employees need to be added to your corporate network. The hours for the accounts must be restricted as follows: Temp1 will work Monday through Saturday, 6 A.M. to 6 P.M., and Temp2 will work Monday through Saturday, 1 P.M. to 6 P.M. Both users should be provided with logon rights to specific computers only. The desktop settings and home directory for each account will be located on the domain controller. You have decided to create these accounts as domain user accounts. You need to create these accounts as soon as possible but you are sitting at a member server rather than a domain controller. To complete this task, you must install Windows 2000 Administration Tools from the Windows 2000 Advanced Server compact disc.

Goal

In this exercise, you will install Windows 2000 Administration Tools, create two domain user accounts (Temp1 and Temp2), and then configure the following account options:

- Log on hours
- Computers to log on to
- Profile folder
- Home folder

You will then verify the configured account options on *Server*T1 and *Server*T2 and verify them.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with a password of **domain**. Install the Windows 2000 Administrative Tools from the Windows 2000 Advanced Server compact disc.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Verify that the Windows 2000 Advanced Server compact disc is in the CD-ROM drive. **c.** Click **Start**, and then click **Run**. **d.** In the **Open** box, type *CD-ROM***:\I386\adminpak.msi** (where *CD-ROM* is the drive letter of your CD-ROM drive), and then click **OK**. **e.** On the **Welcome to the Windows 2000 Administration Tools Setup Wizard** page, click **Next**. *An indicator appears showing the progress of the Windows 2000 Administration Tools installation.* **f.** On the **Completing Windows 2000 Administration Tools Setup Wizard** page, click **Finish**.

Tasks	Detailed Steps
On what computers in the domain would you install Windows 2000 Administrative Tools and why? **Only on those computers that are not domain controllers and that would be used to manage the domain.**	
2. In Active Directory Users and Groups, in *Server*OU (where *Server* is your assigned computer name), create account the Temp1 user account with the logon name of *Server*T1and a password of **password**. Create the Temp2 user account with the logon name of S*erver*T2 and a password of **password**.	**a.** Open Active Directory Users and Computers from the **Administrative Tools** menu. **b.** In the console tree, expand **nwtraders.msft**, and then click *Server* **OU** (where *Server* is your assigned computer name). **c.** Right-click *Server* **OU**, point to **New**, and then click **User**. **d.** Use the following information to complete the **New Object – User** dialog box: First name: **Temp1** User Logon name: *Server***T1** (where *Server* is your assigned computer name) **e.** Click **Next**. **f.** In the **Password** and **Confirm password** boxes, type **password** **g.** Select the **User cannot change password** check box, and then click **Next**. **h.** Review the configuration settings for the Temp1 user account, and then click **Finish**. **i.** Right-click *Server* **OU**, point to **New**, and then click **User**. **j.** Use the following information to complete the **New Object – User** dialog box: First name: **Temp2** User Logon name: *Server***T2** (where *Server* is your assigned computer name) **k.** Click **Next**. **l.** In the **Password** and **Confirm password** boxes, type **password** **m.** Select the **User cannot change password** check box, and then click **Next**. **n.** Review the configuration settings for the Temp2 user account, and then click **Finish**.

Tasks	Detailed Steps
3. Using Active Directory Users and Groups, set the following properties on Temp1: • Logon Hours: Monday through Saturday, 6 A.M. to 9 P.M. • Log On To: *Server* (where *Server* is the name of your computer) and *Partner's Server* (where *Partner's Server* is your partner's assigned computer name) • Account Expires: First Friday from the current date • Profile Path: \\London\Profiles\%username% • Home Folder: H:\\London\Home\%username%	**a.** In Active Directory Users and Computers, in the details pane, double-click **Temp1**. **b.** In the **Temp1 Properties** dialog box, on the **Account** tab, click **Logon Hours**. **c.** In the **Logon Hours for Temp1** dialog box, in the upper-left corner, click **All**, and then click **Logon Denied**. **d.** Drag the cursor on the logon hours so that the description under the calendar displays **Monday through Saturday from 6AM to 9PM**, click **Logon Permitted**, and then click **OK**. **e.** On the **Account** tab, click **Log On To**. **f.** Click **The following computers**, in the **Computer name** box, type *Server* (where *Server* is your assigned computer name), and then click **Add**. **g.** In the **Computer name** box, type *Partner's Server* (where *Partner's Server* is your partner's assigned computer name), click **Add**, and then **OK**. **h.** On the **Account** tab, under **Account expires**, click **End of**, and then select the first Friday from the current date. **i.** On the **Profile** tab, in the **Profile path** box, type **\\london\profiles\%username%**

Where is the shared folder Profiles located? What is the purpose of %username% in the path statement?

The Profiles shared folder is located on the London computer. The %username% entry in the path statement will create a folder under the Profiles shared folder using the logon name of the account.

3. (*continued*)	**j.** Under **Home folder**, click **Connect**, and then click **H:**. **k.** In the **To** box, type **\\london\home\%username%** and then click **OK**.

Tasks	Detailed Steps
4. Using Active Directory Users and Groups, set the following properties on Temp2: • Logon Hours: Monday through Saturday, 12 A.M. to 6 A.M., and Monday through Saturday, 9 P.M. to 12 A.M. • Log On To: Computer55 • Account Expires: First Friday from the current date • Profile Path: \\London\Profiles\%username% • Home Folder: H: \\London\Home\%username%	**a.** In Active Directory Users and Computers, in the details pane, double-click **Temp2**. **b.** In the **Temp2 Properties** dialog box, on the **Account** tab, click **Logon Hours**. **c.** In the **Logon Hours for Temp2** dialog box, click **All**, and then click **Logon Denied**. **d.** Drag the curser on the logon hours so that the description under the calendar displays **Monday through Saturday 12AM to 6AM**, and then click **Logon Permitted**. **e.** Again, drag the cursor on the logon hours so that the description under the calendar displays **Monday through Saturday from 9PM to 12AM**, click **Logon Permitted**, and then click **OK**. **f.** On the **Account** tab, click **Log On To**, click **The following computers**, and then, in the **Computer name** box, type *Server* (where *Server* is your assigned computer name). **g.** Click **Add**, and then click **OK**. **h.** On the **Account** tab, under **Account expires**, click **End of**, and then select the first Friday from the current date. **i.** On the **Profile** tab, in the **Profile path** box, type **\\london\profiles\%username%** **j.** Under **Home folder**, click **Connect**, and then click **H:**. **k.** In the **To** box, type **\\london\home\%username%** and then click **OK**. **l.** Close Active Directory Users and Computers, and then log off.
5. Attempt to log on nwtraders as *Server*T2 (where *Server* is your assigned computer name) with the password of **password** and verify account logon restrictions.	**a.** Attempt to log on using the following information: User Logon name: *Server***T2** (where *Server* is your assigned computer name) Password: **password** Log on to: **nwtraders** *A message appears, indicating that you are unable to log on due to an account restriction.*

What account restriction prevents Temp2 from logging on? Why?

The user account is configured with the logon hours of Monday through Saturday, 12 A.M. to 6 P.M., and Monday through Saturday, 9 P.M. to 12 A.M.

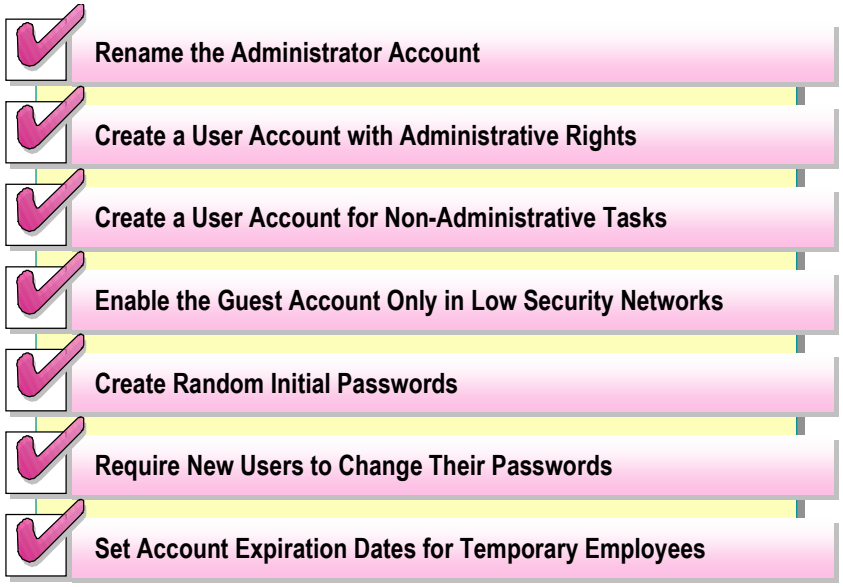
5. (*continued*)	**b.** Click **OK**.

Tasks	Detailed Steps
6. Log on to nwtraders as *Server*T1 (where *Server* is your assigned computer name) with the password of **password**. Open a command prompt and verify the drive letter. Then, create a text file named *Your Name* on the desktop.	**a.** Log on using the following information: User Logon name: *Server***T1** (where *Server* is your assigned computer name) Password: **password** Log on to: **nwtraders** **b.** Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
Why is the command prompt letter H? **Because H was the drive letter that was defined in the Profile tab of *Server*T1 for the home folder location.**	
6. *(continued)*	**c.** Close the command prompt. **d.** Right-click the desktop, click **New**, and then click **Text Document**. **e.** Name the text file *Your Name*. **f.** Close any open windows, and then log off.
7. At your partner's computer, log on to nwtraders as *Server*T1 (where *Server* is your computer name) with the password of **password**. Verify the text file you created in task 6 displays on the desktop.	**a.** At your partner's computer, log on using the following information: User Logon name: *Server***T1** (where *Server* is your computer name) Password: **password** Log on to: **nwtraders** **b.** Verify that the text file you created in task 6 displays on the desktop.
Why does the text file you created in task 6 display when *Server*T2 (where *Server* is your computer name) is logged on to your *partner's server* (where *partner's server* is your partner's server name)? **Because *Server*T2 (where *Server* is your computer name) is configured with a roaming profile.**	
7. *(continued)*	**c.** Log off your partner's server.

Best Practices

Topic Objective
To list the best practices for creating and managing user accounts.

Lead-in
There are several best practices that you should consider when creating and managing user accounts.



**********ILLEGAL FOR NON-TRAINER USE**********

Consider the following best practices for creating and managing user accounts:

- Rename the built-in Administrator account to provide a greater degree of security. Use a name that does not identify it as the Administrator account. This makes it more difficult for unauthorized users to gain access to the account.
- Create a user account for yourself and grant administrator rights to it. You should then use this user account to perform administrative tasks.
- Create a user account that you can use to perform nonadministrative tasks. Log on with the user account that has administrator rights only when you perform administrative tasks.
- Enable the Guest account only in low security networks, and always assign a password to it. The Guest account is disabled by default.
- Create random initial passwords for all new user accounts by using a combination of letters and numbers. Creating a random initial password will help keep the user account secure and increase network security.
- Always require new users to change their passwords the first time they log on to the network. This will ensure that unique, private passwords are used.
- Set user account expiration dates for contract and temporary employees to avoid unauthorized network access when contracts expire.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to User Accounts
- Guidelines for New User Accounts
- Creating Local User Accounts
- Creating and Configuring Domain User Accounts
- Setting Properties for Domain User Accounts
- Customizing User Settings with User Profiles
- Best Practices

**********ILLEGAL FOR NON-TRAINER USE**********

1. You have been asked to create user accounts for a company that has thirty employees. There is one server that is running Active Directory, four member servers to which all employees require access, and thirty-one computers running Windows 2000 Professional. What type of user accounts should you create, and why? On which computer or computers should these accounts reside?

   Create domain user accounts, because the company is using Active Directory to provide users with access to network resources. The domain user accounts should reside on the domain controller.

2. You are a member of the Domain Admins group and you must create several new domain user accounts. However, the domain controller is physically located in a locked office to which you do not have access. Your own computer is running Windows 2000 Professional. How can you create the domain user accounts from your computer?

   Install Windows 2000 Administration Tools on your computer using the Windows 2000 Server or Windows 2000 Advanced Server compact disc. To create the new domain user accounts, open Active Directory Users and Groups from the Administrative Tools menu.

3. You have created a domain user account that is to be used by an employee for data processing work. You do not want this user to be able to log on to any other computers. How can you restrict this account for access to the user's computer only?

   Configure the account for access to the user's computer by clicking the Log On To button on the Account tab of the Properties dialog box for the user account. Add the name of the computer in the Computer name box.

4. A user receives an error message when she attempts to log on. The error message states that Windows cannot locate the user's roaming profile and that the network path was not found. You check the **Profiles** tab in the **Properties** dialog box for the account, and the profile path is set as *share**server**user_logon_name*. Why can't the user log on?

   The path is incorrect. The profile path should be *servershare**user_logon_name*.**

5. User1 has full control permissions to the Research folder. An administrator creates an account for User2 by copying User1's account. When User2 tries to gain access to the Research folder, she receives an error message stating that access is denied. Why can't User2 gain access to the Research folder?

   Permissions and rights that were assigned to the original domain user account are NOT copied to the new domain user account.

6. You are a network administrator but you are logged on as your domain account that does not have administrative rights. You want to run Active Directory Users and Computers to create a new user but your account does not have sufficient rights. Without logging off and then logging back on as administrator, how can you create the new domain user account?

   Open Active Directory Users and Computers with your administrator account by using the runas command. To do this, on the Administrative Tools menu, hold the SHIFT key, right-click Active Directory Users and Computers, and then click Run as. In the Run As Other User dialog box, verify that Run the program as the following user is selected, and then type the user name and password of your administrator account.

7. Employees in the Customer Support group are complaining that when they log on to different computers in their department, their desktop settings are not the same. How can you ensure that the users desktop settings will be the same regardless of which computer they log on to?

   Create a mandatory roaming profile and specify that all Customer Support users must use this mandatory profile.

Microsoft® Training & Certification

Microsoft® Official Curriculum

Module 5: Managing Access to Resources by Using Groups

Contents

Overview	1
Introduction to Windows 2000 Groups	2
Implementing Groups in a Workgroup	5
Implementing Groups in a Domain	10
Lab A: Creating a Global Group	19
Best Practices	23
Review	24

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

Lab:
45 Minutes

This module provides student with the knowledge and skills to set up and administer groups in either a workgroup or a domain. This includes creating groups and adding members, and using the appropriate strategy for the most efficient use of groups.

At the end of this module, students will be able to:

- Identify how groups function and their characteristics.
- Implement groups in a workgroup.
- Implement groups in a domain.
- Identify best practices for implementing groups.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft® PowerPoint® file 2152B_05.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Introduction to Windows 2000 Groups

  First, present information on how groups function. Emphasize that by using groups, an administrator only needs to grant permissions once rather than multiple times. Then, present information on groups in workgroups and domains. Emphasize the difference between an administrator creating groups and groups residing in workgroups and domains.

- Implementing Groups in a Workgroup

  First, present local groups, including information on guidelines for using them and membership rules that apply to them. Then, present built-in groups on client computers and member servers. Next, present the ALP strategy for using local groups in a workgroup, which is to put user accounts (A) into local groups (L), and then grant permissions (P) to the local groups. Finally, present how to create local groups. Do not demonstrate this, but have students gain access to the **New Group** dialog box on their member servers.

- Implementing Groups in a Domain

  First, present information on the group types and group scopes. Be sure to define group types and group scopes. Emphasize that the scope is how a group can be used. You need to mention that this module uses the premise that the network is in native mode and that universal group scope is only visible when a network is in native mode.

  Next, present built-in and predefined groups in a domain. Then present the A G DL P strategy to use groups in a single domain, which is to put user accounts (A) into global groups (G), put global groups into domain local groups (DL), and then grant permissions (P) to the domain local groups. Next, present the guidelines for creating groups in a domain. Demonstrate the procedures for creating and deleting groups. Finally, demonstrate the procedures for adding members to a group.

- Best Practices

  Present the best practices for implementing groups.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

There are no lab setup requirements that affect replication or customization.

To prepare student computers for the labs in this module, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Performing the lab in this module introduces the following configuration changes:

- The creation of the global security group *Server* Backup Admins in *Server*OU (where *Server* is the assigned computer name).
- The global security group *Server* Backup Admins contains the Backup*x* domain account (where *x* is the student's assigned number) from *Server*OU.
- The global security group *Server* Backup Admins is a member of the domain local group Backup Operators.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn how to implement groups to simplify the management of access to network resources.

- **Introduction to Windows 2000 Groups**
- **Implementing Groups in a Workgroup**
- **Implementing Groups in a Domain**
- **Best Practices**

**********ILLEGAL FOR NON-TRAINER USE**********

A *group* is a collection of user accounts. You use groups to simplify the management of user and computer access to shared resources. Groups allow you to grant access permissions to multiple users at one time. After you grant the access permission to a group, you add members to the group that require the permissions.

Microsoft® Windows® 2000 provides different types of groups for different tasks. In this module, you will learn about the various types and characteristics of groups and how to use them.

At the end of this module, you will be able to:

- Identify how groups function and their characteristics.
- Implement groups in a workgroup.
- Implement groups in a domain.
- Identify best practices for implementing groups.

Important This module covers groups in a network in *native* mode instead of *mixed* mode. In native mode, all domain controllers run Windows 2000, while in mixed mode, domain controllers can run either Windows 2000 or Microsoft Windows NT®. The Domain groups react differently depending upon whether the network is in native or mixed mode.

For more information about the mixed mode, see module 3, “Creating a Windows 2000 Domain” in course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Introduction to Windows 2000 Groups

Topic Objective
To list the topics that are relevant to an introduction of groups.

Lead-in
Groups simplify administration by allowing you to grant permissions once rather than multiple times.

- How Windows 2000 Groups Work
- Groups in Workgroups and Domains

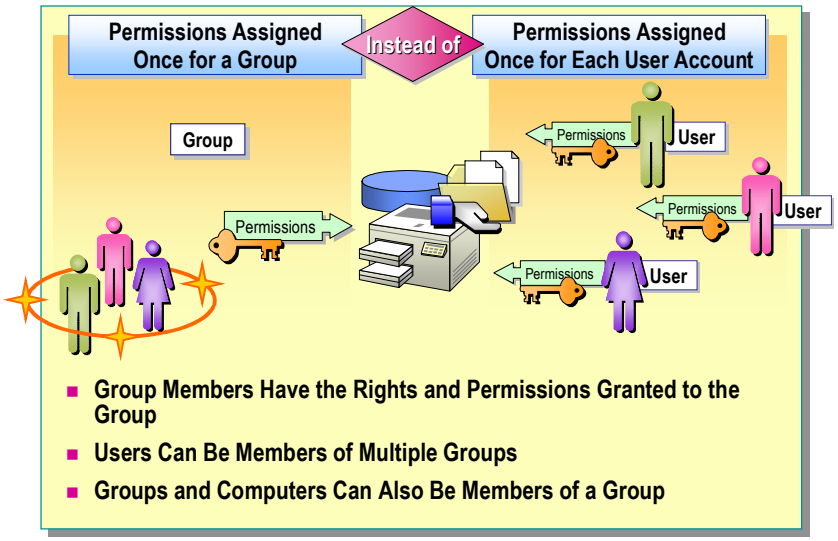
**********ILLEGAL FOR NON-TRAINER USE**********

Before you can use groups effectively, you need to understand their basic purpose and have an overview of how they function in a workgroup or a domain. Where you create and use groups varies depending upon whether you are using them in a workgroup or a domain. For example, in a workgroup you can only use a group on the computer where the group resides. In addition, where a group resides varies depending upon whether it is used in a workgroup or a domain.

How Windows 2000 Groups Work

Topic Objective
To illustrate groups and their purpose.

Lead-in
You use groups to combine user accounts so that you can grant rights and permissions to shared resources once rather than multiple times. This is true whether you are using a group in workgroup or a domain.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Permissions can be granted once to a group of users instead of multiple times to individual users.

A group is a collection of user accounts that you use to manage user access to shared resources, such as network shared folders, files, directories, and printers. A group allows you to grant permissions for shared resource once to the group, instead of multiple times to individual users. This simplifies administration of resource access in a network.

In addition to user accounts, for organizational purposes and administrative tasks, you can make computers and, in some instances, even other groups, members of a group. When you add members to groups, consider the following:

- When you make a user a member of a group, you give the user all of the rights and permissions granted to that group.

  Note If a user is logged on when you make the user a member of a group, the rights and permissions of the group do not take effect until the user logs off and then logs on again.

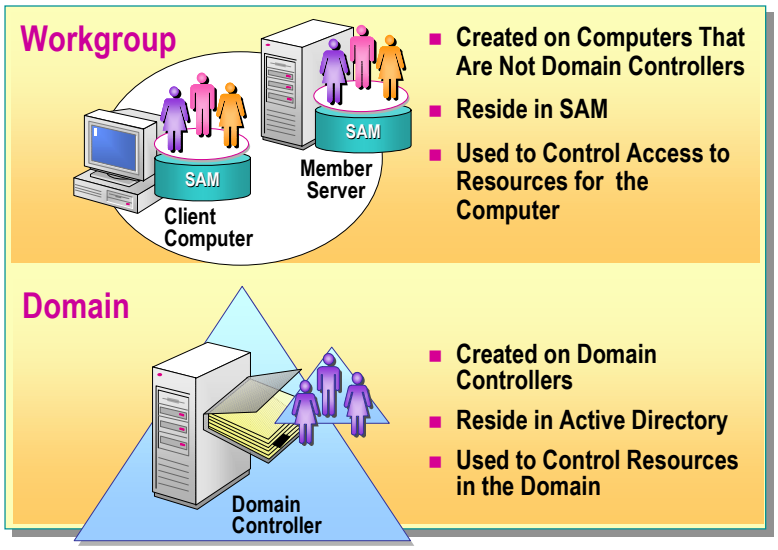
Key Point
A user account can be a member of multiple groups.

- User accounts can be members of multiple groups. This is because a group is simply a list of members, with references to the actual user accounts.

Groups in Workgroups and Domains

Topic Objective
To illustrate the differences between groups in workgroups and domains.

Lead-in
Where you create groups and where they reside is different in workgroups and domains.



**********ILLEGAL FOR NON-TRAINER USE**********

Groups operate differently in a workgroup than in a domain. This includes where they are created and where they reside, as well as how they are used.

Groups in a Workgroup

The characteristics of groups in a workgroup are as follows:

- They are created on computers that are not domain controllers. This includes client computers running Windows 2000 Professional and member servers running Windows 2000 Server or Windows 2000 Advanced Server.
- They reside in the Security Accounts Manager (SAM), which is the local security account database of the computer.
- They are used to grant permissions to resources and grant rights for system tasks only on the computer on which you create the group.

Note For a stand-alone computer, you implement groups in the same manner as you would implement them for a computer in a workgroup.

Groups in a Domain

The characteristics of groups in a domain are as follows:

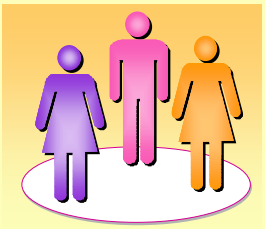
- They are created *only* on domain controllers.
- They reside in the Active Directory™ directory service.
- They are used to grant permissions to resources and grant rights for system tasks on any computer in the domain.

Implementing Groups in a Workgroup

Topic Objective
To list the topics that are relevant to implementing groups in a workgroup.

Lead-in
Local groups are also available for your use. Let's look at how they function and how to create and add members to a local group.

- Local Groups
- Built-in Local Groups
- The Strategy for Using Local Groups in a Workgroup
- Creating Local Groups



**********ILLEGAL FOR NON-TRAINER USE**********

When you implement groups in a workgroup, you implement local groups. You can create local groups only on member servers and on computers running Windows 2000 Professional and you use them to assign permissions to resources only on the local computer. In addition to the groups you create, Windows 2000 provides default groups with specific rights to perform system tasks on the local computer. You simply add users to these groups. There is a group strategy to help you efficiently create and use groups.

Local Groups

Topic Objective
To list the characteristics of local groups.

Lead-in
You can create local groups on a stand-alone server or a computer running Windows 2000 Professional. Use local groups to control access to resources on a specific computer.

- **The Guidelines for Local Groups:**
  - Use local groups on computers that do not belong to a domain
  - Use local groups to control access to resources and who can perform system tasks on the local computer
- **Membership Rules for Local Groups:**
  - Local groups can only contain local user accounts that are on the local computer
  - Local groups cannot be a member of any other group
- **Members of the Administrators Group or Account Operators Group on the Local Computer Can Create Local Groups**

**********ILLEGAL FOR NON-TRAINER USE**********

When you set up local groups you should be aware of the guidelines to follow, how their membership operates, and who can create them. You create them on client computers running Windows 2000 Professional and on member servers running Windows 2000 Server or Windows 2000 Advanced Server.

Guidelines for using local groups include:

Key Point
Use local groups on a computer that is not part of a domain.

- Set up local groups only on computers that do not belong to a domain.

  You can use local groups only on the computer where you create the local groups. Although you can set up local groups on domain client computers and member servers, it is recommended you do not. Using local groups on domain computers prevents you from centralizing group administration. Local groups do not appear in Active Directory and you are required to administer local groups separately for each computer.

Key Points
Although all computers running Windows 2000 have local groups, they should not be used on domain computers. Only domain groups should control access to domain resources.

- Use local groups to control access to resources on the local computer and to perform system tasks for the local computer.

The membership rules for local groups include the following:

- Local groups can only contain local user accounts from the computer where you create the local groups.
- A local group cannot be a member of any other group.

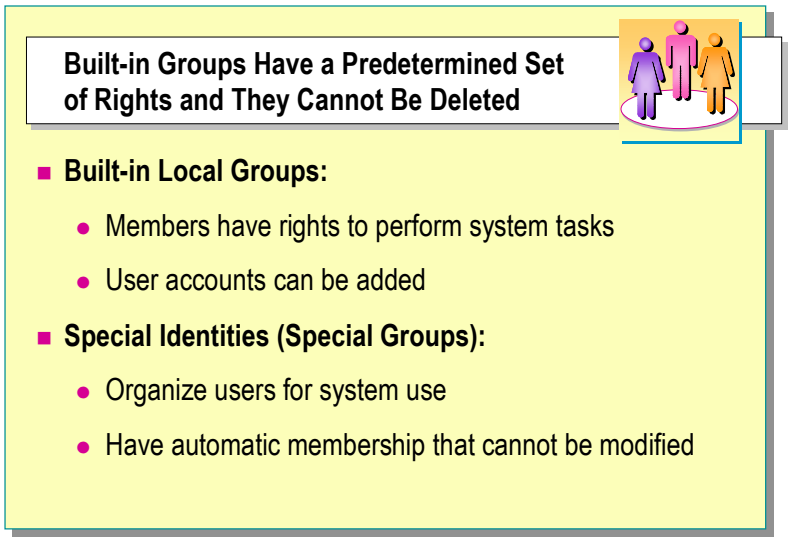
You must be a member of the Administrators group or Account Operators group to create a local group.

Built-in Local Groups

Topic Objective
To list the built-in groups that are automatically created in Windows 2000.

Lead-in
Built-in groups have a predetermined set of rights.

Rights determine the system tasks a user or member of a built-in group can perform.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Have students open the Groups folder in Local Users and Groups in Computer Management and look at the built-in local groups.

Windows 2000 automatically creates built-in groups when you install Windows 2000 Professional on a computer or Windows 2000 Advanced Server on a member server. These built-in groups have a predetermined set of rights. Rights determine the system tasks a user can perform. You cannot delete built-in groups.

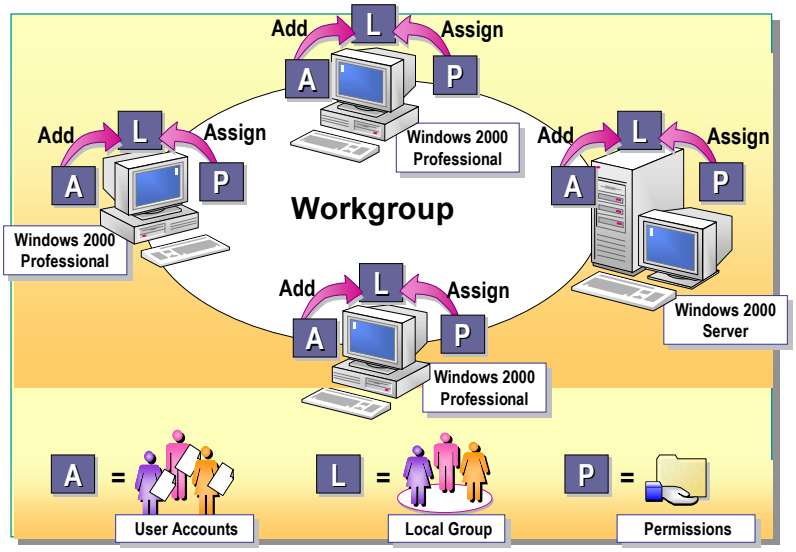
The built-in groups on computers running Windows 2000 and member servers are:

- *Built-in local groups.* These groups give their members the 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 2000. They reside in the Group folder in Local Users and Groups in Computer Management.
- *Special identities.* These groups, also known as special groups, automatically organize users for system use. Administrators cannot modify group membership. Rather, users are either members by default or become members during activities. Special groups are on all computers running Windows 2000. For example, when a user logs on to a computer and gains access to a resource on the computer, through the activity of logging on, the user becomes a member of the special group Interactive.

The Strategy for Using Local Groups in a Workgroup

Topic Objective
To illustrate the strategy for using local groups.

Lead-in
Let's discuss strategies for using local groups to provide access to resources on a local computer that is in a workgroup.



**********ILLEGAL FOR NON-TRAINER USE**********

In a workgroup environment, the strategy you use to grant permissions or grant rights is straightforward. First, you can only use them for the local computer. Any user that wants to gain access to a shared resource or perform a system task on a computer must have a user account on that computer. If multiple users on a computer require access to the same resource or need to perform the same system task, you use a local group to grant the permissions or rights and then add the appropriate user accounts as members.

Key Point
The ALP strategy is limited as an administrator can only grant permissions to resources that reside on the local server.

This method is known as the ALP strategy.

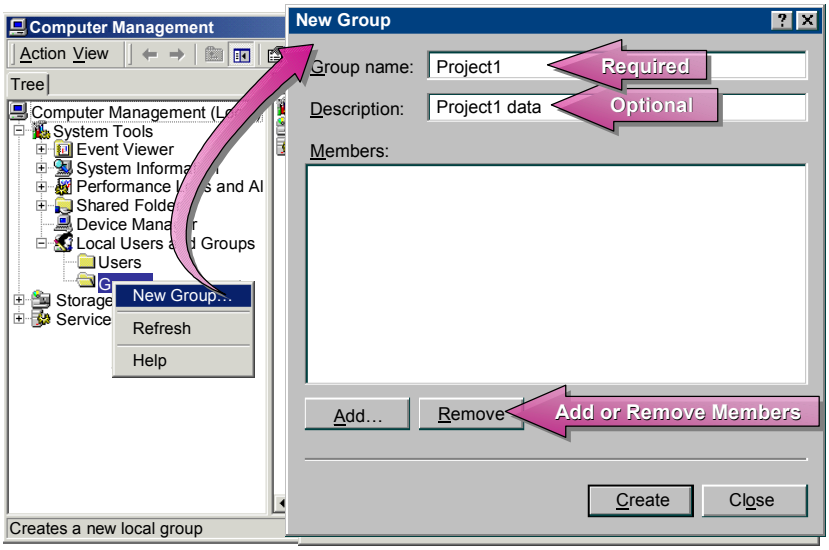
- Place user accounts (A) in a local group (L) on the computer on which the resources reside or on which you want the users to perform system tasks.
- Grant permissions (P) or grant rights to the local group on the computer on which the network resource resides or on which the system tasks are to be performed.

Tip If you can give user accounts rights by putting them in a built-in group, do so rather than creating a new local group.

Creating Local Groups

Topic Objective
To illustrate the user interface for creating local groups on a computer.

Lead-in
Use Computer Management to create local groups on a computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Instruct students to open the Group folder on the computers that are not domain controllers and access the **New Groups** dialog box. Do not have them create local groups as this may affect what they do in the lab.

Use Computer Management to create local groups. You create local groups in the Groups folder. When you create a group you can also add the members. To create a local group and add members, perform the following steps:

1. In Computer Management, expand **Local Users and Groups**.
2. Right-click the **Groups** folder, and then click **New Group**.

   The following table describes the options in the **New Group** dialog box.

Option	Description
Group Name	A unique name for the local group. This is the only required entry. Use any characters except for the backslash (\). The name can contain up to 256 characters; however, very long names may not display in some windows. Make sure the name is intuitive.
Description	A description of the group.
Members	A list of members that belong to the group.

   3. To add a user to the list of members, click **Add**. Select a user or group from the list, click **Add**, and then click **OK**.
   4. To remove a user from the list of members, select the name of the user or group that you want to remove, and then click **Remove**.

5. Click **Create** to create the local group.

Implementing Groups in a Domain

Topic Objective
To list the topics related to implementing groups in a domain.

Lead-in
To create groups in a domain, you should be familiar with the guidelines for creating groups.

- Group Types and Scopes
- Built-in and Predefined Groups in a Domain
- The Strategy for Using Groups in a Single Domain
- Guidelines for Creating Domain Groups
- Creating and Deleting Domain Groups
- Adding Members to Domain Groups

**********ILLEGAL FOR NON-TRAINER USE**********

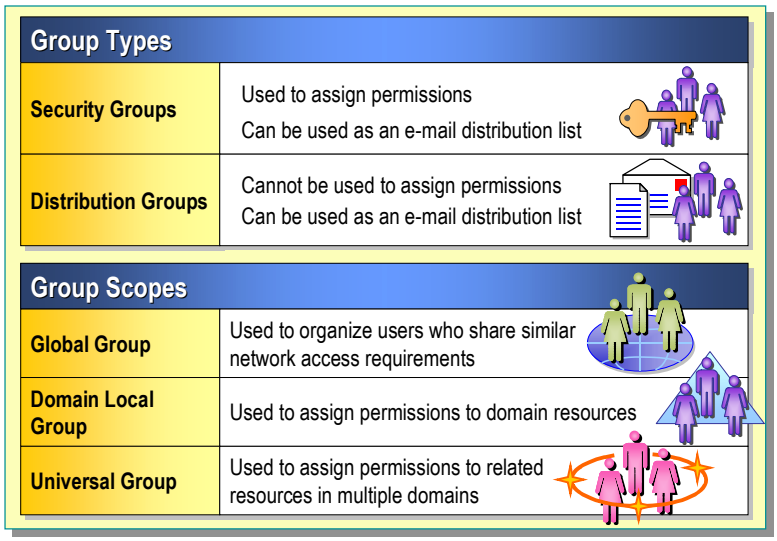
Domain groups enable centralized administration in a domain. All domain groups are created on a domain controller. As with local groups, Windows 2000 creates built-in groups. Because there are more options for using groups in a domain, implementing the appropriate strategy becomes more important.

To implement your group strategy, you should be familiar with the guidelines for creating groups. This enables you to successfully create or delete groups, when necessary, and to add members to groups. Your network will be easier to manage because you took the time to set up groups correctly.

Group Types and Scopes

Topic Objective
To list the group types and group scopes in Windows 2000.

Lead-in
Windows 2000 provides two group types: security and distribution. There are three types of group scopes: global, domain local, and universal.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Because domain groups are stored in Active Directory, an administrator can use them anywhere in the domain and, sometimes, in multiple domains.

In a domain, Active Directory provides support for different types of groups and group scopes. Because they are stored in Active Directory, you can use these groups on any computer in your network. The group *type* determines the type of tasks that you manage with the group. The group *scope* determines whether the group spans multiple domains or is limited to a single domain. Each type of domain group has a scope attribute that identifies how the group is applied on the network.

Group Types

Describe the group types in Active Directory and explain their purpose.

There are two group types in Active Directory, which are:

- *Security groups*. Use security groups for security-related purposes, such as granting permissions to gain access to resources. You can also use them to send e-mail messages to multiple users. Sending an e-mail message to a group sends the message to all members of the group. Therefore, security groups share the capabilities of distribution groups.
- *Distribution groups*. Applications use distribution groups as lists for non-security related functions, such as sending e-mail messages to groups of users. You cannot grant permissions to security groups. Even though security groups have all of the capabilities of distribution groups, distribution groups are still required, because some applications can only read distribution groups.

Note Because distribution groups reside in Active Directory, only applications that are designed to work with Active Directory can use them. For example, future versions of Microsoft Exchange Server will be able to use Windows 2000 groups as distribution lists for e-mail messages.

Group Scopes

Mention that all group scopes are not available unless the network is in native mode. Ensure that the students know the difference between native and mixed mode.

Describe the group scopes in Active Directory and explain their purpose.

The scope of a group determines where you use a group in the domains. The group scope affects group membership and group *nesting*. Nesting is adding a group to another group as a member. Windows 2000 provides three group scopes:

- *Global group scope*. Use this group scope to organize users who share similar network access requirements. You can use a global group to grant permissions to gain access to resources that are located in any domain.
  - Global groups have limited membership. Add user accounts and global groups only from the domain in which you create the global group.
  - Global groups can be nested within other groups. This function allows you to add a global group to another global group in the same domain or to universal and domain local groups in other domains.
- *Domain local group scope*. Use this scope to grant permissions to domain resources that are located in the same domain in which you created the domain local group. The resource does not have to reside on a domain controller.
  - Domain local groups have open membership. Add user accounts, universal groups, and global groups from any domain.
  - Domain local groups cannot be nested within other groups, which means that you cannot add a domain local group to any group, even groups in the same domain.
- *Universal group scope*. Grant permissions to related resources in multiple domains. Use a universal group to grant access permissions to resources that are located in any domain.
  - Universal groups have open membership. All domain user accounts and groups can be members.
  - Universal groups can be nested within other domain groups. This capability allows you to add a universal group to domain local or universal groups in any domain.

Important Security groups with a universal group scope are only available when the domain is in native mode. Native mode is when all domain controllers are running Windows 2000.

Built-in and Predefined Groups in a Domain

Topic Objective
To list the predefined and built-in groups that are automatically created in Windows 2000.

Lead-in
Predefined and built-in groups have a predetermined set of user rights.

User rights determine the system tasks a user or member of a built-in group can perform.

- **Built-in Domain Local Groups Give Users Predefined Rights and Permissions to Perform Tasks:**
  - On domain controllers
  - In Active Directory
- **Special Identities (Special Groups)**
  - Organize users for system use
  - Membership is automatic and cannot be modified
- **Predefined Global Groups Give Administrators Control of Domain Resources**

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Open up Active Directory Users and Computers and show students the built-in and predefined groups on a domain controller.

As with client computers and member servers, domain controllers have default built-in groups. In addition to built-in groups, domain controllers have default predefined groups. When a computer becomes a domain controller, Windows 2000 Advanced Server automatically creates these groups in Active Directory Users and Computers. As with local built-in groups, these groups have predetermined rights, which determine the system tasks members of a built-in or predefined group can perform.

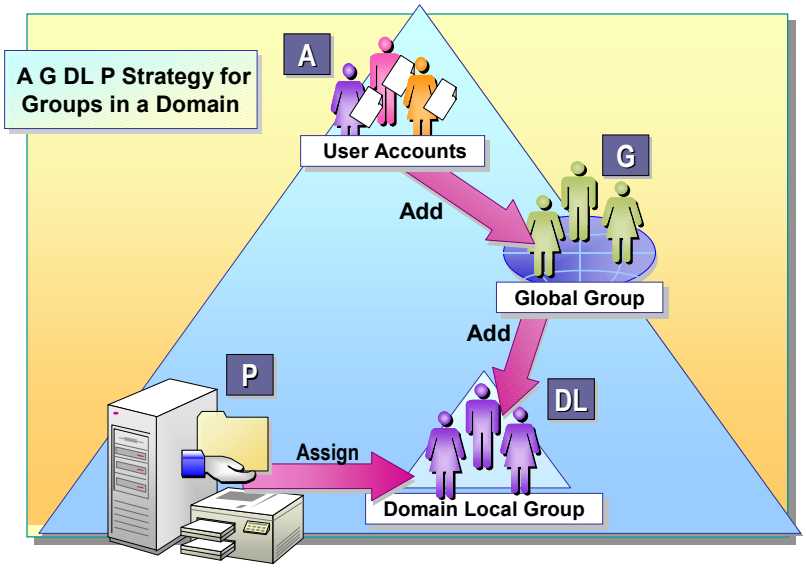
Predefined groups with global scope are located in the Users folder. Built-in groups with domain local scope are located in the Builtin folder. Default domain groups in Windows 2000 include:

- *Built-in domain local groups.* These groups provide users with predefined rights and permissions to perform tasks on domain controllers and in Active Directory. Built-in domain local groups are on domain controllers only. You cannot delete these groups.
- *Special identities.* These groups, also known as special 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 2000. For example, when users connect to a shared folder on a remote computer, they become members of the Network System group. Special groups are not visible in Active Directory Users and Computers.
- *Predefined global groups.* These groups give administrators an easy way of controlling all users in a domain. Predefined global groups are on domain controllers only. These groups reside in the User folder of Active Directory Users and Computers.

The Strategy for Using Groups in a Single Domain

Topic Objective
To illustrate the strategy for using groups in a domain.

Lead-in
The A G DL P strategy is recommended for use in a domain.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Although an administrator could use other strategies, the A G DL P strategy is the most efficient strategy to use.

If students ask why universal groups are not part of the single-domain strategy, mention that universal groups are used in a multi-domain environment because they have open membership and can be added to domain local groups in any domain.

When you use groups in a single domain, you use the *A G DL P* strategy. The A G DL P strategy is: You put user accounts (A) into global groups (G), put the global groups into domain local groups (DL), and then grant permissions (P) to the domain local group.

When setting up the groups, use the following strategy:

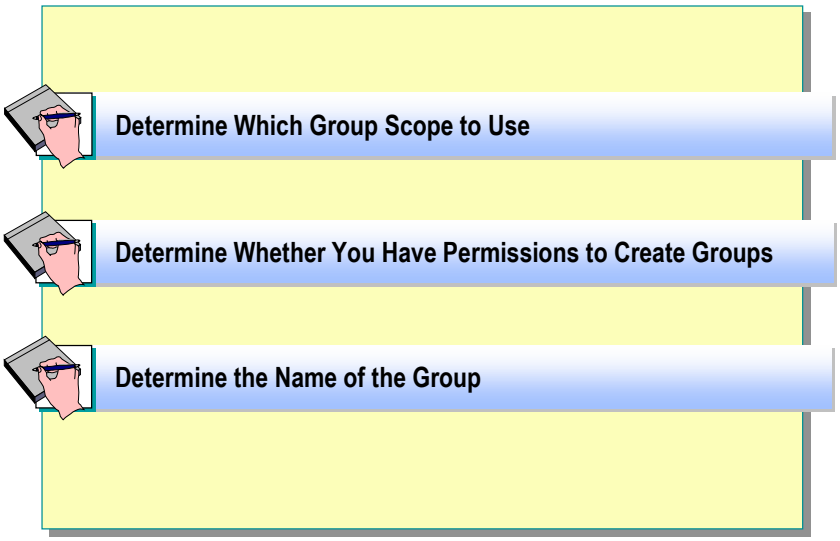
1. Identify users with common responsibilities and add the user accounts to a global group. For example, in a sales department, add user accounts for all sales employees that use the same resources to a global group called Sales.
2. Determine whether you can use a built-in domain local group, or if you need to create one to provide users with access to domain resources. For example, if you want users to be able to print to a shared color printer in the domain, create a domain local group called Color Printer Users.
3. Make all global groups that share the same access needs for resources members of the appropriate domain local group. For example, add the appropriate global groups, including Sales, to the domain local group Color Printer Users.
4. Grant the required permissions to the domain local group on the domain controller. You grant permissions at the resource. For example, grant the necessary permissions to use color printers to the Color Printers Users domain local group.

Note Grant permissions to a domain local group at the resource. For an example of how to grant permissions at the resource, see module 7, "Providing Network Access to File Resources," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Advanced Server*.

Guidelines for Creating Domain Groups

Topic Objective
To list the guidelines for creating groups in a domain.

Lead-in
Follow these guidelines when you create groups in a domain.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Follow the guidelines for creating domain groups before you create them.

Members of the built-in domain Administrator or Account Operators groups can create groups in the domain. An administrator can assign a user the permission to create domain groups.

When creating groups for use in a domain, you should consider the following guidelines:

- Determine the required group scope based on how you want to use the group. For example, use global groups to group user accounts. Alternatively, use domain local groups to grant permissions to a resource.
- Determine whether you have the necessary permissions to create a group in the appropriate domain:
  - By default, members of the Administrators or Account Operators group in a domain have the necessary permissions to create groups.
  - An administrator can give a user the permission to create groups in the domain.
- Determine the name of the group. Make the name intuitive so that it reflects the purpose for which it was created. This is especially useful if administrators from other domains search for it in Active Directory.

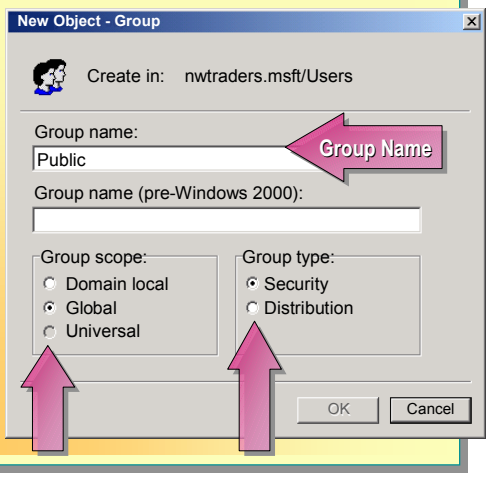
Note If there are parallel groups in multiple domains, make sure that the names are parallel and that they reflect the domain names. For example, if there is a group for managers in each domain, these groups should use a similar naming scheme, such as Managers USA and Managers Australia.

Creating and Deleting Domain Groups

Topic Objective
To list the key points to consider when creating and deleting groups.

Lead-in
Use Active Directory Users and Computers to create or delete groups.

- **You Use Active Directory Users and Computers to Create and Delete Groups**
- **When You Delete a Group Its:**
  - Rights and permissions are removed
  - Members are not deleted
  - SID is never used again



**********ILLEGAL FOR NON-TRAINER USE**********

You create and delete groups in Active Directory Users and Computers. You can create them in the default Users folder or in any folder that you create. When you no longer need a group, be sure to delete it is so that you do not accidentally grant permissions to it.

Delivery Tip
Demonstrate the procedures to create a group by using Active Directory Users and Computers.

Make sure students know what an Active Directory object is.

Creating a Group

To create a group, open Active Directory Users and Computers. Right-click the folder in which you want to create a group, point to **New**, and then click **Group**. The following table describes the options in the **New Object – Group** dialog box.

Option	Description
Group name	The name of the new group. The name must be unique in the domain where you create the group.
Group name (pre-Windows 2000)	The name used to support clients and servers from earlier versions of Windows.
Group scope	The group scope. Click **Domain local**, **Global**, or **Universal**.
Group type	The type of group. Click **Security** or **Distribution**.

Note After you have created a group, Windows 2000 allows you to move a group within your domain structure whenever organizational or administrative functions change. Although it is easy to move a group, because a group is an Active Directory object, ramifications of what happens to the permissions and rights of its members is complex. For information on moving Active Directory objects, see module 4, "Setting Up and Administering Domain Users and Groups," in course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Delivery Tip
Demonstrate how to delete a group by using Active Directory Users and Computers.

Key Point
A group's SID is not reusable. If an administrator deletes a group and then creates a group with the same name, it will have a different SID and Windows 2000 will not recognize it as the same group.

Deleting a Group

When you delete a group, you remove the permissions and rights that are associated with it. Deleting a group does not delete the user accounts or groups that are members of the group.

Each group that you create has a unique, non-reusable identifier, called the security identifier (SID). Windows 2000 uses the SID to identify the group and the permissions that are granted to it. When you delete a group, Windows 2000 never uses the SID again, even if you create a new group with the same name as the group that you deleted. Therefore, you cannot restore access to resources by creating a group with the same name.

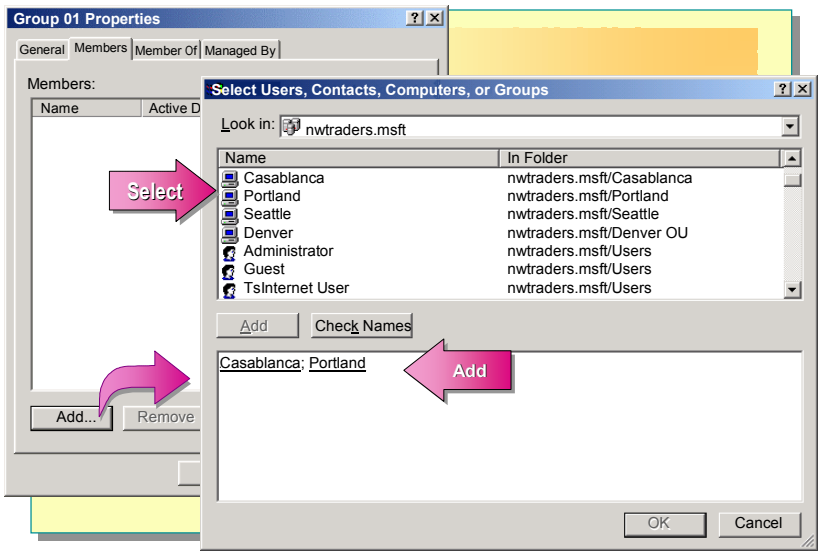
To delete a group, open Active Directory Users and Computers. In the console tree, expand the domain, and then click the folder that contains the group that you want to delete. In the details pane, right-click the group that you want to delete, and then click **Delete**.

Note You cannot delete built-in or predefined groups.

Adding Members to Domain Groups

Topic Objective
To illustrate the user interface for adding members to a group.

Lead-in
You can add user accounts, other groups, and computers to a group by using the **Select Users**, **Contacts**, **Computers, or Groups** dialog box.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the procedure to add members to a group by using Active Directory Users and Computers.

After you create a group, you can add members to that group. Members of groups can include user accounts, other groups, and computers. Use Active Directory Users and Computers to add members to a group.

To add members to a group, perform the following steps:

1. In the **Properties** dialog box for the appropriate group, click the **Members** tab, and then click **Add**.
2. In the **Look in** list, select a domain from which to display user accounts and groups. You can also select **Entire Directory** to view user accounts and groups from anywhere in Active Directory.

Tip When adding members, you can sort members by the name or the folder in which they reside. In the **Select Users**, **Contacts**, **Computers**, **or Groups** dialog box, click the appropriate column.

3. In the **Name** column, select the user account or group that you want to add, and then click **Add**. You can also type the name of the user account or group that you want to add. Repeat this step to add additional user accounts or groups.
4. Click **OK** to add the members to the group, and then click **OK** again.

Tip You can also add a user account or group to another group by using the **Member Of** tab in the **Properties** dialog box for that user account or group. Use this method to add the same user or group to multiple groups quickly.

Lab A: Creating a Global Group

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create a global group, add members, and then add the global groups to a built-in domain local group.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a global group.
- Add a domain user account to a global group.
- Add a global group to a domain local group.

Prerequisite

Before working on this lab, you must have knowledge of domain groups.

Lab Setup

To complete this lab, you need:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- A domain user account named Backup*x* (where *x* is your assigned student number).
- An organizational unit named *Server*OU (where *Server* is your assigned computer name).

Estimated time to complete this lab: 45 minutes

Exercise 1
Creating a Global Group and Completing the A G DL P Process

Scenario

The Human Resources manager wants to implement a backup strategy and needs you to create the users and groups. The computers that need to be backed up are in the nwtraders.msft domain, one is a domain controller and the other is a member server. You need to place the user account specified by your manager into the group that has the user rights required to perform a backup.

Goal

In this exercise, you will create a global group, add a user account to the global group, and then add the global group to a built-in domain local group.

Tasks	Detailed Steps
1. Log on to the nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and, using Active Directory Users and Groups, create the global group named *Server* Backup Admins (where *Server* is your assigned computer name).	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Active Directory Users and Computers from the **Administrative Tools** menu. **c.** In the console tree, expand **nwtraders.msft**, and then click *Server***OU** (where *Server* is your assigned computer name). **d.** Right-click *Server* **OU**, point to **New**, and then click **Group**. **e.** In the **Group name** box, type *Server* **Backup Admins** (where *Server* is your assigned computer name). **f.** Verify that the group scope is **Global**, and that the group type is **Security**, and then click **OK**.
Which step in the A G DL P process have you completed? **Step G. You have created a global group named Server Backup Admins.**	
2. Add the domain user account Backup*x* (where *x* is your assigned student number) to the *Server* Backup Admins group (where *Server* is your assigned computer name).	**a.** In the details pane, double-click *Server* Backup Admins (where *Server* is your assigned computer name). **b.** In the ***Server* Backup Admins Properties** dialog box, on the **Members** tab, click **Add**. **c.** In the **Select Users, Contacts, Computers, or Groups** dialog box, under **Name**, click Backup*x* (where *x* is your assigned student number), click **Add**, and then click **OK**. **d.** Click **OK** to close the ***Server* Backup Admins Properties** dialog box.

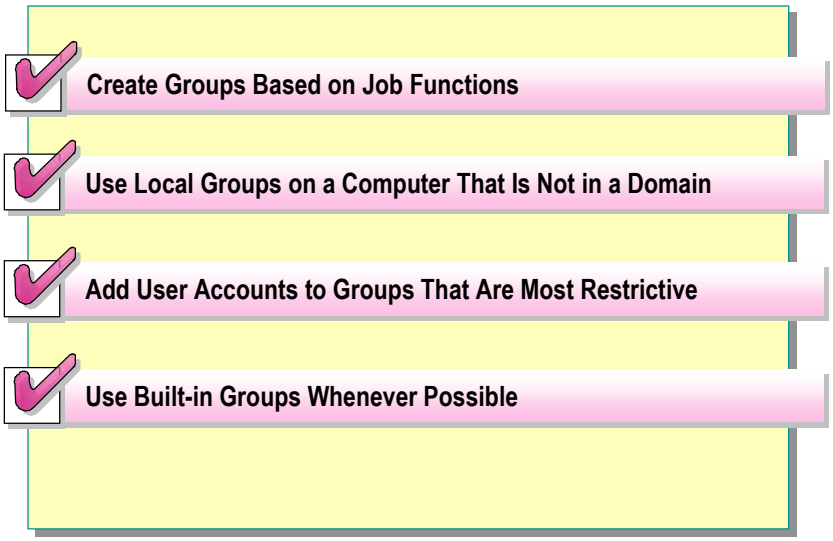
Tasks	Detailed Steps
	At this point in the lab, which step in the A G DL P process have you completed? **A in to G. You have placed the Backup*x* user account into the global group *Server* Backup Admins.**
3. Attempt to add the *Server* Backup Admins group (where *Server* is your assigned computer name) to the built-in domain local group, Backup Operators.	**a.** In the console tree, click **Builtin**, and then in the details pane, double-click **Backup Operators**. **b.** In the **Backup Operators Properties** dialog box, on the **Members** tab, attempt to add the *Server* **Backup Admins** group (where *Server* is your assigned computer name) to the Backup Operators domain local group by clicking **Add**.
	Were you able to add a member to the Backup Operators group? Why or why not? **You could not add a member to the Backup Operators group because you did not have the appropriate rights to perform this operation.**
3. (*continued*)	**c.** Click **Cancel** to close the **Backup Operators Properties** dialog box.
4. Open a second instance of Active Directory Users and Computers, opening the tool as DAdmin with a password of **domain**. Add the *Server* Backup Admins group to the Backup Operators group, and then close this instance of Active Directory Users and Computers.	**a.** Minimize Active Directory Users and Computers. **b.** In the **Administrative Tools** menu, hold the SHIFT key, right-click **Active Directory Users and Computers**, and then click **Run as**. **c.** Complete the **Run As Other User** dialog box using the following information: User name: **DAdmin** Password: **domain** Domain: **nwtraders.msft** **d.** In Active Directory Users and Computers, in the console tree, click **Builtin**, in the details pane, right-click **Backup Operators**, and then click **Properties**. **e.** In the **Backup Operators Properties** dialog box, on the **Members** tab, click **Add**. **f.** In the **Select Users, Contacts, Computers, or Groups** dialog box, under **Name**, click *Server* **Backup Admins** (where *Server* is your assigned computer name), click **Add**, and then click **OK**. **g.** Click **OK** to close the **Backup Operators Properties** dialog box, and then close Active Directory Users and Computers.

Tasks	Detailed Steps
	At this point in the lab, which step in the A G DL P process have you completed? **G into DL. You have placed the global group *Server* Backup Admins into the domain local group Backup Operators.**
	How would you complete step P in the A G DL P process? **By assigning access permissions to a to a folder for a domain local group.**
5. (*continued*)	**a.** Log off.

Best Practices

Topic Objective
To list the best practices for creating groups.

Lead-in
Review this checklist before you create groups.



**********ILLEGAL FOR NON-TRAINER USE**********

The following list provides best practices for implementing groups:

- Create groups based on job functions. When you create a group based on a job function and another person takes over that job, you only need to change the group membership. You do not need to change all permissions that are granted to the individual user account. Because of this, it is sometimes advantageous to create a group that has only one member.
- Use local groups only on computers that are not in a domain, as you cannot centrally administer local groups.
- When there are multiple groups from which to choose, always add user accounts to the group that is most restrictive, while still allowing the appropriate rights and permissions to allow users to accomplish any required task.
- Whenever a built-in group enables users to accomplish a task, use it instead of creating a new group. Create groups only when there are no built-in groups that provide the required rights and permissions.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to Windows 2000 Groups
- Implementing Groups in a Workgroup
- Implementing Groups in a Domain
- Best Practices

**********ILLEGAL FOR NON-TRAINER USE**********

1. Why should you use groups?

   Use groups to simplify administration by granting rights and permissions to the group once, rather than multiple times to each individual member.

2. Can users be members of more than one group?

   Yes, because a group is a list of members with references to the actual user accounts. Therefore, users can be members of more than one group.

3. Can you assign users to a special group?

   No, administrators do not assign users to special groups. Users are either members of special groups by default, or they become members during network activity.

4. Describe the different domain group types and group scopes.

   Group Types: Security groups are used to grant permissions. Distribution groups are used as e-mail distribution lists.

   Group Scopes: Global groups are used to organize users who share similar network access requirements within the same domain.

   Domain local groups are used to grant permissions to resources. Universal groups are used to organize users from multiple domains.

5. Can you create local groups on domain controllers?

   You cannot create local groups on domain controllers because domain controllers cannot have a security database that is independent of the database in Active Directory. Domain controllers can only have domain local groups.

6. What strategy should you apply when granting permissions in a domain?

   A G DL P: Place user accounts (A) into global groups (G), place global groups into domain local groups (DL), and then grant permissions (P) to the domain local group.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 6: Managing Data by Using NTFS

Contents

Overview	1
Introduction to NTFS Permissions	2
How Windows 2000 Applies NTFS Permissions	4
Using NTFS Permissions	11
Using Special NTFS Permissions	15
Lab A: Using NTFS Permissions	19
Compressing Data on an NTFS Partition	24
Configuring Disk Quotas on NTFS Partitions	29
Lab B: Configuring Disk Compression and Quotas	33
Securing Data by Using EFS	39
Lab C: Securing Files by Using EFS	44
Review	50

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

Labs:
75 Minutes

This module provides the knowledge and skills necessary to configure access permissions on an NTFS file system partition, to configure and set disk quotas, and to secure data on an NTFS partition by enabling encryption.

At the end of this module, students will be able to:

- Describe NTFS permissions.
- Explain how Microsoft® Windows® 2000 applies NTFS permissions.
- Use NTFS permissions.
- Grant Special NTFS permissions.
- Compress data on an NTFS partition.
- Configure disk quotas on NTFS partitions.
- Secure data by using Encrypting File System (EFS).

Materials and Preparation

This section provides you with the required materials and preparation tasks needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_06.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.

Other Activities

This section provides procedures for implementing interactive activities to present or review information, such as games or role playing exercises.

Classroom Discussion

► **To prepare for the activity**

1. Read over the discussion questions and answers.
2. Brainstorm a possible list of alternative answers and their advantages and disadvantages.

Module Strategy

Use the following strategy to present this module:

- Introduction to NTFS Permissions

  This topic provides information about NTFS file permissions. Explain how NTFS permissions control the access of user accounts and groups to files and folders.

- How Windows 2000 Applies NTFS Permissions

  This topic provides information about how NTFS permissions are applied in Windows 2000. Explain how multiple permissions combine. Next, explain how NTFS permissions are inherited and how inheritance is prevented. Explain the effect that copying and moving folders and files may have on permissions. Use the class discussion to reinforce students' understanding of how Windows 2000 applies NTFS permissions.

- Using NTFS Permissions

  This topic provides information about granting NTFS permissions to user accounts and groups to control access to file and folders. Demonstrate granting permissions to folder, and then demonstrate how to block inheritance for a file contained in the folder. Explain that subfolders and files inherit permissions from parent folders by default. Discuss best practices for using NTFS permissions.

- Using Special NTFS Permissions

  This topic provides information about the use of special NTFS permissions for user accounts and groups to control access to file and folders. Discuss the difference between special NTFS permissions and standard NTFS permissions. Explain that standard NTFS permissions are comprised of special NTFS permissions. Briefly discuss the two special permissions mentioned in the module.

- Compressing Data on an NTFS Partition

  This topic provides information about the use of compression on NTFS partitions to save hard disk space. Mention the three characteristics of compressed files and folders. Then, demonstrate how to set the compression state for a folder and an alternate color for the folder display. Use the animated slide to describe the compression of files and folders that are copied or moved. Discuss best practices for compressing data.

- Configuring Disk Quotas on NTFS Partitions

  This topic provides information about the use of disk quotas to manage storage growth. Discuss the characteristics of disk quotas. Demonstrate how to enable disk quotas for all users and one user.

- Securing Data by Using EFS

  This topic provides information about the use of EFS on NTFS partitions to secure data. Discuss the purpose of encrypting and decrypting files and folders. Demonstrate how to encrypt and decrypt a file. Explain the procedure for recovering an encrypted file.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

The labs in this module require each pair of student computers to be a member server of the nwtraders.msft domain. To prepare the student computers to meet this requirement, complete lab A, "Installing Windows 2000," in module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- The NTFS permissions on C:\MOC\Win2152b\Labfiles\Lab06\Data will be modified from the default NTFS permissions.
- The Inetpub folder (and its contents) will be compressed.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about managing data on an NTFS partition.

- **Introduction to NTFS Permissions**
- **How Windows 2000 Applies NTFS Permissions**
- **Using NTFS Permissions**
- **Using Special NTFS Permissions**
- **Compressing Data on an NTFS Partition**
- **Configuring Disk Quotas on NTFS Partitions**
- **Securing Data by Using EFS**

**********ILLEGAL FOR NON-TRAINER USE**********

The NTFS file system in Microsoft® Windows® 2000 is extremely efficient in the way it stores data on a partition. With NTFS, you can grant permissions to folders and files in order to control the level of access that users have to resources. NTFS also uses hard disk space more efficiently by allowing you to compress data and configure disk quotas. In addition, NTFS allows you to encrypt file data on the physical hard disk using the Encrypting File System (EFS). It is important that you understand NTFS and its capabilities so that you can efficiently implement this feature of Windows 2000.

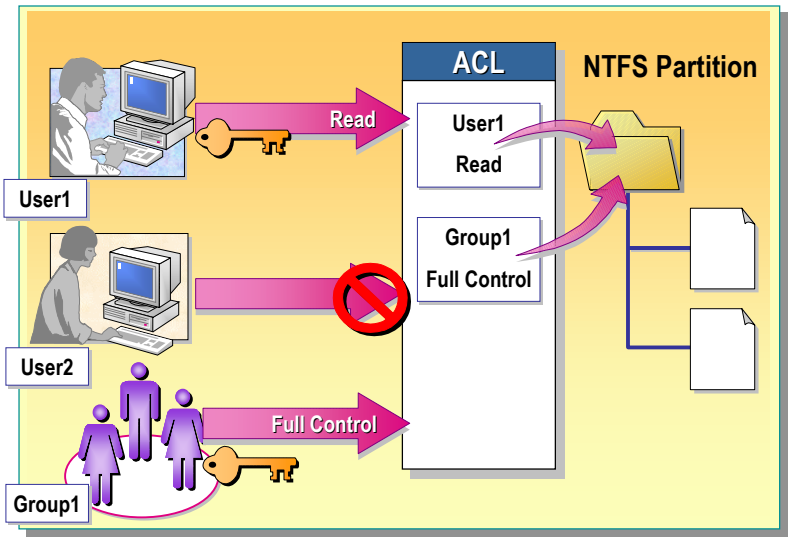
At the end of this module, you will be able to:

- Describe NTFS permissions.
- Explain how Windows 2000 applies NTFS permissions.
- Use NTFS permissions.
- Grant special NTFS permissions.
- Compress data on an NTFS partition.
- Configure disk quotas on NTFS partitions.
- Secure data by using EFS.

Introduction to NTFS Permissions

Topic Objective
To introduce NTFS permissions.

Lead-in
Use NTFS permissions to control the access of user accounts and groups to folders and individual files.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
NTFS permissions are only available on NTFS partitions. NTFS permissions are not available on partitions that are formatted with FAT or FAT32 file systems.

Windows 2000 only provides NTFS permissions on NTFS formatted partitions. To secure files and folders on NTFS partitions, you grant NTFS permissions for each user account or group that needs access to the resource. Users must be granted explicit permission to gain access to resources. If no permission is granted, the user account cannot gain access to the file or folder. NTFS security is effective whether a user gains access to a folder or file at the computer or over the network.

Access Control List

NTFS stores an access control list (ACL) with every file and folder on an NTFS partition. The ACL contains a list of all user accounts, groups, and computers that have been granted access for the file or folder, and the type of access that they have been granted. In order for a user to access to a file or folder, the ACL must contain an entry, called an access control entry (ACE), for the user account, group, or computer to which the user belongs. The entry must specifically allow the type of access the user is requesting in order for the user to be able to gain access to the file or folder. If no ACE exists in the ACL, Windows 2000 denies the user access to the resource.

NTFS Permissions

You use NTFS permissions to specify which users, groups, and computers can access files and folders. NTFS permissions also dictate what users, groups, and computers can do with the contents of the file or folder.

NTFS Folder Permissions

You grant folder permissions to control access to folders and the files and subfolders that are contained within those folders. The following table lists the standard NTFS folder permissions that you can grant and the type of access that each permission provides.

Explain that Read-only, Hidden, Archive, and System (file) are examples of folder attributes.

NTFS folder permission	Allows the user to
Read	View files and subfolders in the folder and view folder attributes, ownership, and permissions.
Write	Create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
List Folder Contents	View the names of files and subfolders in the folder.
Read & Execute	Traverse folders, plus perform actions permitted by the Read permission and the List Folder Contents permission.
Modify	Delete the folder and perform actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions.

NFTS File Permissions

You grant file permissions to control access to files. The following table lists the standard NTFS file permissions that you can grant and the type of access that each permission provides to users.

NTFS file permission	Allows the user to
Read	Read the file, and view file attributes, ownership, and permissions.
Write	Overwrite the file, change file attributes, and view file ownership and permissions.
Read & Execute	Run applications and perform the actions permitted by the Read permission.
Modify	Modify and delete the file and perform the actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, and perform the actions permitted by all other NTFS file permissions.

Important When you format a partition with NTFS, Windows 2000 automatically grants the Full Control permission for the root folder to the Everyone group. By default, the Everyone group will have Full Control to all folders and files that are created in the root folder. To restrict access to authorized users, you should change the default permissions for folders and files that you create.

How Windows 2000 Applies NTFS Permissions

Topic Objective
To introduce how Windows 2000 applies NTFS permissions for files and folders.

Lead-in
There are rules associated with how NTFS applies permissions for files and folders.

- **Multiple NTFS Permissions**
- **NTFS Permissions Inheritance**
- **Copying and Moving Files and Folders**
- **Class Discussion: Applying NTFS Permissions**

**********ILLEGAL FOR NON-TRAINER USE**********

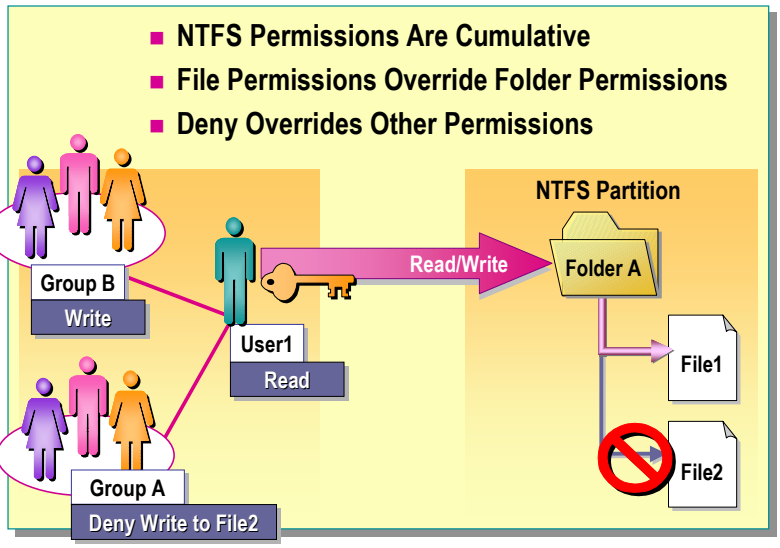
By default, when you grant permissions to users and groups for a folder, the users or groups have access to the subfolders and files contained in the folder. It is important that you understand how subfolders and files inherit NTFS permissions from parent folders so that you can use inheritance to propagate permissions to files and folders.

If you grant permissions to an individual user account or to a group of which the user is a member for a file or folder, then the user has multiple permissions for the same resource. There are rules and priorities that are associated with how NTFS combines multiple permissions. In addition, you can also affect permissions when you copy or move files and folders.

Multiple NTFS Permissions

Topic Objective
To explain how multiple NTFS permissions combine.

Lead-in
It is important to understand how NTFS permissions combine and take priority.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how multiple permissions combine, how file permissions take priority over folder permissions, and how the Deny permission overrides other permissions.

Explain the illustration on the slide.

If you grant NTFS permissions to an individual user account in addition to a group to which the user belongs, then you have granted multiple permissions to the user. There are rules for how NTFS combines these multiple permissions to produce the user's effective permission.

Permissions Are Cumulative

A user's effective permissions for a resource are the combination of the NTFS permissions that you grant to the individual user account and the NTFS permissions that you grant to the groups to which the user belongs. For example, if a user has the Read permission for a folder and is a member of a group with the Write permission for the same folder, then the user has both the Read and Write permissions for that folder.

File Permissions Override Folder Permissions

NTFS file permissions take priority over NTFS folder permissions. For example, a user with the Change permission for a file will be able to make changes to the file even if he or she has only the Read permission for the folder containing the file.

Deny Overrides Other Permissions

Explain the difference between the Deny permission and no permissions.

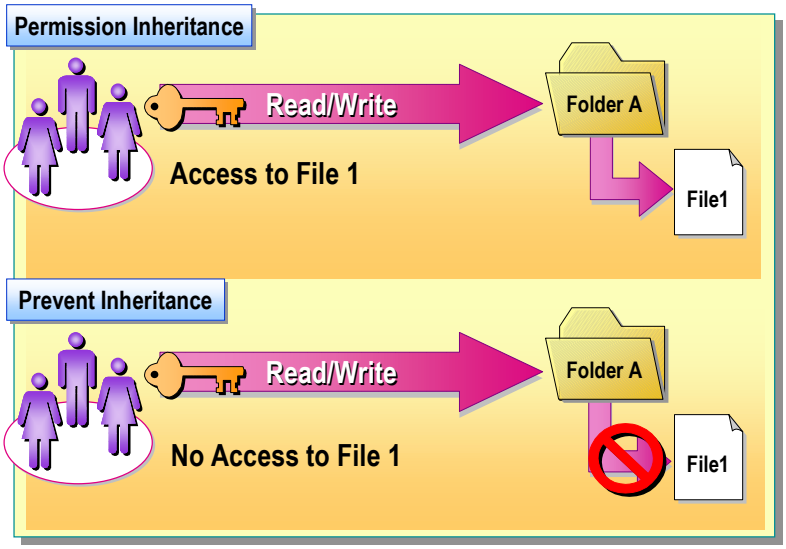
You can deny access to a specific file or folder by granting the Deny permission to the user account or group. Even if a user has permission to access the file or folder as a member of a group, denying permission to the user blocks any other permission that the user has. Therefore, the Deny permission is an exception to the cumulative rule. You should avoid denying permission because it is easier to allow access to users and groups than to specifically deny access. It is preferable to structure groups and organize resources in folders so that allowing permissions is sufficient.

Note With Windows 2000, there is a difference between a user not having access, and specifically denying a user access by adding a deny entry to the ACL for the file or folder. This means that as an administrator, you have an alternative to denying access. Instead, you can simply choose to not allow a user access to a file or folder.

NTFS Permissions Inheritance

Topic Objective
To explain how NTFS permissions are inherited and how inheritance is prevented.

Lead-in
NTFS permissions are inherited from the folder in which they are created or contained.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how permissions are inherited and how to prevent inheritance.

Grant permissions and show students how permissions are propagated from a folder to its subfolders and files. Also, show students how to add permissions to a file or folder that has inherited permissions from a parent folder.

Explain the illustration on the slide.

By default, permissions that you grant to a parent folder are inherited by and propagated to the subfolders and files that are contained in the parent folder. However, you can prevent permissions inheritance if you want folders or files to have different permissions than their parent folder.

Permissions Inheritance

Whatever permissions you grant for a parent folder also apply to the subfolders and files that are contained within. When you grant NTFS permissions to give access to a folder, you grant permissions for the folder, for any existing files and subfolders, and for any new files and subfolders that are created in the folder.

Preventing Permissions Inheritance

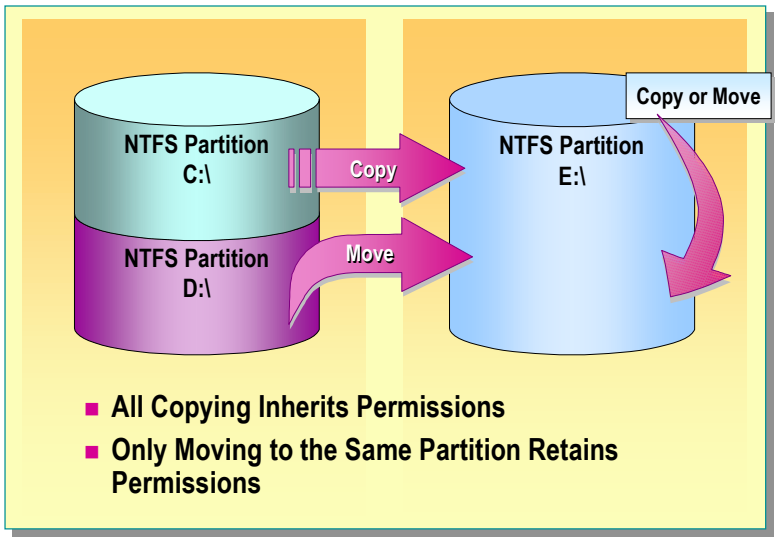
You can prevent permission inheritance, thereby preventing subfolders and files from inheriting permissions from parent folders. To prevent permission inheritance, you remove the inherited permissions and retain only the permissions that were explicitly granted.

The subfolder for which you prevent permission inheritance from its parent folder now becomes the new parent folder. The subfolders and files that are contained within this new parent folder inherit the permissions granted for its parent folder.

Copying and Moving Files and Folders

Topic Objective
To illustrate what happens to NTFS permissions when you copy or move files or folders.

Lead-in
Copying or moving files or folders within and between NTFS partitions may have an effect on permissions.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
When you copy a file within an NTFS partition or between NTFS partitions, Windows 2000 treats the file as a new file. As a new file, it takes on the permissions of the destination folder.

You must have the Write permission for the destination folder in order to be able to copy files and folders.

When you copy or move a file or folder, the permissions may change depending on where you move the file or folder. It is important to understand the changes that the permissions undergo when being copied or moved.

Copying Files and Folders

When you copy files or folders from one folder to another folder, or from one partition to another partition, permissions for the files or folders may change. Copying a file or folder has the following effects on NTFS permissions:

- When you copy a folder or file within a single NTFS partition, the copy of the folder or file inherits the permissions of the destination folder.
- When you copy a folder or file between NTFS partitions, the copy of the folder or file inherits the permissions of the destination folder.
- When you copy files or folders to non-NTFS partitions such as file allocation table (FAT), the folders and files lose their NTFS permissions, because non-NTFS partitions do not support NTFS permissions.

To copy files and folders within a single NTFS partition or between NTFS partitions, you must have Read permission for the originating folder and Write permission for the destination folder.

Key Points
To move a file or folder, you must have the Write permission for the destination folder and the Modify permission for the source folder.

Moving Files and Folders

When you move a file or folder, permissions may change, depending on the permission of the destination folder. Moving a file or folder has the following effects on NTFS permissions:

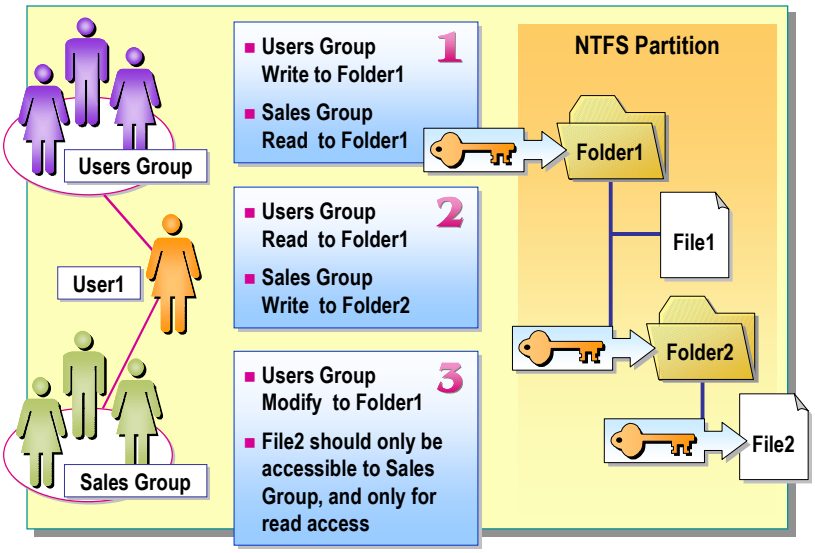
- When you move a folder or file within an NTFS partition, the folder or file retains its original permissions.
- When you move a folder or file between NTFS partitions, the folder or file inherits the permissions of the destination folder. When you move a folder or file between partitions, you actually copy the folder or file to the new location and then delete it from the old location.
- When you move files or folders to non-NTFS partitions, the folders and files lose their NTFS permissions, because non-NTFS partitions do not support NTFS permissions.

To move files and folders within an NTFS partition or between NTFS partitions, you must have both Write permission for the destination folder and Modify permission for the source folder or file. The Modify permission is required to move a folder or file because Windows 2000 removes the folder or file from the source folder after it copies it to the destination folder.

Class Discussion: Applying NTFS Permissions

Topic Objective
To reinforce students' understanding of how Windows 2000 applies NTFS permissions to files and folders.

Lead-in
Let's look at some examples of the results of applying NTFS permissions to files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

User1 is a member of the Users group and the Sales group.

1. The Users group has Write permission and the Sales group has Read permission for Folder1. What permissions does User1 have for Folder1?

   User1 has Write and Read permissions for Folder1, because User1 is a member of the Users group, which has Write permission, and the Sales group, which has Read permission.

2. The Users group has Read permission for Folder1. The Sales group has Write permission for Folder2. What permissions does User1 have for File2?

   User1 has Read and Write permissions for File2, because User1 is a member of the Users group, which has Read permission to Folder1, and the Sales group, which has Write permission to Folder2. File2 inherits permissions from both Folder2 and Folder1.

3. The Users group has Modify permission for Folder1. File2 should only be accessible to the Sales group, and only for reading. What steps should you take to ensure that the Sales group has only Read permission for File2?

   Disable permissions inheritance for Folder2 or File2. Remove permissions for Folder2 or File2 that Folder2 has inherited from Folder1. Grant only the Read permission to the Sales group for Folder2 or File2.

Using NTFS Permissions

Topic Objective
To introduce the topics related to using NTFS permissions.

Lead-in
Administrators and owners of files and folders control access to files and folders.

- Granting NTFS Permissions
- Setting Permission Inheritance
- Best Practices for Granting NTFS Permissions

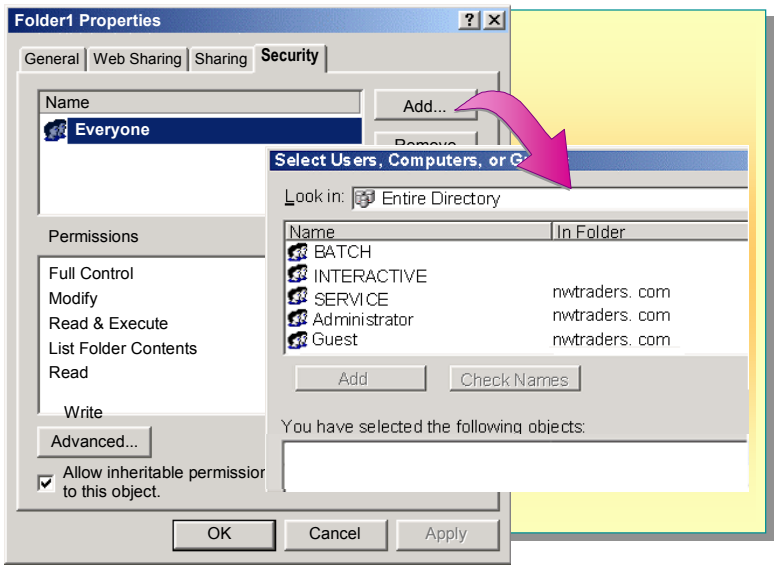
**********ILLEGAL FOR NON-TRAINER USE**********

Administrators, users with the Full Control permission, and owners of files or folders can grant permissions to user accounts and groups for file and folders. When granting NTFS permissions and controlling inheritance, you should follow best practices to help you grant permissions in the most effective manner. You should always grant permissions according to the needs of your groups and users.

Granting NTFS Permissions

Topic Objective
To illustrate how to grant NTFS permissions.

Lead-in
By default, Windows 2000 grants the Full Control permission when you create a file or folder or when you format a partition with NTFS.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate granting permissions to a folder. Then demonstrate blocking permissions inheritance for a file that is contained in the folder. Finally, grant new permissions for the file on which you blocked permissions inheritance.

You grant NTFS permissions in the **Properties** dialog box for the folder. When you grant or modify NTFS permissions for a file or a folder, you can either add or remove users, groups, or computers for the file or folder. By selecting a user or group, you can modify the permissions for the user or group.

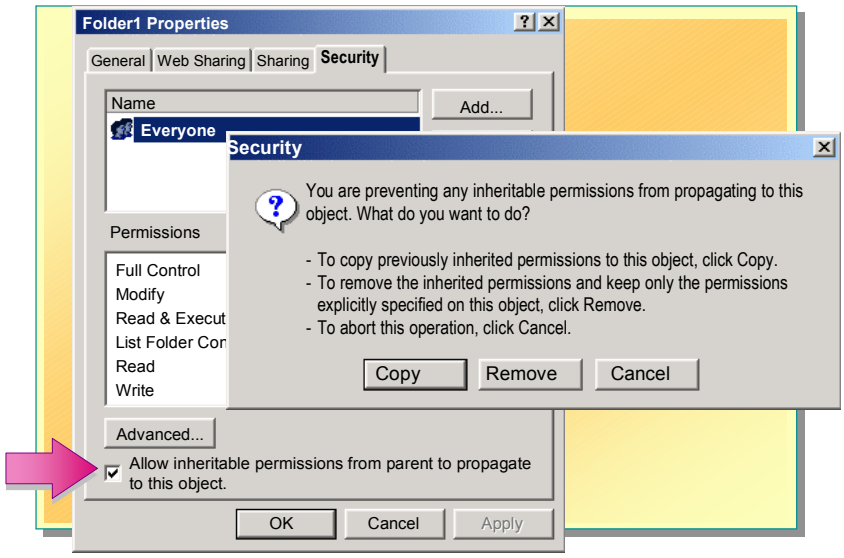
On the **Security** tab of the **Properties** dialog box for the file or folder, configure the options described in the following table.

Option	Description
Name	Selects the user account or group for which you want to change permissions or that you want to remove from the list.
Permissions	Allows a permission when you select the **Allow** check box.
	Denies a permission when you select the **Deny** check box.
Add	Opens the **Select User, Groups, or Computers** dialog box, which you use to select user accounts and groups to add to the **Name** list.
Remove	Removes the selected user account or group and the associated permissions for the file or folder.

Setting Permission Inheritance

Topic Objective
To illustrate how to control permissions inheritance.

Lead-in
By default, the permissions that you grant for a folder are inherited by the subfolders and files contained within.



**********ILLEGAL FOR NON-TRAINER USE**********

In general, you should allow Windows 2000 to propagate permissions from a parent folder to subfolders and files contained in the parent folder. Permissions propagation simplifies the assignment of permissions for resources.

However, there are times when you may want to prevent permission inheritance. For example, you may need to keep all sales department files in one sales folder for which everyone in the sales department has the Write permission. However, you need to limit permissions for a few files in the folder to the Read permission only. To do this, you would prevent inheritance so that the Write permission does not propagate to the files contained in the folder.

By default, subfolders and files inherit permissions that you grant for their parent folders, as shown on the **Security** tab in the **Properties** dialog box when the **Allow inheritable permissions from parent to propagate to this object** check box is selected.

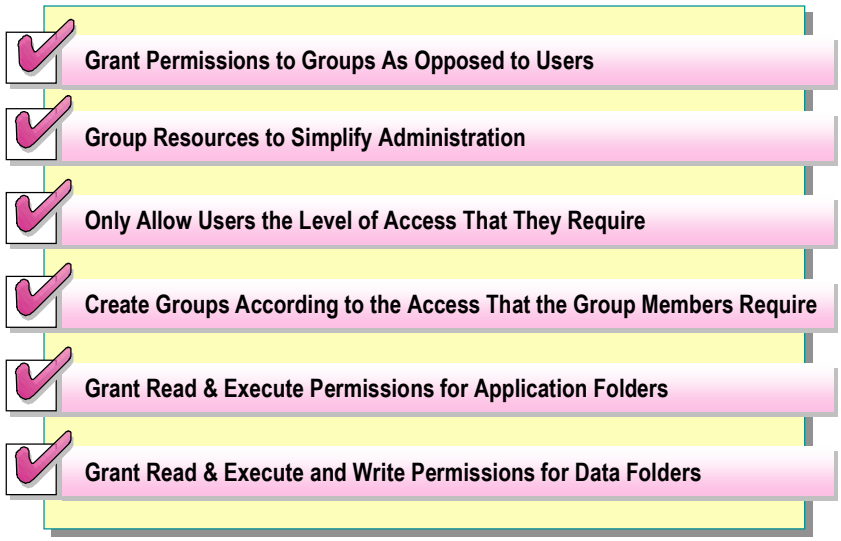
To prevent a subfolder or file from inheriting permissions from a parent folder, clear the **Allow inheritable permissions from parent to propagate to this object** check box, and then select one of the two options described in the following table.

Option	Description
Copy	Copies previously inherited permissions from the parent folder to the subfolder or file and denies subsequent permissions inheritance from the parent folder.
Remove	Removes the inherited permission that is granted for the parent folder from the subfolder or file and retains only the permissions that you explicitly grant for the subfolder or file.

Best Practices for Granting NTFS Permissions

Topic Objective
To provide best practices for granting NTFS permissions.

Lead-in
Consider these guidelines when granting NTFS permissions.



**********ILLEGAL FOR NON-TRAINER USE**********

Consider the following best practices when granting NTFS permissions:

- Grant permissions to groups as opposed to users. It is easier to manage groups than users. This keeps the ACL short, which increases performance.
- To simplify administration, group files into application folders where commonly used applications are kept, data folders containing data files shared by multiple users, and home folders that contain each individual user's files. Centralize home folders and data folders on a separate partition.
- Only allow users the level of access that they require. If a user only needs to read a file, grant the user, or group to which the user has been added, the Read permission for the file.
- Create groups according to the access that the group members require for resources, and then grant the appropriate permissions to the groups.
- When you grant permissions for application folders, grant the Read & Execute permission to the Users and Administrators groups. This prevents data and application files from being accidentally deleted or damaged by users or viruses.
- When you grant permissions for data folders, grant the Read & Execute and Write permissions to the Users group and the Full Control permission to the Owner. This gives users the ability to read and modify documents that other users create, and the ability to read, modify, and delete the files and folders that they themselves create.

Note You should use Deny permissions only when it is essential to deny access to a specific user account or group.

Using Special NTFS Permissions

Topic Objective
To identify the topics related to granting special NTFS permission.

Lead-in
The standard NTFS permissions generally provide all of the access control that you need to secure your resources, but if you need more specific levels of access, you can use NTFS special access permissions.

- Introduction to Special NTFS Permissions
- Granting Special NTFS Permissions

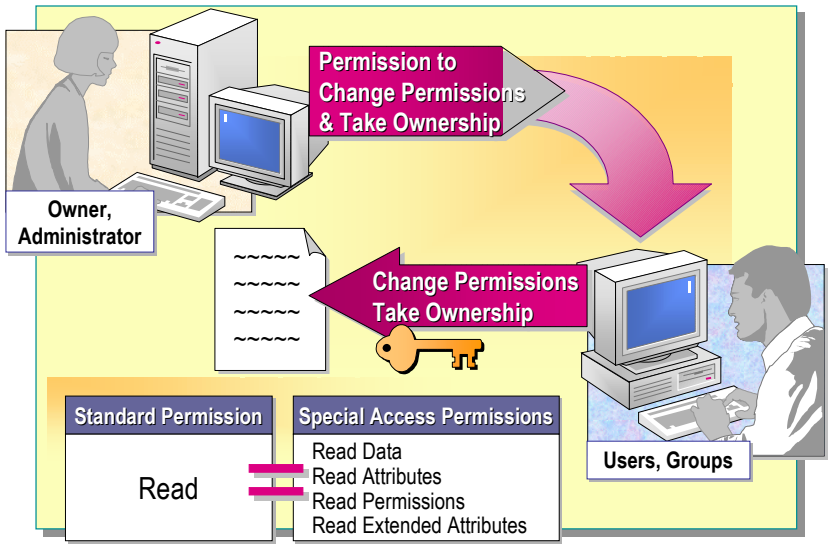
**********ILLEGAL FOR NON-TRAINER USE**********

The standard NTFS permissions generally provide all of the access control that you need to secure your resources. However, there are instances when the standard NTFS permissions will not provide the specific level of access that you may want to grant to users. To create a specific level of access, you grant NTFS special access permissions.

Introduction to Special NTFS Permissions

Topic Objective
To illustrate special NTFS permissions.

Lead-in
Special access permissions provide you with a greater degree of control for granting access to resources.



**********ILLEGAL FOR NON-TRAINER USE**********

Special access permissions provide you with a greater degree of control for granting access to resources. The 13 special access permissions, when combined, constitute the standard NTFS permissions. For example, the standard Read permission comprises the Read Data, Read Attributes, Read Permissions, and Read Extended Attributes special access permissions.

Two of the special access permissions are especially useful for managing access to files and folders:

- *Change Permissions*. Grant this permission to provide a user the ability to change permissions for a file or folder.
- *Take Ownership*. Grant this permission to provide a user the ability to take ownership of files and folders.

Change Permissions

You can give other administrators and users the ability to change permissions for a file or folder without giving them the Full Control permission over the file or folder. In this way, the administrator or user cannot delete or write to the file or folder, but can grant permissions to the file or folder.

To give administrators the ability to change permissions, grant Change Permissions for the file or folder to the Administrators group.

Take Ownership

You can transfer ownership of files and folders from one user account or group to another user account or group. You can also give someone the ability to take ownership or, as an administrator, you can take ownership of a file or folder.

The following rules apply for taking ownership of a file or folder:

- The current owner or any user with Full Control permission can grant the Full Control standard permission or the Take Ownership special access permission to another user account or group. This will allow the user account or a member of the group to take ownership.
- A member of the administrators group can take ownership of a folder or file, regardless of granted permissions for that folder or file. If an administrator takes ownership, the Administrators group becomes the owner, and any member of the Administrators group can change the permissions for the file or folder and grant the Take Ownership permission to another user account or group.

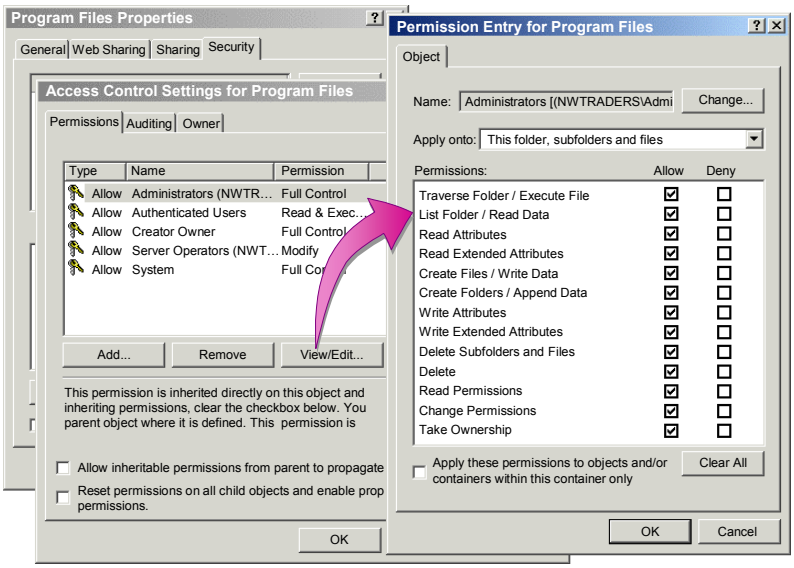
  For example, if an employee leaves the company, an administrator can take ownership of the employee's files and grant the Take Ownership permission to another employee, and then that employee can take ownership of the previous employee's files.

Note To become the owner of a file or folder, a user or group member with Take Ownership permission must explicitly take ownership of the file or folder. You cannot automatically grant anyone ownership of a file or folder. The owner of a file, a member of the administrators group, or anyone with Full Control permission can grant Take Ownership permission to a user account or group, which then allows them to take ownership.

Granting Special NTFS Permissions

Topic Objective
To illustrate the interface for granting permissions.

Lead-in
You can grant special access permissions to change file and folder permissions or take ownership of files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

To grant special access permissions to users and groups, perform the following steps:

1. In the **Properties** dialog box for a file or folder, on the **Security** tab, click the **Advanced** button.
2. In the **Access Control Settings** dialog box for the file or folder, on the **Permissions** tab, select the user account or group for which you want to apply NTFS special access permissions, and then click **View/Edit**.
3. In the **Permissions Entry** dialog box for the file or folder, configure the options that are described in the following table.

Option	Description
Name	Specify the user account or group name. To select a different user account or group, click **Change**.
Apply onto	Specify the level of the folder hierarchy at which the special NTFS permissions are inherited. The default is **This folder**, **subfolders and files**.
Permissions	Allow the special access permissions. To allow the Change Permissions or Take Ownership permissions, select the **Allow** check box next to each.
Apply these permissions to objects and/or containers within this container only	Specify whether subfolders and files within a folder inherit the special access permissions from the folder. Select this check box to propagate the special access permissions to files and subfolders. Clear this check box to prevent permission inheritance.
Clear All	Click this button to clear all selected permissions.

Lab A: Using NTFS Permissions

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will use NTFS permissions to control access to files and folders.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Assign NTFS file system folder and file permissions to user accounts and groups.
- Test NTFS folder and file permissions.
- Explain what happens to permissions when you copy and move folders and files on NTFS partitions and non-NTFS partitions.

Prerequisites

Before working on this lab, you must have:

- Knowledge of users and groups in Windows 2000.
- Knowledge of the difference between a workgroup and a domain.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.

Estimated time to complete this lab: 30 minutes

Exercise 1
Assigning NTFS Permissions

Scenario

Corporate policy dictates that you must remove the default NTFS permissions from NTFS files and folders and assign permissions based on the permissions needed by the groups and users in your company. You are setting up a server that will contain files and folders that users will need to gain access to across the network. You have created the folder structure and you now need to assign the proper permissions. You have a data folder into which users will be saving their work. Users need to have the ability to save and modify their own work but not to change files that belong to other users. You also want to ensure that only authorized users on the network can gain access to the folder.

Goal

In this exercise, you will remove the default NTFS permissions from the Data folder and provide permissions as instructed. You will then test those permission assignments.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and remove the default permissions from the Data folder by blocking inheritance.	**a.** Log on using the following information: Username: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, navigate to C:\MOC\Win2152b\Labfiles\Lab06, and then open the **Properties** dialog box for the Data folder. **c.** In the **Data Properties** dialog box, on the **Security** tab, view the permissions for the Data folder.
What are the existing folder permissions, and why are they shaded? **The Everyone group has Full Control. The permissions are shaded, indicating that the permissions are inherited from the parent folder.**	
1. (*continued*)	**d.** Under **Name**, click **Everyone**, and then click **Remove**. *A message appears, indicating that you cannot remove the Everyone group because the object is inheriting permissions from its parent.* **e.** Click **OK** to close the message. **f.** Clear the **Allow inheritable permissions from parent to propagate to this object** check box to prevent permission inheritance. *A message appears, prompting you to copy the currently inherited permissions to the folder or to remove all permissions for the folder except those that you explicitly specify.*

Tasks	Detailed Steps
1. (*continued*)	**g.** In the **Security** dialog box, click **Remove**.
2. Assign permissions to the Users group for the Data folder.	**a.** In the **Data Properties** dialog box, click **Add**. **b.** In the **Select Users, Computers, or Groups** dialog box, in the **Look in** box, verify that **nwtraders.msft** appears. **c.** Under **Name**, click **Domain Users**, click **Add**, and then click **OK**.

What are the existing allowed folder permissions?

The Domain Users group has the Read & Execute, List Folder Contents, and Read permissions. These are the default permissions that Windows 2000 assigns when you add a user account or group to the list of permissions.

2. (*continued*)	**d.** In the **Data Properties** dialog box, verify that **Domain Users** is selected, and then allow the Write permission.

How do you give users the ability to modify only the files that they created?

You assign the Full Control permissions to the Creator Owner group. This way, any file that a user creates in the folder will be owned by that user and given Full Control.

3. Assign Full Control permissions to the Creator Owner group for the Data folder.	**a.** In the **Data Properties** dialog box, click **Add**. **b.** In the **Select Users, Groups, or Computers** dialog box, in the **Look in** box, verify that **nwtraders.msft** appears. **c.** Under **Name**, click **Creator Owner**, click **Add**, and then click **OK**. **d.** In the **Data Properties** dialog box, verify that **Creator Owner** is selected, and then allow the Full Control permission.
4. Assign Full Control permissions to the local Administrators group for the Data folder and create a file called Admin.txt.	**a.** In the **Data Properties** dialog box, click **Add**. **b.** In the **Select Users, Groups, or Computers** dialog box, in the **Look in** box, click *Server* (where *Server* is your assigned computer name). **c.** Under **Name**, click **Administrators**, click **Add**, and then click **OK**. **d.** In the **Data Properties** dialog box, verify that **Administrators** is selected, and then allow the Full Control permission. **e.** Click **OK** to close the **Data Properties** dialog box.

Tasks	Detailed Steps
4. (*continued*)	**f.** In the C:\MOC\Win2152b\Labfiles\Lab06\Data folder, create a text file named Admin.txt. This text file will be used to test permissions. **g.** Close any open windows, and then log off.
5. Log on to nwtraders as Student*x* (where *x* is your assigned student number) with the password of **domain** and test the folder permissions that you assigned for the Data folder.	**a.** Log on using the following information: Username: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on from: **nwtraders** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab06\Data folder. **c.** In the Data folder, attempt to create a text file named Student.txt.

Were you successful? Why or why not?

Yes, because the Users group is assigned the Write permission for the Data folder.

5. (*continued*)	**d.** Attempt to perform the following tasks on the file that you just created, noting which tasks you are able to complete. • Open the file • Modify the file • Save the file • Delete the file

Were you successful?

Yes. The tasks that you can complete are opening, modifying, saving, and deleting the file because Creator Owner has been assigned the NTFS Full Control permission for the Data folder.

5. (*continued*)	**e.** Attempt to perform the following tasks on the Admin.txt file, noting which tasks you are able to complete. • Open the file • Modify the file • Save the file • Delete the file

Tasks	Detailed Steps
Were you successful? **Partially successful. The tasks that you can complete are opening, modifying, and saving the file, but you cannot delete the file. This is because you are logged on as a member of Domain Users, which is a member of the Users group. The Users group has been assigned the NTFS Read & Execute, List Folder Contents, Read, and Write permissions for the Data folder. Files that are created in the folder inherit these folder permissions. Therefore, Student*x* can only read and modify the file that the administrator created.**	
5. (*continued*)	**f.** Close all open windows, and then log off.

Compressing Data on an NTFS Partition

Topic Objective
To introduce the topics related to NTFS data compression management.

Lead-in
You compress files and folders so that they occupy less space on a partition.

- Introduction to Compressed Files and Folders
- Compressing Files and Folders
- Copying and Moving Compressed Files and Folders
- Best Practices for Compressing Data

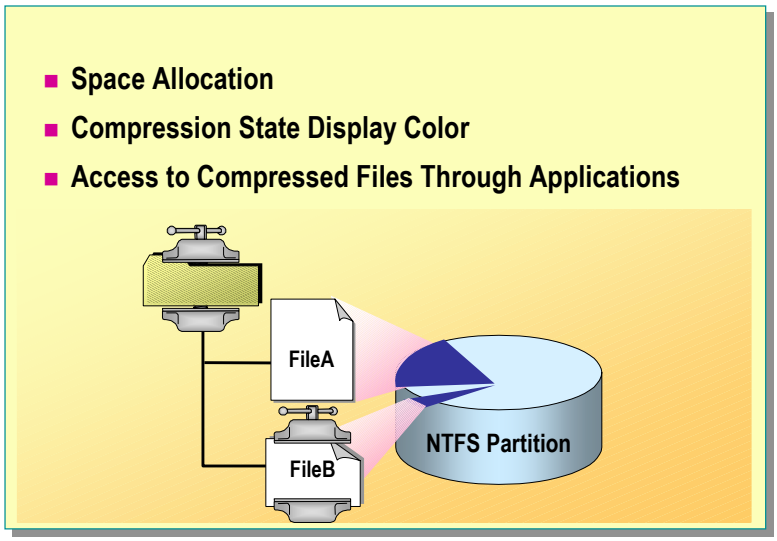
**********ILLEGAL FOR NON-TRAINER USE**********

NTFS file system data compression enables you to compress files and folders. Compressed files and folders occupy less space on an NTFS-formatted partition, enabling you to store more data. You set the compression state, either compressed or uncompressed, of files and folders. Files and folders that you copy or move can retain their compression states, or they can inherit the compression state of the target folder to which they are copied or moved. You should follow the best practices for managing data compression.

Introduction to Compressed Files and Folders

Topic Objective
To illustrate the concept of compressed files and folders.

Lead-in
Compressed files and folders occupy less space on NTFS-formatted partitions.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
NTFS allocates space for compressed files and folders based on the uncompressed size of the file or folder when it is copied or moved.

Each file and folder on an NTFS partition has a compression state, which is either *compressed* or *uncompressed*. The compression state for a folder does not necessarily reflect the compression state of the files and subfolders in that folder. For example, a folder can be compressed, yet all of the files in that folder can be uncompressed. Note that an uncompressed folder can contain compressed files.

Consider the following when working with compressed files or folders:

- Space allocation

  NTFS allocates disk space based on the uncompressed file size. If you copy a compressed file to an NTFS partition that does not have enough space for the uncompressed file, you will get an error message stating that there is not enough disk space for the file.

- Compression state display color

  You can change the color that displays compressed files and folders in order to distinguish them from uncompressed files and folders.

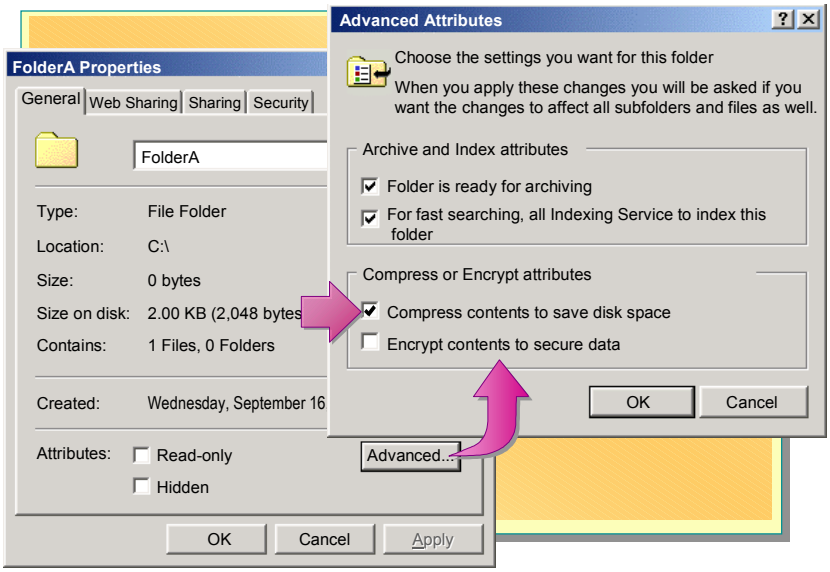
- Access to compressed files through applications

  Compressed files can be read, and written to, by any Windows-based or MS-DOS®-based application without first being uncompressed by another program. When an application or an operating system command requests access to a compressed file, Windows 2000 automatically uncompresses the file. When you close or save a file, Windows 2000 compresses it again.

Compressing Files and Folders

Topic Objective
To describe how to compress files and folders.

Lead-in
By using Windows Explorer you can set the compression state for files and folders and change the display color for compressed files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Show students how to set the compression state for a folder.

Show students how to set an alternate display color for compressed folders and files.

Windows Explorer enables you to set the compression state of files and folders and change the display color for compressed files and folders.

Note You cannot compress a file or folder if it is encrypted. If the **Encrypt contents to secure data** check box is selected, you cannot compress the file or folder.

Setting Compression State

To set the compression state of a folder or file, in the **Advanced attributes** dialog box, select the **Compress contents to save disk space** check box.

If you compress a folder, Windows 2000 displays the **Confirm Attribute Changes** dialog box, which has the two additional options. These options are described in the following table.

Option	Description
Apply changes to this folder only	Compresses only the folder that you have selected and any files or folders added to it
Apply changes to this folder, subfolders and files	Compresses the folder and all subfolders and files that are contained within it and added to it

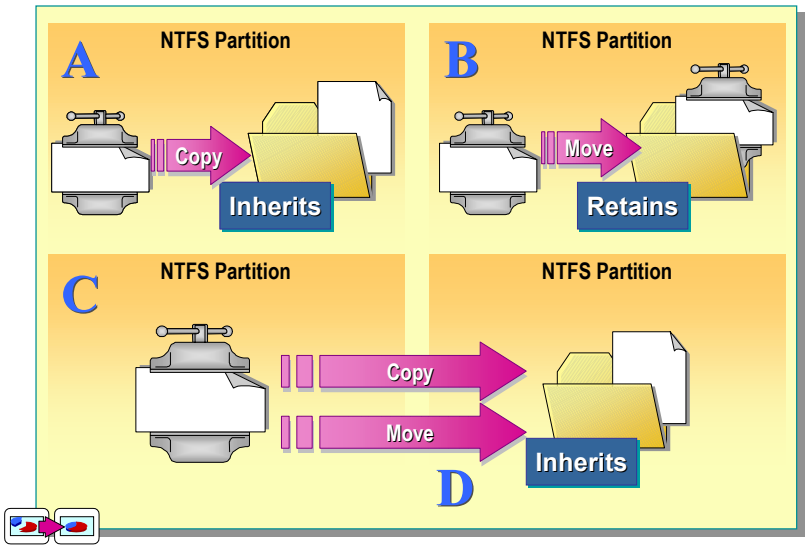
Changing Display Color

You can set an alternate display color for compressed files and folders. In Windows Explorer, on the **Tools** menu, click **Folder Options**. On the **View** tab, select the **Display compressed files and folders with alternate color** check box.

Copying and Moving Compressed Files and Folders

Topic Objective
To explain compression of files and folders that are copied and moved within and between partitions.

Lead-in
Certain rules determine whether the compression state of files and folders is retained when you copy or move them within and between NTFS and non-NTFS partitions.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic is animated. Begin by explaining to students how the compression state of a file inherits the compression state of the target folder.

Key Points
Moving a file or folder from one NTFS partition to another is treated as a copy and then a delete.

NTFS compression is not supported on non-NTFS partitions. Windows 2000 automatically uncompresses compressed files that you move or copy to a non-NTFS partition.

The following list describes how Windows 2000 treats the compression state of a file or folder when you copy or move a compressed file or folder within or between NTFS partitions, or between NTFS and non-NTFS partitions:

- As shown in section A of in the illustration, when you copy a file or folder within an NTFS partition, the file inherits the compression state of the target folder. For example, if you copy a compressed file or folder to an uncompressed folder, the file or folder is automatically uncompressed.
- As shown in section B of the illustration, when you move a file or folder within an NTFS partition, the file or folder retains its original compression state. For example, if you move a compressed file to an uncompressed folder, the file remains compressed.
- As shown in section C of the illustration, when you copy a file or folder between NTFS partitions, the file or folder inherits the compression state of the target folder.
- As shown in section D of the illustration, when you move a file or folder between NTFS partitions, the file or folder inherits the compression state of the target folder. Because Windows 2000 treats a move between partitions as a copy and then a delete, the files inherit the compression state of the target folder.

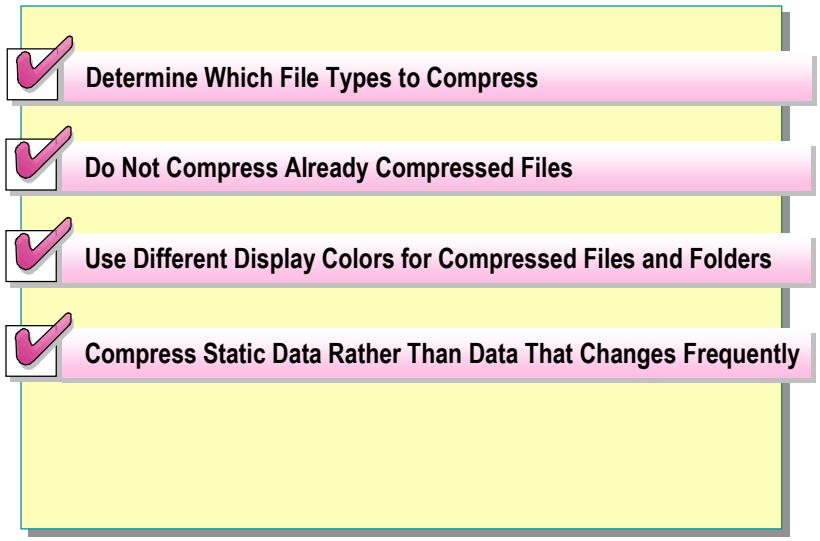
Important Windows 2000 supports compression only for NTFS partitions. When you move or copy a compressed file or folder to a non-NTFS partition or disk, Windows 2000 automatically uncompresses the file or folder.

Note When you copy a compressed file, Windows 2000 uncompresses the file, copies the file, and then compresses the file again as a new file. This may cause performance degradation.

Best Practices for Compressing Data

Topic Objective
To present best practices for managing NTFS compression.

Lead-in
Review this checklist before you compress files and folders on NTFS partitions.



**********ILLEGAL FOR NON-TRAINER USE**********

Consider the following best practices for managing compression on NTFS partitions:

- Because some file types compress to smaller sizes than others, select file types to compress based on the resulting anticipated file size. For example, because Windows bitmap files contain more redundant data than application executable files, this file type compresses to a smaller size. Bitmaps will often compress to less than 50 percent of the original file size, while application files rarely compress to less than 75 percent of the original size.
- Do not compress already compressed files. Windows 2000 will attempt to compress the file even more, wasting system time and yielding no additional disk space.
- To make it easier to locate compressed data, use different display colors for compressed folders and files.
- Compress static data rather than data that changes frequently. Compressing and uncompressing files incurs some system overhead. By choosing to compress files that are accessed infrequently, you minimize the amount of system time that is dedicated to compression and uncompression activities.

Configuring Disk Quotas on NTFS Partitions

Topic Objective
To identify the topics related to configuring disk quotas on NTFS partitions.

Lead-in
Use disk quotas to manage increased requirements for data storage.

- **Using Disk Quotas**
- **Setting Disk Quotas**

**********ILLEGAL FOR NON-TRAINER USE**********

Use disk quotas to manage storage growth in distributed environments. Disk quotas allow you to allocate available disk space to users based on the files and folders that they own. Disk quotas allow you to control the amount of disk space users have for storing files. It is important that you have an understanding of how disk quotas work so that you can implement them in your network in an efficient manner.

Using Disk Quotas

Topic Objective
To identify types of disk quotas.

Lead-in
Disk quotas allow you to monitor and control the amount of disk space being used. You can set warning thresholds to log an event when users are approaching their limit.

- **Usage Calculation Based on File and Folder Ownership**
- **Compression Ignored When Calculating Usage**
- **Free Space for Applications Based on Quota Limit**
- **Disk Quotas Tracked for Each NTFS Partition**

**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 disk quotas track and control disk space usage on a per-user, per-partition basis. As such, Windows 2000 tracks every user's disk space regardless of the folder in which they store files. The following list describes the characteristics of Windows 2000 disk quotas:

- Disk usage is based on file and folder ownership. When a user copies or saves a new file to an NTFS partition or takes ownership of a file on an NTFS partition, Windows 2000 charges the disk space for the file against the user's quota limit.
- Disk quotas do not use disk compression. Users are charged for each uncompressed byte, regardless of how much hard disk space is actually used. One reason for this is that file compression produces different degrees of compression for different types of files.
- Free space for applications is based on the quota limit. When you enable disk quotas, the free space that Windows 2000 reports to applications for the partition is the amount of space remaining within the user's disk quota limit.
- Windows 2000 tracks disk quotas independently for each NTFS partition, even if the partitions reside on the same physical hard disk.

Important Apply disk quotas only to partitions that are formatted under the NTFS file system in Windows 2000.

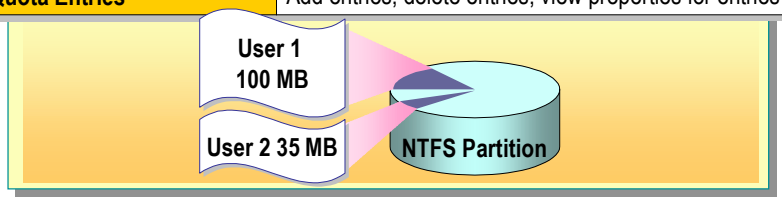
In order to control the amount of disk space users have available for storing files, set a disk quota warning to specify when Windows 2000 should log an event, indicating that the user is nearing the specified limit. Enforce disk quota limits and deny users access if they exceed their limit, or override the disk quota and allow them continued access.

Setting Disk Quotas

Topic Objective
To illustrate the options for setting disk quotas.

Lead-in
You can configure disk quotas to enforce quota limits for all users and for individual users.

Option	Description
Enable quota management	Enable disk quota management
Deny disk space to users exceeding quota limit	Users cannot write to volume when they exceed their hard disk space allocation
Do not limit disk usage	No hard disk space limit for users
Limit disk space to	Specify amount of disk space users can use
Set warning level to	Specify amount of disk space users can fill before event is logged
Quota Entries	Add entries, delete entries, view properties for entries



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to enable disk quotas for all users. Then demonstrate how to enable disk quotas for one user.

You can configure disk quotas to enforce disk quota warnings and limits for all users and for individual users.

Enabling Disk Quotas

To enable disk quotas, open the **Properties** dialog box for a disk. On the **Quota** tab, configure the options that are described in the following table.

Option	Description
Enable quota management	Select this check box to activate disk quota management for the disk.
Deny disk space to users exceeding quota limit	Select this check box so that users receive an **Out of disk space** message and are prohibited from writing to the disk when they exceed their hard disk space allocation.
Do not limit disk usage	Select this option when you do not want to limit the amount of hard disk space for users.
Limit disk space to	Configure the amount of disk space that is available to users.
Set warning level to	Configure the amount of disk space that is available to a user before Windows 2000 logs an event to indicate that the user is nearing his or her limit.
Quota Entries	Click this button to add a new entry, delete an entry, and view the properties for a quota entry.

Enforcing Disk Quotas for All Users

To enforce quota limits for all users, perform the following steps:

1. In the **Limit disk space to** and **Set warning level to** boxes, enter the values for the limit and warning level that you want to set.
2. Select the **Deny disk space to users exceeding quota limit** check box.

   Windows 2000 will monitor usage and will not allow users to create files or folders on the partition when they exceed the limit.

Enforcing Disk Quotas for Individuals

To enforce quota limits for a specific user, perform the following steps:

1. In the **Properties** dialog box for a disk, on the **Quota** tab, click the **Quota Entries** button.
2. In the **Quota Entries for** dialog box, create an entry by clicking **New Quota Entry** on the **Quota** menu, and then selecting a user.

Configure the disk space limit and the warning level for the individual user.

Lab B: Configuring Disk Compression and Quotas

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will configure disk compression and quotas.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure an NTFS volume for compression.
- Assign disk quotas for a user account.

Prerequisites

Before working on this lab, you must have:

- Knowledge of the NTFS file system.
- Knowledge of the difference between a workgroup and a domain.
- Knowledge of assigning quotas on a NTFS file system.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server.

Estimated time to complete this lab: 30 minutes

Exercise 1
Configuring Disk Compression

Scenario

To provide the maximum storage capacity for your network, the IT manager has decided that NTFS disk compression will be enabled for data folders on all member servers. You have been tasked with enabling disk compression for specified folders on your member server.

Goal

In this exercise, you will enable disk compression and view the effects of compression on the Inetpub folder and subfolders.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with the password of **domain** and configure Windows Explorer to display compressed files and folders in another color.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, on the **Tools** menu, click **Folder Options**. **c.** In the **Folder Options** dialog box, on the **View** tab, select the **Display compressed files and folders with alternate color** check box, and then click **OK**.
2. Compress the Inetpub folder hierarchy.	**a.** In the console tree, expand **Local Disk (C:)**, right-click **Inetpub**, and then click **Properties**.
What are the **Size** and **Size on disk** values for the Inetpub folder? **Answers will vary.**	
2. (*continued*)	**b.** In the **Inetpub Properties** dialog box, click **Advanced**. **c.** In the **Advanced Attributes** dialog box, under **Compress or Encrypt attributes**, select the **Compress contents to save disk space** check box, and then click **OK**. **d.** Click **OK** to close the **Inetpub Properties** dialog box. **e.** In the **Confirm Attribute Changes** dialog box, click **Apply changes to this folder, subfolders and files**, and then click **OK**. *In the console tree, the Inetpub folder appears in a different color.* **f.** Open the **Properties** dialog box for the Inetpub folder.

Tasks	Detailed Steps
What are the **Size** and **Size of disk** values for the Inetpub folder? How much disk space does using disk compression save? (Hint: compare the values recorded before disk compression was enabled with the values after disk compression was enabled.) **Answers will vary.**	
2. (*continued*)	**g.** Click **OK** to close the **Inetpub Properties** dialog box.

Exercise 2
Assigning Disk Quotas

Scenario

The users on your network store files on your server, and most of them have not been trained in proper disk storage space management. Therefore, your server is always running out of disk space. The IT managers for your department want you to limit the amount of disk space on your server that is available to users. You must enable disk quotas on your server and limit storage space to 10 MB per user. When the users have used 60 percent of their allotted storage space, you want them to receive a message indicating that they are close to exceeding their allotted storage space.

Goal

In this exercise, you will enable the disk quota system on the drive C: partition, and then create a console containing the Local User Manager snap-in. You will then use Local User Manager to enable the guest account to which you will assign a disk quota.

Tasks	Detailed Steps
1. Configure default quota management settings for drive C. Disk Space Limit: **10 MB** Disk Space Warning: **6 MB**	**a.** In Windows Explorer, display the **Properties** dialog box for Local Disk (C:). **b.** In the **Local Disk (C:) Properties** dialog box, on the **Quota** tab, select the **Enable quota management** and the **Deny disk space to users exceeding quota limit** check boxes. **c.** Under **Select the default quota limit for new users on this volume**, verify that **Limit disk space to** is selected. **d.** In the **Limit disk space to** box, type **10** and then change the unit size to MB. **e.** In the **Set warning level to** box, type **6** and then change the unit size to MB. **f.** Click **Apply**. *A message appears, warning you that the volume will be rescanned if you enable quotas.* **g.** Click **OK**, and then click **Quota Entries**. **h.** On the **Quota** menu, click **New Quota Entry**. **i.** In the **Select Users** dialog box, in the **Look in** box, click *Server* (where *Server* is your assigned computer name). **j.** Under **Name**, click **QuotaUser**, click **Add**, and then click **OK** to close the **Select Users** dialog box. *The **Add New Quota Entry** dialog box appears. Notice that the quota limits that you set for drive C have been applied.* **k.** Click **OK** to close the **Add New Quota Entry** dialog box. **l.** Close the **Quota Entries for Local Disk (C:)** window. **m.** Click **OK** to close the **Local Disk (C:) Properties** dialog box. **n.** Close any open windows, and then log off.

Exercise 3
Testing and Removing Quota Limits

Scenario

You have enabled disk quotas on your server and now need to test them to verify that they are operating as expected. To do this, you will set a quota limit and a warning level for the QuotaUser user account. You will then log on as that user and test the disk quota settings to ensure they are operating properly by copying enough data to the partition that you configured to exceed those limits.

Goal

In this exercise, you will test the quota settings for the QuotaUser account, and then remove the disk quota limits.

Tasks	Detailed Steps
1. Log on to *Server* (where *Server* is your assigned computer name) with the password of **password** and test quota limits for the QuotaUser account by viewing the free space on drive C. Copy the Program Files folder to the My Documents folder.	**a.** Log on using the following information: User name: **QuotaUser** Password: **password** Log on to: *Server* (where *Server* your assigned computer name) **b.** In Windows Explorer, in the console tree, click **Local Disk (C:)**.
How much free disk space is reported? Why? **Less than 10 MB. This indicates that the quota is working properly.**	
1. (*continued*)	**c.** Expand **Local Disk (C:)**, right-click **Program Files**, and then click **Properties**.
If disk quotas are working, will you be able to copy the entire Program Files folder logged on as QuotaUser? **No. The disk space required to copy the entire Program Files folder would exceed the quota limit for the QuotaUser user account.**	

Tasks	Detailed Steps
1. (*continued*)	**d.** In the console tree, click **OK** to close the **Program Files Properties** dialog box. **e.** Right-click **Program Files**, and then click **Copy**. **f.** In the console tree, right-click **My Documents**, and then click **Paste**. *A message appears, indicating that the copy process has begun. The **Error Copying File or Folder** message appears, indicating that there is not enough available disk space and instructing you to delete one or more files to make more disk space available.*
Why did you get this error message? **This is the error message that appears when there is not enough available space to continue the copy operation due to quota limits.**	
1. (*continued*)	**g.** Click **OK** to close the **Error Copying File or Folder** message. **h.** Close Windows Explorer, and then log off.
2. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of domain and disable quota management for drive C.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, in the console tree, right-click **Local Disk (C:)**, and then click **Properties**. **c.** On the **Quota** tab, clear the **Enable quota management** check box. *Notice that the quota settings for drive C are no longer available.* **d.** Click **Apply**. *The **Disk Quota** message appears, warning you that if you disable quotas, the volume will be rescanned if you enable them later.* **e.** Click **OK** to close the **Disk Quota** message. **f.** Click **OK** to close the **Local Disk (C:) Properties** dialog box. **g.** Close any open windows, and then log off.

Securing Data by Using EFS

Topic Objective
To introduce the topics related to recovering encrypted files.

Lead-in
EFS, built into the NTFS file system in Windows 2000, enables public key-based protection at the file or folder level.

- Introduction to EFS
- Encrypting a Folder or File
- Decrypting a Folder or File
- Recovering an Encrypted Folder or File

**********ILLEGAL FOR NON-TRAINER USE**********

The Encrypting File System (EFS) provides file-level encryption for NTFS files. EFS encryption technology is public key-based, runs as an integrated system service, and enables file recovery by a designated EFS recovery agent.

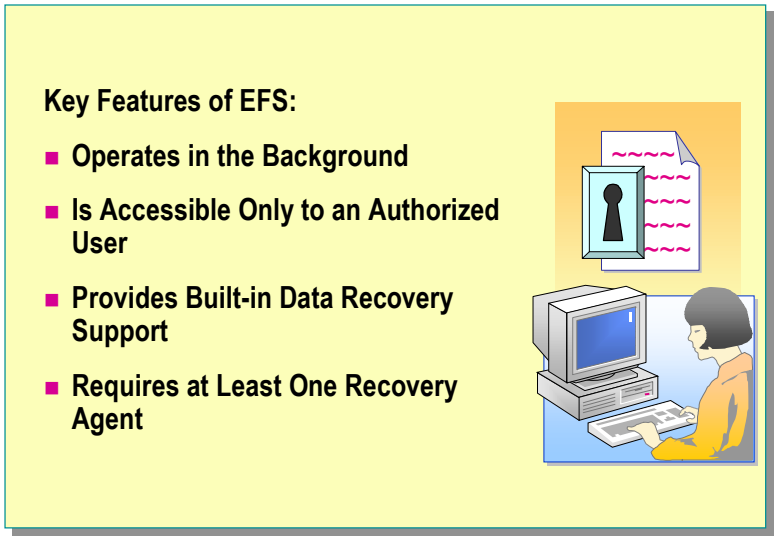
EFS is easy to manage because when it is necessary to gain access to critical data that a user has encrypted, and the user or his or her key is unavailable, the EFS recovery agent (typically an administrator) can decrypt the file.

Understanding the benefits of EFS will help you efficiently use this technology on your network.

Introduction to EFS

Topic Objective
To identify the key features of EFS.

Lead-in
EFS allows users to store their data on the hard disk in encrypted format.



**********ILLEGAL FOR NON-TRAINER USE**********

Briefly discuss the purpose and the process of encrypting and decrypting files and folders.

EFS allows users to store data on the hard disk in encrypted format. After a user encrypts a file, the file remains encrypted for as long as it is stored on disk. Individual users can use EFS to encrypt files for confidentiality.

EFS has several key features:

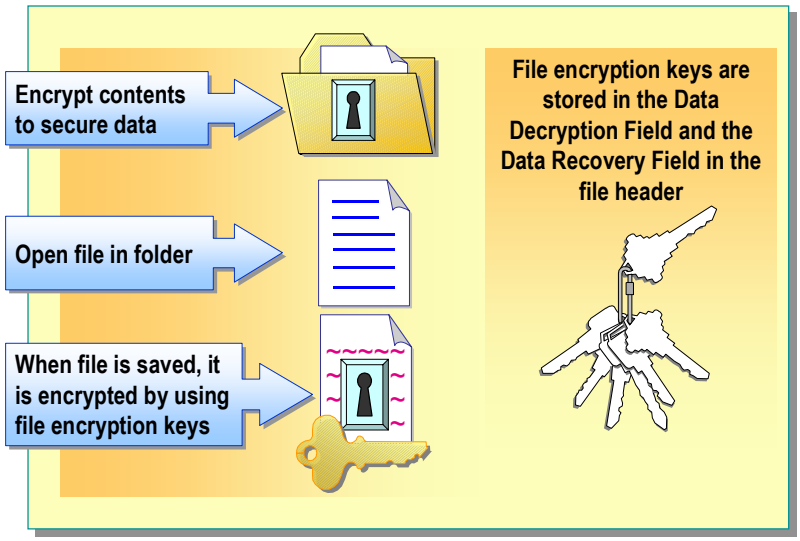
- It operates in the background and is transparent to users and applications.
- It allows only the authorized user to gain access to an encrypted file. EFS automatically decrypts the file for use and then encrypts the file again when it is saved. Administrators can recover data that was encrypted by another user. This ensures that data is accessible if the user that encrypted the data is unavailable or loses his or her private key.
- It provides built-in data recovery support. The Windows 2000 Server security infrastructure enforces the configuration of data recovery keys. You can use file encryption only if the local computer is configured with one or more recovery keys. EFS automatically generates recovery keys and saves them in the registry when access to the domain is not possible.
- It requires at least one recovery agent to recover encrypted files. You can designate multiple recovery agents to manage your EFS recovery program. Each recovery agent requires an EFS Recovery Agent certificate.

Note Encryption and compression are mutually exclusive. Therefore, it is recommended that you either encrypt or compress a file, but not both.

Encrypting a Folder or File

Topic Objective
To illustrate the procedure for encrypting files and folders on an NTFS partition.

Lead-in
A file is encrypted by using file encryption keys.



**********ILLEGAL FOR NON-TRAINER USE**********

To encrypt files or folders, create an NTFS folder, and then encrypt it in the **Properties** dialog box for the folder. On the **General** tab, click **Advanced**, and then click **Encrypt contents to secure data**.

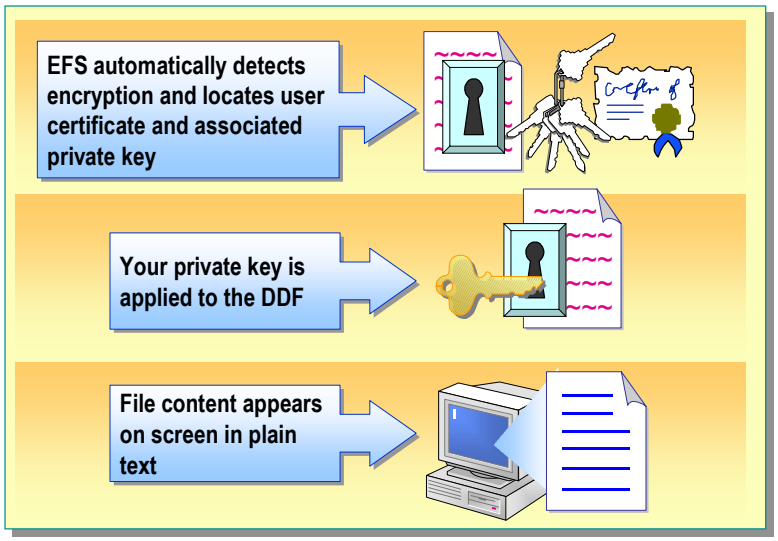
After you encrypt the folder, the files saved in that folder are automatically encrypted with file encryption keys. File encryption keys are fast, symmetric keys that are designed for bulk encryption. Windows 2000 encrypts the file in blocks, with a different file encryption key for each block. All of the file encryption keys are stored in the Data Decryption Field (DDF) and the Data Recovery Field (DRF) in the file header.

All files and subfolders that you create in an encrypted folder are also automatically encrypted. Each file has a unique encryption key, making it safe to rename files. If you move a file from an encrypted folder to an unencrypted folder on the same partition, the file remains encrypted.

Decrypting a Folder or File

Topic Objective
To describe the methodology for decrypting files and folders on an NTFS partition.

Lead-in
You can decrypt a folder or file on an NTFS partition by using your private key.



**********ILLEGAL FOR NON-TRAINER USE**********

When you open an encrypted file, EFS automatically detects an encrypted file and locates a user certificate and the associated private key in the file header. EFS applies your private key to the DDF to unlock the list of file encryption keys, allowing the file contents to appear in plain text.

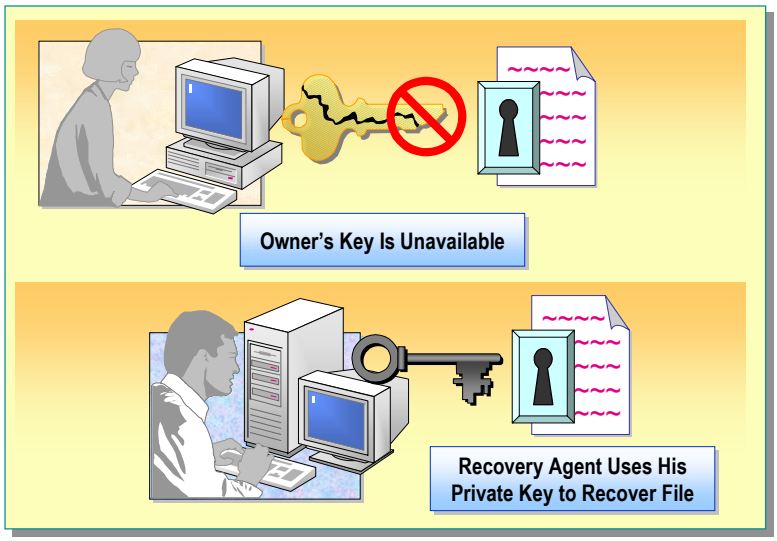
Access to the encrypted file is denied to everyone except the owner of the private key. Only the owner of the file or a recovery agent can decrypt the file. This is true even if administrators change permissions or file attributes, or take ownership of the file. Even if you own an encrypted file, you cannot read it unless you have the private key or you are a recovery agent.

Note You cannot share an encrypted file with other users.

Recovering an Encrypted Folder or File

Topic Objective
To explain the process of EFS recovery.

Lead-in
In the event of the owner losing the private key, the recovery agent can still recover the encrypted file.



**********ILLEGAL FOR NON-TRAINER USE**********

If the owner's private key is unavailable, recovery agent personnel can open the file by using his or her own private key, which is applied to the DRF to unlock the list of file encryption keys. If the recovery agent is using another computer on the network, you must send the file to the recovery agent. The recovery agent can bring his or her private key to the owner's computer, but copying a private key onto another computer is not a recommended security practice.

It is good security practice to rotate recovery agents. However, if the agent designation changes, then access to the file is denied. For this reason, it is recommended that you keep recovery certificates and private keys until all files that are encrypted with them have been updated.

To recover an encrypted file or folder as a designated recovery agent, perform the following steps:

1. Use Windows Backup or another backup tool to restore a user's backup version of the encrypted file or folder to the computer where your file recovery certificate is located.
2. In Windows Explorer, open the **Properties** dialog box for the file or folder. On the **General** tab, click **Advanced**.
3. Clear the **Encrypt contents to secure data** check box.
4. Make a backup version of the decrypted file or folder, and then return the backup version to the user.

Lab C: Securing Files by Using EFS

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will secure files by using EFS.

**********ILLEGAL FOR NON-TRAINER USE**********

Objectives

After completing this lab, you will be able to:

- Export the recovery agent's certificate.
- Encrypt files by using EFS.
- Import the recovery agent's certificate.
- Recover an encrypted file.

Prerequisites

Before working on this lab, you must have:

- Knowledge about how Windows 2000 secures files when using EFS.
- Knowledge about the role of a recovery agent and certificates in encrypting and decrypting files.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Server configured as a member server in the nwtraders.msft domain.
- A user account on your computer that is called EfsUser.
- The folder C:\MOC\Win2152b\Labfiles\Lab06\Efs, containing a file called Confidential.txt.
- A blank, formatted disk.

Estimated time to complete this lab: 15 minutes

Exercise 1
Securing the Recovery Agent Certificate

Scenario

Your company's security policy requires that your stand-alone servers use EFS to secure data. The security policy also requires you remove the recovery agent's certificate from all stand-alone computers that use EFS and to store the recovery keys in a secure location.

Goal

In this exercise, you will make your computer a stand-alone server and export the recovery agent certificate.

Tasks	Detailed Steps
1. Log on as Admin*x* (where *x* is your assigned student number) with the password of **domain** and make your computer a stand-alone server.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Control Panel, double click **System**. **c.** In the **System Properties** dialog box, on the **Network Identification** tab, click **Properties**. **d.** Under **Member of**, click **Workgroup**, in the **Workgroup** box type **Workgroup** and then click **OK**. **e.** In the **Network Identification** message, click **OK** twice. **f.** Click **OK** to close the **System Properties** dialog box. **g.** Close Control Panel. **h.** In the **System Settings Change** dialog box, click **Yes** to restart your computer.
2. Log on as Administrator with a password of **password** and export the file encryption certificate for Administrator to a disk.	**a.** Log on to your server using the following information: User name: **Administrator** Password: **password** **b.** Click **Start**, and then click **Run**. **c.** In the **Open** box, type **mmc** and then click **OK**. **d.** In the **Console1** window, on the **Console** menu, click **Add/Remove Snap-in**. **e.** In the **Add/Remove Snap-in** dialog box, click **Add**. **f.** In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**. **g.** In the **Certificates snap-in** dialog box, verify that **My user account** is selected, and then click **Finish**. **h.** Click **Close** to close the **Add Standalone Snap-in** dialog box, and then click **OK** to close the **Add/Remove Snap-in** dialog box *Certificates - Current User appears in the console tree.*

Tasks	Detailed Steps
2. (*continued*)	**i.** On the **Console** menu, click **Save As**. **j.** In the **Save As** dialog box, in the **Save in** box verify that **Administrative Tools** appears. **k.** In the **File name** box, type **Certificates** and then click **Save**. **l.** In the console tree, expand **Certificates - Current User**, expand **Personal**, and then click **Certificates**. **m.** In the details pane, right click **Administrator**, point to **All Tasks**, and then click **Export**. **n.** On the **Welcome to the Certificate Export Wizard** page, click **Next**. **o.** On the **Export Private Key** page, verify that **Yes, export the private key** is selected, and then click **Next**. **p.** On the **Export File Format** page, select the **Delete the private key if the export is successful** check box, and then click **Next**. **q.** On the **Password** page, in the **Password** and **Confirm password** boxes, type **password** and then click **Next**. **r.** On the **File to Export** page, in the **File name** box, type **a:\certificate** **s.** Insert a disk into the floppy disk drive, and then click **Next**. **t.** On the **Completing the Certificate Export Wizard** page, click **Finish**. **u.** In the **Certificate Export Wizard** message, click **OK**. **v.** Remove the disk from the floppy disk drive. **w.** Close Certificates, save the console settings, and then log off.

Exercise 2
Encrypting a File by Using the Encrypting File System (EFS)

Scenario

Your company's security policy requires you to encrypt confidential files so that only you can access them.

Goal

In this exercise, you will encrypt a file by using EFS.

Tasks	Detailed Steps
1. Log on as EfsUser with the password of **password** and encrypt the Confidential file in the C:\MOC\Win2152b\Labfiles\Lab06\Efs folder.	**a.** Log on using the following information: User name: **EfsUser** Password: **password** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab06\Efs folder, verify that you can read the contents of the Confidential.txt file, and then close Notepad. **c.** Display the **Properties** dialog box for the Confidential.txt file. **d.** On the **General** tab, click **Advanced**. **e.** In the **Advanced Attributes** dialog box, select the **Encrypt contents to secure data** check box, and then click **OK**. **f.** Click **OK** to close the **Confidential Properties** dialog box. **g.** In the **Encryption Warning** dialog box, click **Encrypt the file only**, and then click **OK**. **h.** Verify that you can still read the contents of the Confidential.txt file, and then close the Notepad. **i.** Close Windows Explorer, and then log off.

Exercise 3
Recover an Encrypted File by Using the Recovery Agent Certificate

Scenario

A user has left the company and you have deleted her user account. After deleting the account you realize that this user has encrypted a file that contains important company data. Your boss needs to gain access to this data.

Goal

In this exercise, you will import the recovery agent certificate and recover the encrypted file that contains the data your boss needs to gain access to.

Tasks	Detailed Steps
1. Log on as Administrator with the password of **password** and attempt to open the Confidential file in the C:\MOC\Win2152b\Labfiles\Lab06\Efs folder.	**a.** Log on using the following information: User name: **Administrator** Password: **password** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab06\Efs folder, and then attempt to read the contents of the Confidential.txt file.
Can you read the contents of Confidential.txt? Why or why not? **No. You cannot read the file's contents because another user encrypted the file.**	
1. (*continued*)	**c.** Click **OK**, close Notepad, and then minimize Windows Explorer.
2. Import the recovery agent's certificate and decrypt the Confidential file in the C:\MOC\Win2152b\Labfiles\Lab06\Efs folder.	**a.** Insert the disk containing the certificate file into the floppy disk drive. **b.** Open Certificates from the **Administrative Tools** menu. **c.** In the console tree, expand **Certificates – Current User** if necessary, right-click **Personal**, point to **All Tasks**, and then click **Import**. **d.** On the **Welcome to the Certificate Import Wizard** page, click **Next**. **e.** On the **File to Import** page, in the **File name** box, type **a:\certificate.pfx** and then click **Next**. **f.** On the **Password** page, in the **Password** box, type **password** and then click **Next**. **g.** On the **Certificate Store** page, click **Next**, and then on the **Completing the Certificate Import Wizard** page, click **Finish**.

Tasks	Detailed Steps
2. (*continued*)	**h.** In the **Certificate Import Wizard** message, click **OK**, and then close Certificates, saving the console settings if prompted. **i.** Restore Windows Explorer, and then attempt to read the contents of the Confidential.txt file.
Can you read the contents of Confidential? Why or why not? **Yes. You can read the file's contents because you are using the recovery agent certificate.**	
2. (*continued*)	**j.** Close Notepad, and then display the **Properties** dialog box for Confidential.txt. **k.** On the **General** tab, click **Advanced**. **l.** In the **Advanced Attributes** dialog box, clear the **Encrypt contents to secure data** check box, and then click **OK**. **m.** Click **OK** to close the **Confidential Properties** dialog box, and then close Windows Explorer.
3. Join the nwtraders.msft domain.	**a.** In Control Panel, double-click **System**. **b.** On the **Network Identification** tab, click **Properties**. **c.** Under **Member of**, click **Domain**, in the **Domain** box type **nwtraders.msft** and then click **OK**. **d.** In the **Domain Username and Password** dialog box, in the **Name** box, type **Admin***x* (where *x* is your assigned student number). **e.** In the **Password** box, type **domain** and then click **OK**. **f.** In the **Network Identification** message, click **OK** twice. **g.** Click **OK** to close the **System Properties** dialog box, and then close Control Panel. **h.** Remove the disk from the disk drive. **i.** In the **System Settings Change** dialog box, click **Yes** to restart your computer.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to NTFS Permissions
- How Windows 2000 Applies NTFS Permissions
- Using NTFS Permissions
- Using Special NTFS Permissions
- Compressing Data on an NTFS Partition
- Configuring Disk Quotas on NTFS Partitions
- Securing Data by Using EFS

**********ILLEGAL FOR NON-TRAINER USE**********

1. The Sales Manager was recently promoted to Vice President of Sales, and a regional sales manager was promoted to refill the position. The new Sales Manager needs ownership of the monthly sales report files. How can special NTFS permissions be used to transfer ownership of files to the new Sales Manager?

   The owner of the files can give the new sales manager the Take Ownership NTFS permission. This will allow the new sales manager to take ownership of the existing files.

2. You have a computer that several people use. What can you do to ensure that the authorized users for that computer can only access their own data files?

   You can convert the drive to NTFS, create a folder for each user, and then configure each folder's NTFS permissions so the users are the only ones with access their folder.

3. A user named JDRoland is a member of the Engineers group, the ENGManagers group, and the Users group. The NTFS permissions on the Drawings folder are:
   JDRoland – None
   Engineers – Full Control
   ENGManagers – Read
   Users – None
   What rights does JDRoland have in the Drawings folder? Why?

   Full Control. Though the user account does not provide any specific rights, the user account is a member of the Engineers group. Because NTFS permissions are cumulative, the JDRoland user account has Full Control.

4. You are configuring NTFS permissions on a folder and you notice that some of the **Permissions** check boxes are selected, but are shaded and you cannot clear them. Why is this and how would you clear them?

   The shaded Permissions check box indicates that the permissions are inherited from the parent folder. To change these rights, first remove the check from the Allow inheritable permissions from the parent to propagate to this object check box, remove the inherited rights, and then set permissions as desired.

5. You enabled disk compression on a folder named Archive and use it to store event logs and other historical data. Once a week, you move the files to the archive folder. After doing this several times, you notice that not all of the files are compressed. What could be causing this inconsistency?

   Some of the files you are moving are on the same partition as the Archive folder, and others are not. When you move files on the same partition, the files retains its attributes. When you move them from a different partition, the file inherits the attributes from the destination folder.

6. Your company uses a data center for centralized storage and control of corporate documents. Each user is allocated a certain amount of storage at the data center, and the user's department is charged a monthly fee for usage. In the past, the data center's strategy has been to partition the drives on the servers to configure each user's allocation. This creates problems when the allocations must be changed. The data center is going to be upgrading all of its servers to Windows 2000. Which feature of Windows 2000 will make setting the allocations easier?

   Windows 2000 supports disk quotas that allow administrators to dynamically change the quotas.

7. A user shares a computer with to other users. The user attempts to access a file on the computers local drive and receives an **Access denied** message. After verifying that the NTFS permissions allow the user Full Control. What is causing the denied access message to display and how can the user obtain access to the file?

   The file is encrypted using EFS. Only the individual who encrypted the file can decrypt the file. If a user needs access to the file the individual who encrypted the file must decrypt the file.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 7: Providing Network Access to File Resources

Contents

Overview	1
Introduction to Shared Folders	2
Creating Shared Folders	3
Combining NTFS and Shared Folder Permissions	13
Using Administrative Shared Folders	14
Publishing a Shared Folder in Active Directory	16
Lab A: Sharing and Securing Network Resources	17
Configuring Shared Folders by Using Dfs	25
Lab B: Configuring Domain-based Dfs	34
Review	40

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware.

Instructor Notes

Presentation:
75 Minutes

Labs:
60 Minutes

This module provides students with the knowledge and skill to set up shared folders and to control access to the folders through permissions. This includes combining shared folder permissions with NTFS file system permissions.

At the end of this module, students will be able to:

- Explain the purpose and use of shared folders.
- Create shared folders.
- Combine NTFS permissions and shared folder permissions.
- Use Administrative shared folders.
- Publish a folder in the Active Directory™ directory service.
- Configure shared folders by using Distributed file system (Dfs).

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft® PowerPoint® file 2152B_07.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Introduction to Shared Folders

  Present an overview of shared folders, including their purpose and benefits.

- Creating Shared Folders

  First, present the requirements for sharing a folder. Then, demonstrate sharing a folder while explaining the options. Next, present shared folder permissions. Emphasize that if there are conflicting permissions, being denied a permission takes precedence over being granted the same permission. Then, demonstrate how to grant shared folder permissions and how to modify shared folder settings. Finally, demonstrate how to connect to a shared folder using My Network Places, **Map Network Drive**, or the **Run** command.

- Combining NTFS and Shared Folder Permissions

  Present the information on combining NTFS and shared folder permissions. Emphasize that the resulting permissions is the most restrictive of either the combined NTFS permissions or the combined shared folder permissions.

- Using Administrative Shared Folders

  Present the information about administrative shared folders. Emphasize that these folders are automatically created by Microsoft Windows® 2000, hidden from users who browse, and only accessible to users with administrative privileges. In addition, mention that the Admin$ shared folder is where Windows 2000 is installed.

- Publishing a Shared Folder in Active Directory

  Present information on the benefits of publishing shared folders in Active Directory. Emphasize that users can find a published shared folder even if its physical location changes.

- Configuring Shared Folders by Using Dfs

  First, provide an overview of Dfs, including its benefits. Emphasize that Dfs provides a logical tree structures for folders and files that are physically located anywhere on the network. Then, present the different types of Dfs roots. Mention that a domain-based Dfs root provides fault tolerance. Next, provide information on how a user gains access to files and folders in a Dfs hierarchy. Emphasize that Dfs does not use separate NTFS permissions or shared folder permissions for Dfs links.

  Then, present information on creating a Dfs root. Demonstrate the process. Follow this with information on adding Dfs links. Demonstrate the process. Next, present information on configuring replicas. Mention the role of the File Replication service (FRS) in keeping replicas automatically synchronized.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

To prepare student computers for the labs in this module, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

- Performing the labs in this module introduces no configuration changes.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about providing network access to files and network resources in Windows 2000.

- **Introduction to Shared Folders**
- **Creating Shared Folders**
- **Combining NTFS and Shared Folder Permissions**
- **Using Administrative Shared Folders**
- **Publishing a Shared Folder in Active Directory**
- **Configuring Shared Folders by Using Dfs**

**********ILLEGAL FOR NON-TRAINER USE**********

Defer any student questions about Dfs until the Dfs section of this module.

As an administrator you must ensure that users can gain access to folders on the network that contain the files that they need to do their work. You can do this by sharing these folders. To enhance security, you can control who can gain access to these shared folders. If the files and folders users need are stored throughout the network, you can use Distributed file system (Dfs) to make it easier for users to gain access to these files and folders.

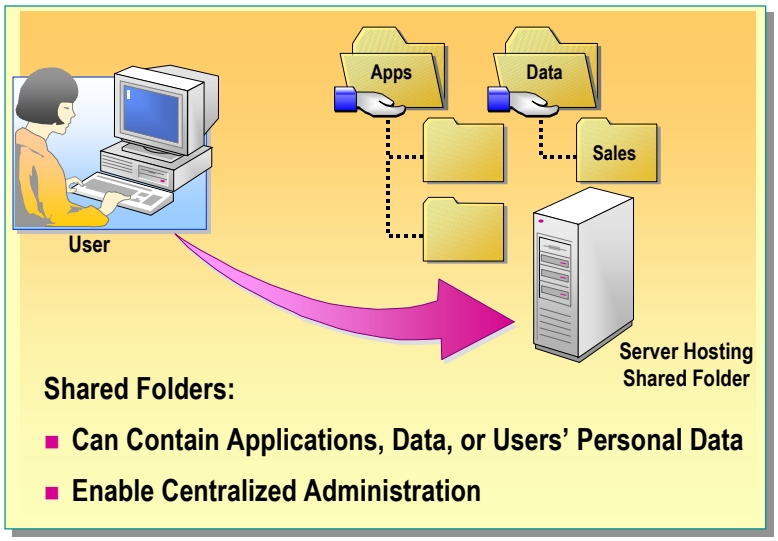
At the end of this module, you will be able to:

- Explain the purpose and use of shared folders.
- Create shared folders.
- Combine NTFS file system permissions and shared folder permissions.
- Use Administrative shared folders.
- Publish a folder in the Active Directory™ directory service.
- Configure shared folders by using Dfs.

Introduction to Shared Folders

Topic Objective
To illustrate the use of shared folders.

Lead-in
You can use shared folders to provide network users with access to files and network resources.



**********ILLEGAL FOR NON-TRAINER USE**********

Use shared folders to provide users with access to files and folders across a network. Users can connect to the shared folder over the network to access the folders and files they contain. Shared folders can contain applications, data, or a user's personal data. Using shared application folders centralizes administration by allowing you to install and maintain applications on a server instead of on client computers. Using shared data folders provides a central location for users to gain access to common files and makes it easier for you to back up data contained in those files.

Creating Shared Folders

Topic Objective
To identify the topics related to creating shared folders.

Lead-in
To share a folder, you must have rights on the computer where the folder resides.

- Requirements for Sharing Folders
- Sharing a Folder
- Shared Folder Permissions
- Granting Permissions and Modifying Shared Folder Settings
- Connecting to Shared Folders

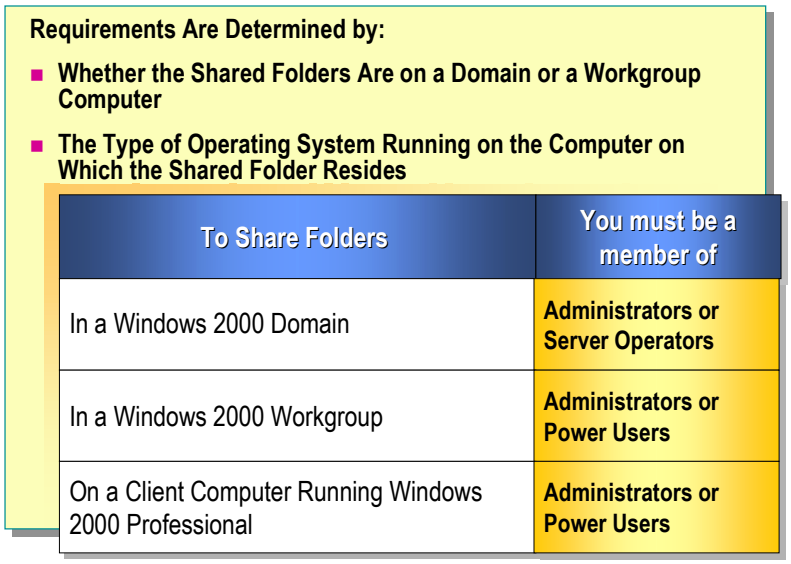
**********ILLEGAL FOR NON-TRAINER USE**********

To share a folder, you must be a member of one of the groups that have the rights to share folders on the type of computer where the folder resides. When you share a folder, you can control access to the folder and its contents by granting permissions to selected users and groups. You can also control access to the folder by limiting the number of users who can concurrently connect to the shared folder. After you create a shared folder, you may want to modify the folder properties to stop sharing the folder, change the shared folder name, or change user and group permissions to the shared folder. Microsoft® Windows® 2000 also shares some folders automatically for administrative purposes.

Requirements for Sharing Folders

Topic Objective
To identify the requirements for sharing folders.

Lead-in
To share a folder, you must be a member of the Administrators, Server Operators, or Power Users groups.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Groups with the ability to share folders include the Administrators, Server Operators, and Power Users groups.

In Windows 2000, the only groups that can share folders are the Administrators, Server Operators, and Power Users groups. These groups are default accounts that are installed in the User folder in Computer Management, or in the Builtin folder in Active Directory Users and Groups. The requirements for sharing folders are determined by the following:

- Whether the shared folder resides on a computer that is in a domain or in a workgroup.
- The type of operating system running on the computer on which the shared folder resides.

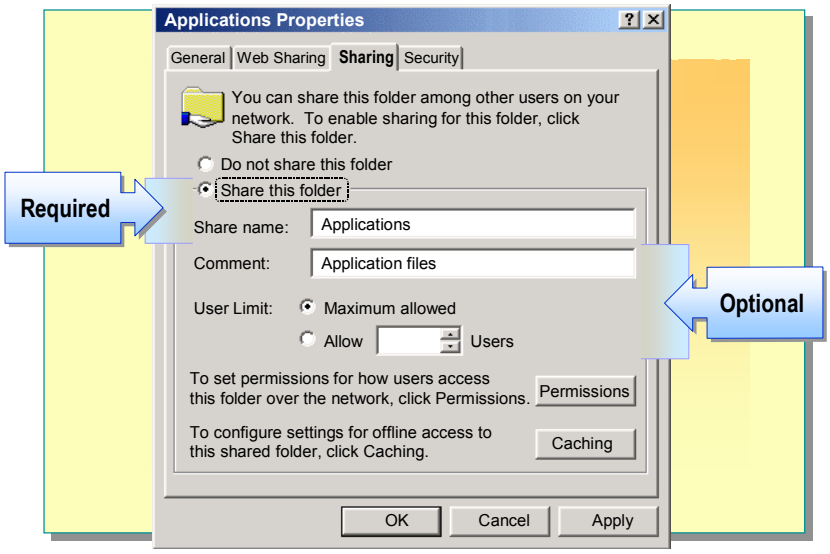
The following table describes who can share folders.

To share folders	You must be a member of
In a Windows 2000 domain	The Administrators or Server Operators group. Note that the Power Users group can share folders residing on a stand-alone server in a Windows 2000 domain.
In a Windows 2000 workgroup	The Administrators or Power Users group.
On client computer running Windows 2000 Professional	The Administrators or Power Users group.

Sharing a Folder

Topic Objective
To illustrate the options for sharing folders.

Lead-in
The first step for sharing a folder is to assign it a shared folder name.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the steps to share a folder.

Mention to students that because some client computers only see a limited number of characters in a shared folder name when they connect, they should be sure that all of the client computers on their network can see the shared folder names they set up.

When you share a folder, you give it a shared folder name, provide a comment to describe the folder and its contents, limit the number of users who have access to the folder, and grant permissions. You also have the option to share the same folder multiple times. This enables you to consolidate multiple shared folders into one folder, while allowing users to use the same shared folder name that was used before the folders were consolidated.

To create a shared folder, right-click the folder in Windows Explorer, and then click **Sharing**. On the **Sharing** tab, configure the options described in the following table.

Option	Description
Share this folder	Click to share the folder.
Share name	Enter the name that users from remote locations use to make a connection to the shared folder. The default shared folder name is the folder name. This option is required. **Note**: Some client computers that connect to a share point only see a limited number of characters.
Comment	Enter an optional description for the shared folder name. The comment appears in addition to the shared folder name when users at client computers browse the server for shared folders. You can use this comment to identify the contents of the shared folder.

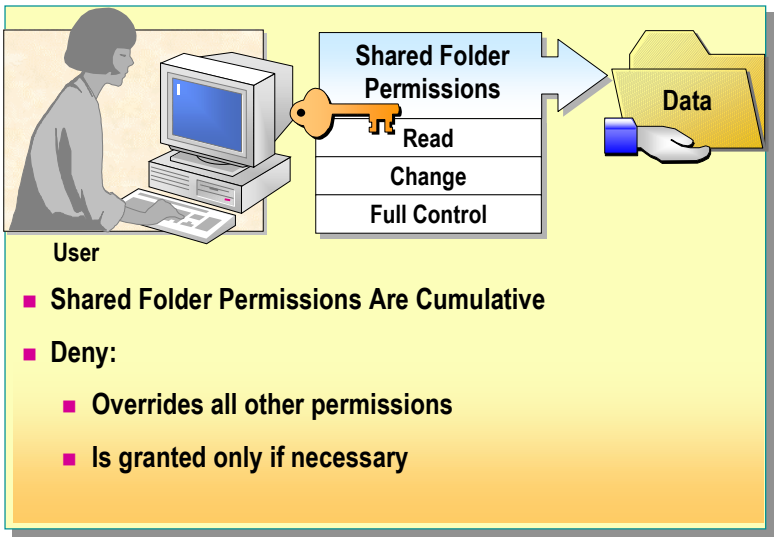
(continued)

Option	Description
User Limit	Enter the number of users who can concurrently connect to the shared folder. This option is not required. If you click **Maximum Allowed**, Windows 2000 Professional supports up to 10 connections. Windows 2000 Server can support as many connections as the number of licenses purchased.
Permissions	Click to set the shared folder permissions that apply only when the folder is accessed over the network. This option is not required. By default, the Everyone group is granted the Full Control permission for all new shared folders.

Shared Folder Permissions

Topic Objective
To identify shared folder permissions.

Lead-in
You can use shared folders to provide network users with access to files and network resources.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Using shared folders centralizes administration and provides a central location for users to gain access to common resources.

Shared folder permissions apply to folders and not to individual files.

If students want an example of when they would grant permissions to a computer account, mention a specific computer on which any user that logs on to the computer should be able to access a shared folder.

Explain that the Full Control permission is granted to the Everyone group by default when you share a folder.

Users can be granted or denied permission to shared folders. Folder permissions only apply to users who connect to the folder over the network; they do not restrict access to users who gain access to the folder at the computer where the folder is stored. You can grant shared folder permissions to user accounts, groups, and computer accounts.

The Permissions

To control how users gain access to a shared folder, you use shared folder permissions. Shared folder permissions apply to folders that are shared, not to individual files. The following table describes what each of these permissions allows a user to do.

Permission	Allows the user to
Read	Display folder names, file names, file data, and attributes; run application files; and change folders within the shared folder.
Change	Create folders; add files to folders; change data in files; append data to files; change file attributes; delete folders and files; and perform actions permitted by the Read permission.
Full Control	Change file permissions; take ownership of files; and perform all tasks permitted by the Change and Read permission. By default, the Everyone group has this permission.

Key Points
If an administrator only wants certain users to gain access to a shared folder, the administrator must remove the default Everyone group.

Make sure the students understand what the Everyone group is.

Important If you want to give only some users permission to a shared folder, remove the Everyone group, otherwise all users have the Full Control permission to the folder. If you change the permission for the Everyone group to Deny, then all users are denied access to the shared folder including the users you want to have access to the file.

Permissions Are Cumulative

A user's effective permissions for a resource are the combination of the shared folder permissions that you grant to the individual user account and the shared folder permissions that you grant to the groups to which the user belongs. For example, if a user has the Read permission for a folder and is a member of a group with the Write permission for the same folder, then the user has both the Read and Write permissions for that folder.

Denying Overrides Other Permissions

Key Point
Denied permissions take precedence over any permission you otherwise grant for user accounts and groups.

You can also deny shared folder permissions. Denied permissions override any allowed permission set for user accounts and groups. It is recommended you only deny shared folder permissions when you want to ensure specific users do not have access to a shared folder. If you deny shared folder permissions to a user, the user will not have that permission, even if you allow that permission for a group of which the user is a member. If you simply do not grant a shared folder permission to a user, that user could become a member of a group that has the shared folder permission and would then have the permission.

Tip Use the Authenticated Users group instead of the Everyone group to assign most rights and permissions. Doing so minimizes the risk of unauthorized access because Windows 2000 makes only valid user accounts on the computer, or in Active Directory, members of the Authenticated Users system group.

Granting Permissions and Modifying Shared Folder Settings

Topic Objective
To illustrate the dialog boxes for granting permissions and modifying shared folders.

Lead-in
After you share a folder, you can specify which users have access to it by granting shared folder permissions to selected user accounts and groups. In addition, you can always modify shared folder settings.

- **When You Grant Shared Folder Permissions:**
  - A shared folder can reside on an hard disk formatted to NTFS, FAT, or FAT32 file system
  - Users also need the appropriate NTFS permission on an NTFS volume
- **You Can Modify Shared Folder Settings to:**
  - Stop sharing a folder
  - Modify the share name
  - Modify permissions
  - Create multiple shares for a shared folder
  - Remove a share

**********ILLEGAL FOR NON-TRAINER USE**********

After you share a folder, you can control which user accounts, groups, and computers have access to it by using shared folder permissions. You can also modify the existing shared folder settings.

Delivery Tip
Demonstrate the steps to grant shared folder permissions.

Granting Shared Folder Permissions

You can grant shared folder permissions when the folder is on a drive formatted to use the NTFS, FAT (file allocation table), or FAT32 file system.

Important For users to gain access to a shared folder on a NTFS volume, they need the appropriate NTFS permissions for each file and folder in addition to the shared folder permissions. You set NTFS permissions for files and folders that reside on a NTFS volume on the **Security** tab in the **Properties** dialog box.

To grant shared folder permissions to user accounts, groups, and computer accounts, perform the following steps:

1. Open the **Properties** dialog box for the shared folder. On the **Sharing** tab, click **Permission** to open the **Permissions** dialog box.
2. Click **Add**. In the **Select User, Groups, or Computers** dialog box, click **Look in** to see a list of domains (including the local computer) from which you can select user account and group names.
3. Select the user account or group for which you want to grant permissions.
4. Select the **Allow** check box of the appropriate permissions for the user account, group, or computer.

Modifying Shared Folder Settings

Delivery Tip
Demonstrate the steps to modify a shared folder setting.

You can modify shared folders on the **Sharing** tab in the **Properties** dialog box for the folder.

The following table provides the different modifications you can make to shared folders and describes how to make them.

Key Point
If an administrator modifies a shared folder name by stop sharing and then re-sharing a folder, the original shared folder permissions are lost and have to be redone.

To	Do this
Stop sharing a folder	Click **Do not share this folder**.
Modify the share name	Click **Do not share this folder** to stop sharing the folder, and then click **Apply** to apply the change. Click **Share this folder**, and then type the new shared folder name in the **Share name** box. **Important**: This removes all existing shared folder permissions, which need to be recreated.
Modify shared folder permissions	Click **Permissions**. In the **Permissions** dialog box, add or remove users or modify permissions by selecting the user. Then, select the individual permissions to allow or deny.
Share a folder multiple times	Click **New Share** to share a folder with an additional shared folder name. Use additional shared folder names to consolidate multiple shared folders into one folder. This allows users to continue to use the original shared folder name. This option only appears when the folder is already shared.
Remove a shared folder name	Click **Remove Share**. This option only appears after the folder has been shared more than once.

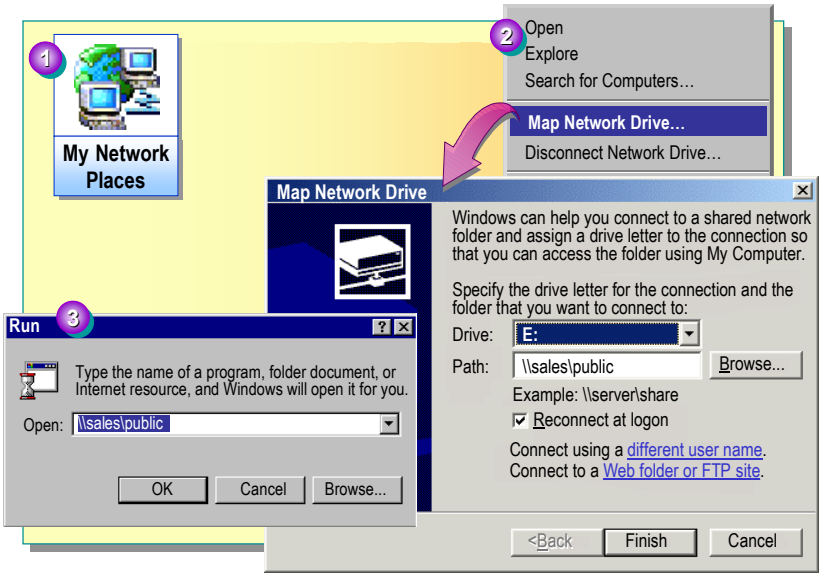
Key Points
If an administrator stops sharing a folder while a user has a file open, the user may lose data. In addition, if a user is connected to the shared folder when an administrator stops sharing it, Windows 2000 displays a dialog box notifying the administrator of this situation.

Important If you stop sharing a folder while a user has a file open, the user may lose data. If you click **Do not share this folder**, and a user has a connection to the shared folder, Windows 2000 displays a dialog box notifying you that a user has a connection to the shared folder.

Connecting to Shared Folders

Topic Objective
To illustrate the options for connecting to a shared folder.

Lead-in
There are three ways to gain access to a shared folder on another computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate connecting to a shared folder by using the three different methods. If you are short of time, show only one of the methods.

After you share a folder, users can gain access to the folder across the network. Users can gain access to a shared folder on another computer by using My Network Places, **Map Network Drive**, or the **Run** command.

Using My Network Places

In many instances, the easiest way to gain access to a shared folder is to use My Network Places.

To connect to a shared folder by using My Network Places, perform the following steps:

1. Double-click **My Network Places**.
2. Enter the network path of the shared folder you want to connect to or click **Browse** to find the computer on which the shared folder is located.
3. Double-click the shared folder to open it.

Note When you open a shared folder over the network, Windows 2000 automatically adds it to My Network Places.

Using Map Network Drive

Map a network drive if you want a drive letter and icon associated with a specific shared folder. This makes it easier to reference the location of a file in a shared folder. For example, instead of pointing to *\\Server\Shared_Folder_Name\File*, you would point to Drive:\File. You use drive letters to gain access to shared folders for which you cannot use a universal naming convention (UNC) path, such as a folder for an older application.

To map to a network drive, perform the following steps:

1. Right-click **My Network Places**, and then click **Map Network Drive**.
2. In the Map Network Drive wizard, select the drive letter that you want to use.
3. Enter the name of the shared folder you want to connect to or click **Browse** to find the shared folder.

   To gain access to a shared folder that you will use on a recurring basis, select **Reconnect at logon** to connect automatically each time you log on.

Using the Run Command

When you use the **Run** command to connect to a network resource, a drive letter is not required, which allows for an unlimited number of connections that are independent of available drive letters.

To connect a shared folder to a network drive, perform the following steps:

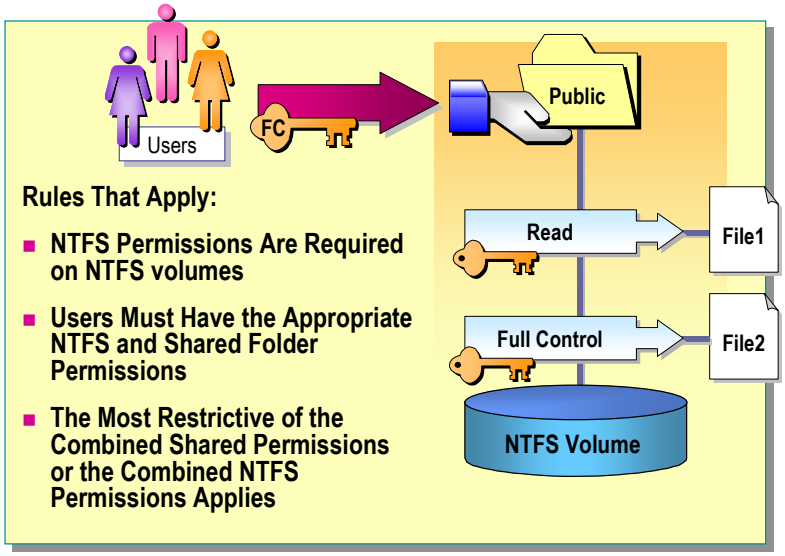
1. Click **Start**, and then click **Run**.
2. In the **Run** dialog box, enter a UNC path in the **Open** box, and then click **OK**.

   When you enter the server name in the **Open** box, a list of available shared folder names appears. Windows 2000 gives you the option to choose one of the entries based on the shared folders that are available to you.

Combining NTFS and Shared Folder Permissions

Topic Objective
To illustrate the combination of shared folder permissions and NTFS permissions.

Lead-in
One strategy for controlling access to an NTFS volume is to share folders with the default permissions and then control access to these folders by granting NTFS permissions.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Identify the group's effective permissions for File1 and File2 in the slide.

One strategy for controlling access to network resources on an NTFS partition is to share folders with the default shared folder permissions, and then to control access to these folders by granting NTFS permissions.

When you share a folder on a partition formatted with NTFS, both the shared folder permissions and the NTFS permissions combine to secure file resources. NTFS permissions apply whether the resource is accessed locally or over a network.

Key Point
When an administrator combines NTFS and shared folder permissions, the most restrictive of the combined NTFS permissions or the combined shared folder permissions applies.

When you grant shared folder permissions on an NTFS volume, the following rules apply:

- NTFS permissions are required on NTFS volumes. By default, the Everyone groups has the Full Control permission.
- Users must have the appropriate NTFS permissions for each file and subfolder in a shared folder, in addition to shared folder permissions, in order to gain access to those resources.
- When you combine NTFS permissions and shared folder permissions, the resulting permission is the most restrictive permission of the combined shared folder permissions or the combined NTFS permissions.

Using Administrative Shared Folders

Topic Objective
To identify hidden administrative shared folders.

Lead-in
Windows 2000 provides hidden shared folders for administrative purposes.

- **Administrators Use Administrative Shared Folders to Perform Administrative Tasks**
- **Administrative Shared Folders Are Hidden From Normal Users**
- **Administrators Have the Full Control Permission**

Share	Purpose
C$, D$, E$	The root of each partition is automatically shared
Admin$	The C:\Winnt folder is shared as Admin$
Print$	The folder containing the printer driver files is shared as Print$ (created when the first printer is created)

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Administrative shared folders are hidden from users that browse their computers.

The Admin$ is the *systemroot* folder. Administrators can use a shared folder name to gain access to Windows 2000 without knowing the name of the folder it is installed in.

Delivery Tip
Demonstrate creating a hidden shared folder by appending a dollar sign to the shared folder name.

Windows 2000 automatically shares folders that enable you to perform administrative tasks. These shared folders are appended with a dollar sign ($). The dollar sign hides the shared folder from users who browse the computer in My Network Places. The root of each drive including hard drives and CD-ROMs, the systemroot folder, and the location of the printer drivers are all hidden shared folders that Windows 2000 creates automatically.

By default, members of the Administrators group have the Full Control permission for administrative shared folders. You cannot modify the permissions on administrative shared folders. The following table describes the purpose of the administrative shared folders that Windows 2000 automatically provides.

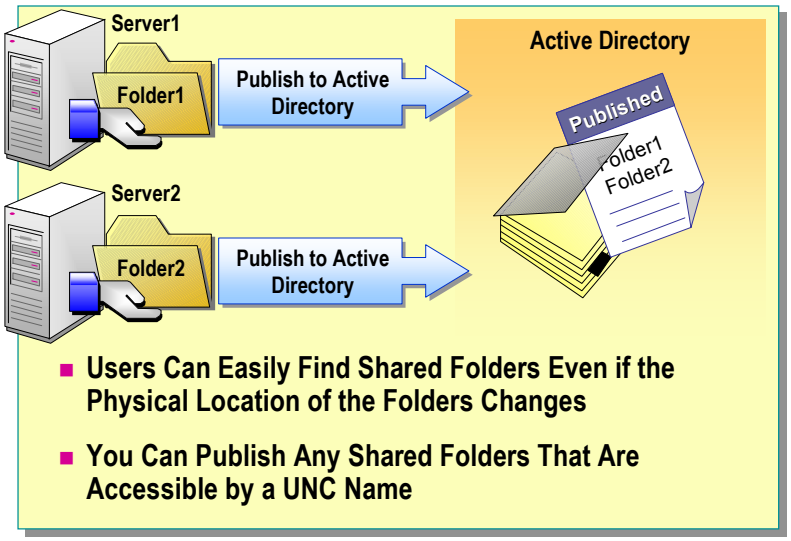
Shared Folder	Purpose
C$, D$, E$, and so on	These shared folders are used to remotely connect to a computer and perform administrative tasks. The root of each partition on a hard disk is automatically shared. When you connect to this folder, you have access to the entire partition.
Admin$	The systemroot folder, which is C:\Winnt by default. Administrators can gain access to this shared folder to administer Windows 2000 without knowing the folder in which it is installed.
Print$	This folder provides access to printer driver files for client computers. When you install the first shared printer, the *Systemroot*\System32\Spool\Drivers folder is shared as Print$. Only members of the Administrators, Server Operators, and Print Operators groups have Full Control permission. The Everyone group has Read permission.

Hidden shared folders are not limited to those that Windows 2000 automatically creates. You can share additional folders and append a dollar sign ($) to the end of the shared folder name. Then, only users who know the folder name can gain access to it. These hidden folders are not considered administrative shared folders.

Publishing a Shared Folder in Active Directory

Topic Objective
To illustrate the process of publishing folders in Active Directory.

Lead-in
In Windows 2000, you can publish shared folders in Active Directory. This method of sharing makes it very convenient to locate a shared folder.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Publishing a shared folder in Active Directory, enables users to find the folder even if its physical location changes.

To be published, a shared folder must be accessible by a UNC name.

Publishing resources, including shared folders, in Active Directory enables users to search Active Directory and find resources on the network even if the physical location of the resources changes. For example, if you move a shared folder to another computer, all shortcuts pointing to the Active Directory object that represents the published shared folder will continue to work, as long as you update the reference to the physical location. Users do not have to update their connections.

You can publish any shared folder in Active Directory that can be accessed by using a UNC name. After a shared folder is published, a user at a computer running Windows 2000 can use Active Directory to locate the object representing the shared folder and then connect to the shared folder.

Delivery Tip
Demonstrate the steps for publishing a shared folder in Active Directory.

To publish a shared folder in Active Directory, perform the following steps:

1. Open Active Directory Users and Computers from the **Administrative Tools** menu.
2. In the console tree of Active Directory Users and Computers, right-click the domain in which you want to publish the shared folder, point to **New**, and then click **Shared Folder**.
3. In the **Shared Folder Name** box, type the folder name as you want it to appear in Active Directory.
4. In the **Network Path** box, type the path to the shared folder (UNC name), and then click **OK**.

   Administrators and users can find information in Active Directory by using the **Search** command on the **Start** menu, **My Network Places** on the desktop, or Active Directory Users and Computers.

Lab A: Sharing and Securing Network Resources

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will share a folder and assign permissions. Then, you will configure shared folder settings.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Share a folder.
- Assign shared folder permissions to user accounts and groups.
- Connect to a shared folder.
- Stop sharing a folder.
- Determine the effects of combining shared folder and NTFS file system permissions.

Prerequisites

Before working on this lab, you must have knowledge of how Windows 2000 uses shared folder and NTFS permissions to secure access to networks.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.

Estimated time to complete this lab: 30 minutes

Exercise 1
Sharing Folders

Scenario

Users on your network need to gain access to a number of applications on a server that you administer. You have already installed the applications in a folder, named Apps, and have assigned NTFS permissions on all of the application folders within. You now need to share the Apps folder and configure the permissions for it so that the users can access the folder from the network.

Goal

In this exercise, you will create share points on your member server to provide access to the Apps folder from the network.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with the password of **domain** and share the C:\MOC\Win2152b\Labfiles\Lab7\Apps folder as Apps.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab07\Apps folder. **c.** Open the **Properties** dialog box for the Apps folder, and then click the **Sharing** tab.
Note: Notice that the Apps folder currently is not shared.	
1. (*continued*)	**d.** Click **Share this folder**. *The share name defaults to the name of the folder. If you wanted the share name to be different from the name of the folder, you would change it here.* **e.** In the **Comment** box, type **Shared Applications** and then click **OK**.
How does Windows Explorer change the appearance of the Apps folder to indicate that it is a shared folder? (You may have to refresh your screen by pressing F5.) **Windows Explorer shows an icon of a hand holding the Apps folder. The icon indicates that the folder is shared.**	

Exercise 2
Assigning Shared Folder Permissions

Scenario

You have shared the folder that contains the applications used by all the employees of your company, giving users the ability to connect to it over the network. Even though you have configured NTFS permissions to provide user rights, company policy dictates that the default permissions for the folder be removed and replaced with the permissions listed in the company policy.

To configure share permissions, you must determine what the current permissions are for the shared applications folder, and then assign shared folder permissions to groups in your domain in accordance with company policy.

Goal

In this exercise, you will modify the default share permissions on the Apps folder to limit access rights to a specific group of users.

Tasks	Detailed Steps
1. Determine the current permissions for the Apps shared folder.	**a.** Open the **Properties** dialog box for Apps. **b.** On the **Sharing** tab, click **Permissions**.
What are the default permissions for the Apps shared folder? **Everyone has Full Control.**	
2. Remove the default permissions and assign the Full Control permission to the local Administrators group.	**a.** In the **Permissions for Apps** dialog box, verify that **Everyone** is selected, and then click **Remove**. **b.** Click **Add**. **c.** In the **Look in** box, click *Server* (where *Server* is your assigned computer name). **d.** Under **Name**, click **Administrators**, click **Add**, and then click **OK**.

Tasks	Detailed Steps
What type of access does the Administrators group have? **Read permission.**	
2. (*continued*)	**e.** Under **Permissions**, allow the Administrators group the Full Control permission, and then click **OK**. **f.** Click **OK** to close the **Apps Properties** dialog box, and then close Windows Explorer.

Exercise 3
Connecting to a Shared Folder

Scenario

You have installed a number of applications, configured NTFS permissions to limit access to the different applications, and configured a share to provide your network users with access to those applications across the network. You now need to verify that users can connect to the applications folder from other computers on the network by using various methods to connect to the shared applications folder.

Goal

In this exercise, you will log on as a user that should have limited access rights to the shares created in earlier exercises in order to verify that access is limited as expected.

Tasks	Detailed Steps
1. Connect to the shared Apps folder on your computer by using the **Run** command.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type *Server* (where *Server* is your assigned computer name), and then click **OK**.
Which shared folders are currently available? **In addition to the share you just created, the Printers, Colorpri, Reports, and Scheduled Tasks folders are available. Any shared printers also appear. On a domain controller, the Netlogon and Sysvol folders are also shared.**	
Note: Normally you would connect to another computer to verify the functionality of a shared folder. For the purpose of this lab, you will connect to your computer.	
1. (*continued*)	**c.** Double-click **Apps** to confirm that you can gain access to the folder. **d.** Close the **Apps on** *Server* (where S*erver* is your computer name) window.
2. Map a network drive to the shared folder on the instructor computer \\London\Corpdata by using Map Network Drive.	**a.** Right-click My Network Places, and then click Map Network Drive. **b.** In the **Drive** box, click **P**. **c.** In the **Folder** box, type **\\london\corpdata** **d.** Clear the **Reconnect at logon** check box.
Note: You will gain access to this shared folder in this exercise only. Disabling the option to reconnect will ensure that Windows 2000 does not automatically attempt to reconnect to this shared folder later.	

Tasks	Detailed Steps
2. (*continued*)	**e.** To complete the connection, click **Finish**. *Windows Explorer opens, showing the contents of the new shared folder. Notice that the title bar displays **Corpdata on London**.* **f.** Close the Corpdata on London window. **g.** Open My Computer, and then locate **Corpdata on London (P:)**.
How does My Computer indicate that this drive points to a remote shared folder? **My Computer uses an icon that shows a network cable attached to the drive. The icon indicates a mapped network drive.**	
3. Disconnect the mapped network drive from the shared CorpData folder on the instructor computer using My Computer.	**a.** In My Computer, right-click **CorpData on London (P:)**, and then click **Disconnect**. **b.** Close My Computer, and then log off.
4. Log on to nwtraders as Student*x* (where *x* is your assigned student number) with the password of **domain** and attempt to connect to the shared CorpData folder on the instructor computer.	**a.** Log on using the following information: User name: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Right-click **My Network Places**, and then click **Map Network Drive**. **c.** In the **Drive** box, click **P**. **d.** In the **Folder** box, type **\\london\corpdata** **e.** Clear the **Reconnect at logon** check box if necessary, and then click **Finish**. *Windows 2000 displays a message indicating that access is denied.*
Why were you denied access to the CorpData shared folder? **Because the user account that you used to log on does not have the required permissions to gain access to the shared folder. Only the Administrators group can gain access to the CorpData shared folder.**	
4. (*continued*)	**f.** Click **OK** to close the message.

Tasks	Detailed Steps
5. Connect to the shared CorpData folder as Admin*x* (where *x* is your assigned student number) with the password of **domain**.	**a.** Right-click My Network Places, and then click Map Network Drive. **b.** In the **Drive** box, click **P:\London\Corpdata**. **c.** In the **Folder** box, type **\\London \Corpdata** **d.** Click **Connect using a different user name**. **e.** In the **Connect As** dialog box, in the **User name** box, type **Admin***x* (where *x* is your assigned student number). **f.** In the **Password** box, type **domain** and then click **OK**. **g.** Clear the **Reconnect at logon** check box if necessary, and then click **Finish**. *A message appears, indicating that drive P is already connected. This is because there is an IPC connection from the previous attempt.* **h.** Click **Yes** to replace the current connection.
In Windows Explorer, can you gain access to drive P? Why or why not? **Yes. The Admin*x* account has the appropriate permissions to gain access to the shared folder.**	
5. (*continued*)	**i.** Close all windows, and log off.

Exercise 4
Removing a Folder Share

Scenario

You need to perform extensive changes to the applications folder and need to prevent users from accessing the files while you are making changes. You will stop sharing the folder in order to prevent users from connecting.

Goal

In this exercise, you will stop sharing the Apps folder on your member server.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with the password of **domain** and stop sharing the Apps folder.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab07 folder. **c.** Open the **Properties** dialog box for the Apps folder. **d.** On the **Sharing** tab, click **Do not share this folder**, and then click **OK**. *Windows 2000 no longer displays the icon that identifies Apps as a shared folder*. **e.** Close Windows Explorer. **f.** Click **Start**, and then click **Run**. **g.** In the **Open** dialog box, type *Server***Apps** (where *Server* is your computer name), and then click **OK**.
Were you able to make a connection to *Server*\Apps? **No. The folder is no longer shared.**	
1. (*continued*)	**h.** Click **OK** to close the message, click **Cancel** to close the **Run** dialog box, and then log off.

◆ Configuring Shared Folders by Using Dfs

Topic Objective
To introduce the topics for configuring shared folders by using Dfs.

Lead-in
Dfs provides a mechanism for administrators to create logical views of folders and files, regardless of where those files are physically located on the network.

- Introduction to Dfs
- Types of Dfs Roots
- Accessing Files Resources Through Dfs
- Creating a Dfs Root
- Adding Dfs Links
- Adding Replicas for Fault Tolerance
- Configuring Replication

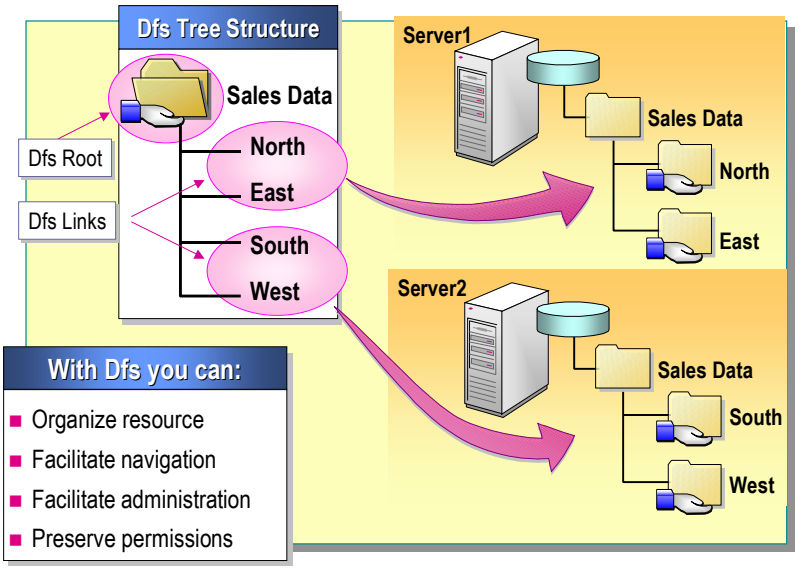
**********ILLEGAL FOR NON-TRAINER USE**********

With more and more files being distributed across local area networks (LANs), administrators face growing problems as they try to provide users with the access that they need. Dfs provides a mechanism for administrators to create logical views of folders and files, regardless of where those files are physically located on the network. Dfs also allows administrators to distribute shared folders and workloads across several servers for more efficient network and server resource use. Fault-tolerant network storage resources are also available by using Dfs. Domain-based Dfs features ensure that users can continue to gain access to shared folders even if a server becomes unavailable.

Introduction to Dfs

Topic Objective
To illustrate the structure of Dfs.

Lead-in
Dfs organizes shared folders and simplifies navigation to the shared folders.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain to students that Dfs provides a single network access point that Dfs clients can use for accessing resources located on several servers.

Dfs is a service that provides a single point of reference and a logical tree structure for file system resources that may be physically located anywhere on the network. Using Dfs to share network resources across the network, provides the following benefits:

- *Organizes resources*. Dfs uses a tree structure that contains a root and Dfs links. A *Dfs link* is a portion of the Dfs hierarchy. Each Dfs root can have multiple links beneath it, each of which points to a shared folder.

Key Point
Users can easily navigate through a Dfs tree without knowing the physical location of the folder or file they are seeking.

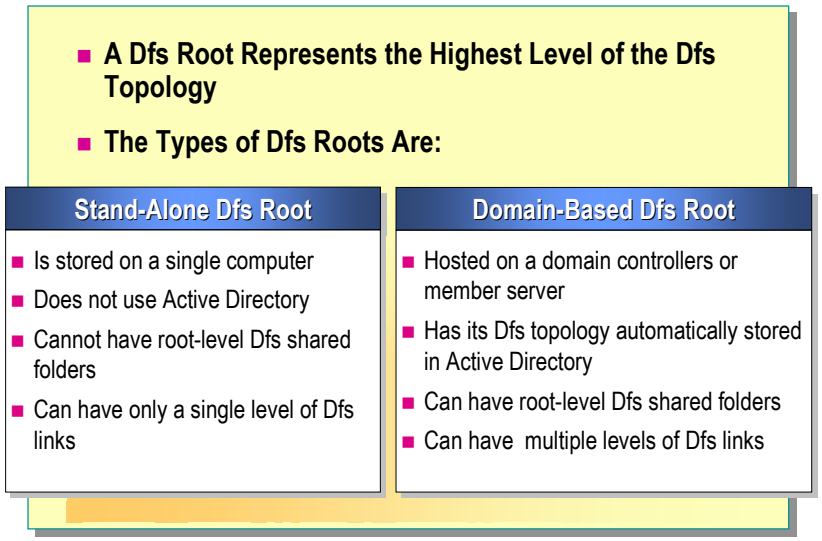
- *Facilitates navigation*. A user who navigates through a Dfs tree does not need to know the name of the server that physically stores the resource to locate a specific resource on the network. After connecting to a Dfs root, users can browse and gain access to all resources below the root, regardless of the physical location of the server on which the resource is located.
- *Facilitates administration*. Dfs simplifies the administration of multiple shared folders. If a server fails, you can move the location of the shared folder from one server to another without users being aware of the change. Users continue to use the same path for the link.
- *Preserves permissions*. A user can gain access to a shared folder through Dfs as long as the user has the required permission to gain access to the shared folder.

Note Only client computers with Dfs client software can gain access to Dfs resources. Computers running Windows 2000, Microsoft Windows NT® version 4.0, and Microsoft Windows 98 include Dfs client software. You must download and install a Dfs client on computers running Microsoft Windows 95.

Types of Dfs Roots

Topic Objective
To identify the two types of Dfs roots.

Lead-in
You have the option of establishing either a stand-alone Dfs root or a domain-based Dfs root.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
A stand-alone Dfs root provides no fault tolerance because the Dfs topology is stored on a single computer.

A domain-based Dfs root provides fault tolerance because the Dfs topology is stored in Active Directory.

A Dfs root is the highest level of the Dfs topology and is the starting point for the hierarchy of shared folders. A Dfs root can be defined at the domain level or at the server level. A domain may have any number of Dfs roots, but each server running Windows 2000 can host only one Dfs root. You can configure the following types of Dfs roots:

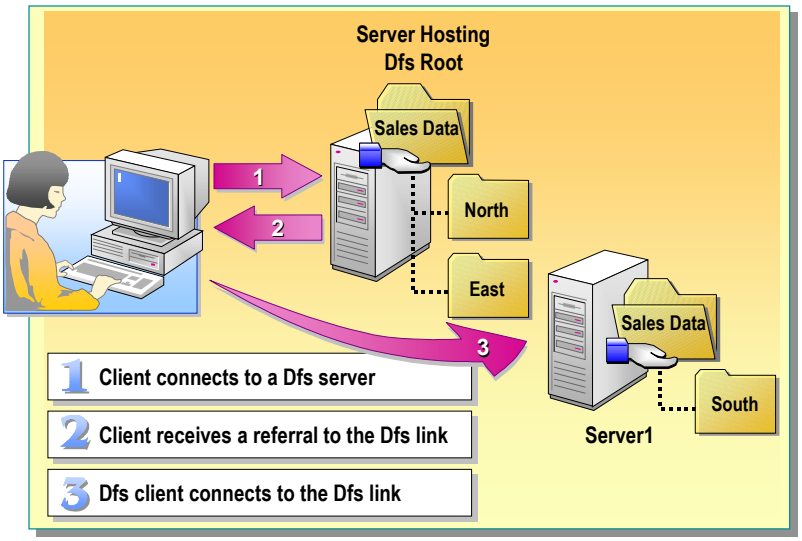
- *Stand-alone Dfs roots*. This Dfs root is hosted on a single computer and the Dfs topology is stored on that computer. A stand-alone Dfs root provides no fault tolerance if the computer that stores the shared folders or Dfs topology fails. *Fault tolerance* ensures data integrity when a hardware failure occurs. In addition, a stand-alone Dfs cannot have root-level Dfs shared folders and supports only a single level of Dfs links.
- *Domain-based Dfs roots*. This Dfs root is hosted on several domain controllers or member servers and the Dfs topology is stored in Active Directory. Because changes to a Dfs tree are automatically synchronized with Active Directory, you can restore a Dfs tree topology if the server hosting a Dfs root should fail. In addition, a domain-based Dfs root can have root-level Dfs shared folders and can support multiple levels of Dfs links.

Note You can only use domain-based Dfs roots on computers that are members of a domain.

Accessing File Resources Through Dfs

Topic Objective
To describe how to gain access to file resources through Dfs.

Lead-in
You gain access to file resources through Dfs in the same way that you gain access to other shared folders. The process of gaining access is transparent to users.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain the three steps on the slide.

Key Points
When a Dfs client connects to a Dfs root, the Dfs client sees all first-level Dfs links.

When a Dfs client connects to a Dfs link, it requests the location of the shared folder representing the Dfs link.

Because a Dfs hierarchy appears just as a regular folder hierarchy, users can gain access to file resources through Dfs in the same way that they gain access to regular shared folders. The difference is that Dfs provides users with a single access point for resources that can be located in several physical locations. Users can navigate through Dfs by using Windows Explorer.

When a user connects to a Dfs root, the user sees all first level Dfs links as folders in the Dfs root. The user can then connect to one of the Dfs links by opening the folder that the link represents. The user can also directly connect to a Dfs link. Whenever a user accesses a Dfs link, the following happens:

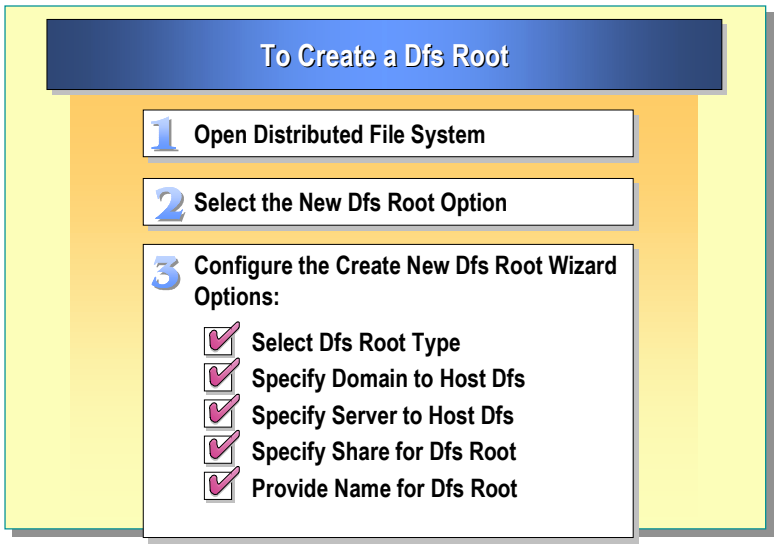
1. The Dfs client establishes a connection to the server that hosts Dfs.
2. The server that hosts Dfs returns the physical location of the shared folder that the Dfs link represents.
3. The Dfs client establishes a connection with the server that contains the shared folder. The Dfs client then caches this referral so that it can continue to connect to the shared folder represented by the Dfs link without contacting the server hosting the Dfs root again. Periodically the Dfs client contacts the server hosting the Dfs root to update the referral.

Important Dfs does not use separate NTFS permissions or shared folder permissions for Dfs links. Windows 2000 applies all permissions that you assign to the shared folder to which the Dfs link points.

Creating a Dfs Root

Topic Objective
To identify the options for creating a Dfs root.

Lead-in
When you create a Dfs root, you select the type of Dfs root, specify a host domain or host server, assign a shared folder to host the Dfs root, and then name the Dfs root.



**********ILLEGAL FOR NON-TRAINER USE**********

When you create a Dfs root, you select the type of Dfs root, specify a host domain or host server, assign a shared folder to host the Dfs root, and then name the Dfs root. For a standalone Dfs root, client computers connect to a server and shared folder. For a domain-based Dfs root, client computers connect to a domain and a shared folder. To create a domain-based or stand-alone Dfs root, perform the following steps:

Delivery Tip
Demonstrate the steps for creating a Dfs root.

Explain that the steps for creating a domain-based and stand-alone Dfs root are similar.

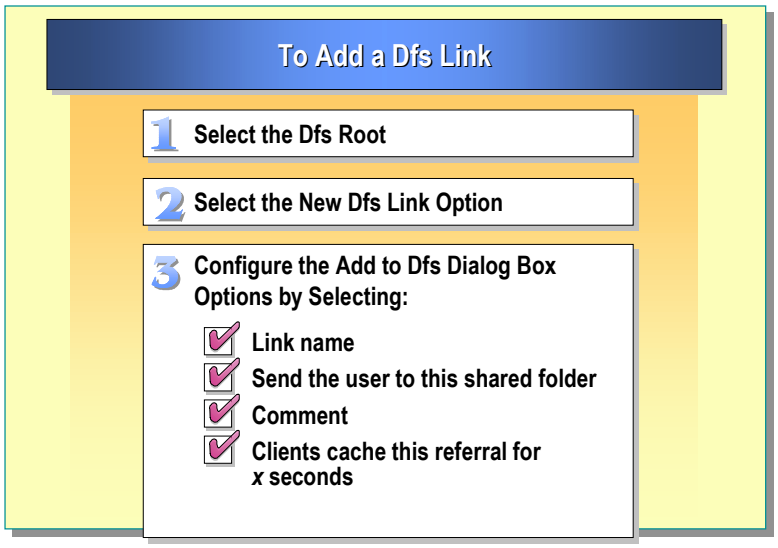
1. On the Administrative Tools menu, click Distributed File System.
2. On the Action menu, click New Dfs Root.
3. In the Create New Dfs wizard, configure the options that are described in the following table.

Option	Description
Select the Dfs root type	Selects the type of Dfs root that you want to create. Click **Create a domain Dfs root** or **Create a standalone Dfs root**.
Specify the host domain for the Dfs root	Specifies the domain that stores the Dfs topology. A domain can host multiple Dfs roots.
-or-	
Specify the host server for the Dfs root	Specifies the first host server, which is the initial connection point for all resources in the Dfs tree. You can create a Dfs root on any server running Windows 2000.
Specify the Dfs root share	Specifies the shared folder to host the Dfs root. You can choose an existing shared folder or create a new shared folder.
Name the Dfs root	Provides the descriptive name for the Dfs root that Windows Explorer displays.

Adding Dfs Links

Topic Objective
To identify the options for adding Dfs links.

Lead-in
A Dfs link exists below the Dfs root and can refer to a shared folder with or without subfolders.



**********ILLEGAL FOR NON-TRAINER USE**********

A link is mapped to a standard shared folder on the network. A new Dfs link can refer to a shared folder with or without subfolders. A Dfs link can also point to another Dfs root. This configuration allows you to create a large Dfs tree that combines other Dfs trees.

Delivery Tip
Demonstrate the steps for adding a Dfs link.

To add a Dfs link, perform the following steps:

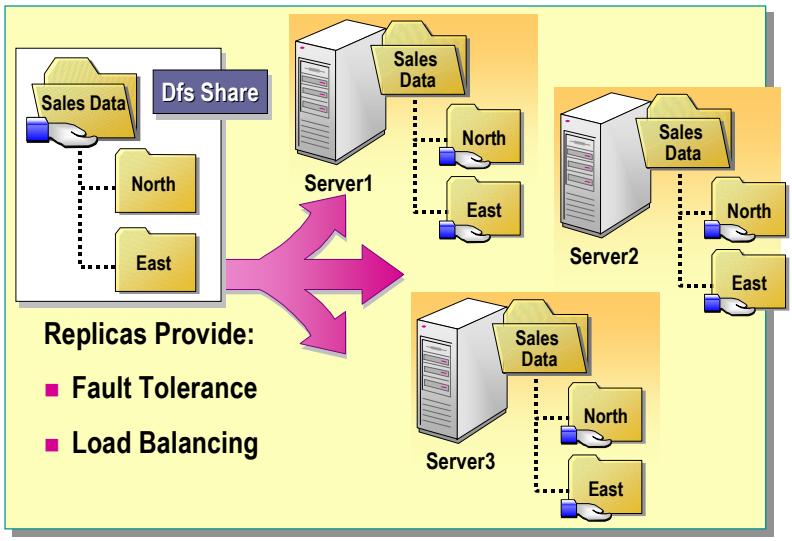
1. In Distributed File System, click the Dfs root to which you will add a Dfs link.
2. On the **Action** menu, click **New Dfs Link**.
3. In the **Add to Dfs** dialog box, configure the options described in the following table.

Option	Description
Link name	Specifies the logical name for a subfolder of a Dfs root. The link name appears as a folder in the Dfs logical hierarchy and is the name users will see when they connect to Dfs.
Send the user to this shared folder	Specifies the physical location of the shared folder to which the link refers.
Comment	Additional information (optional) to help keep track of the shared folder.
Clients cache this referral for *x* seconds	Length of time for which client computers cache a referral to a Dfs link. After the referral time expires, a client computer queries the Dfs server about the location of the link, even if the client computer has previously established a connection with the link.

Adding Replicas for Fault Tolerance

Topic Objective
To illustrate the use of replicas for fault tolerance.

Lead-in
Configuring multiple replicas of a Dfs link creates fault tolerance.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Replicas provide fault tolerance and load balancing.

A *replica* is another instance of a Dfs link. Copies of a Dfs link reside on at least one other server. These replicas provide fault tolerance. When one replica of a Dfs link becomes unavailable (for example, because the computer hosting the replica is unavailable), Dfs clients automatically connect to the other replica. This ensures uninterrupted access to shared folders. In addition, when multiple client computers connect to a Dfs link that has multiple replicas, these client computer requests are distributed across all of the servers hosting the replicas. This load balancing ensures that users experience faster response times because multiple servers are simultaneously responding to client computer requests.

To add a replica, perform the following steps:

1. In Distributed File System, right-click the Dfs link for which you want to create a new replica, and then click **New Replica**.
2. In the **Add a New Replica** dialog box, click **Browse** to select the shared folder for the new replica.

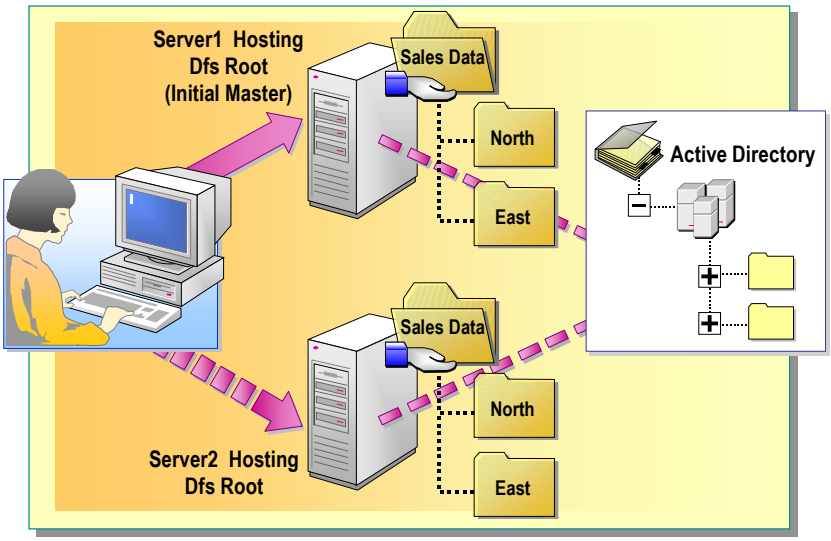
   Note Each Dfs link can have up to 32 replicas.

3. Select **Automatic Replication** if you want the File Replication service (FRS) to automatically replicate any changes that occur in any replica of the Dfs link to all other replicas. Select **Manual Replication** if you want no replication. Click **OK**.

Configuring Replication

Topic Objective
To illustrate the replication process.

Lead-in
You configure replication among multiple replicas of a Dfs link to ensure that each replica contains the same data.



**********ILLEGAL FOR NON-TRAINER USE**********

Mention the role that FRS plays in automatic replication.

Key Points
You configure replication among multiple replicas of a Dfs link after creating the replicas to keep the contents of the replicas synchronized.

When you configure multiple replicas of the same Dfs link, you need to ensure that each replica always contains the same data. To automatically keep the contents of the replicas synchronized as changes to one or more of the replicas occur, Windows 2000 provides the File Replication service. If you do not use FRS, you must manually copy files that change to all replicas of a Dfs link.

Setting Up Automatic Replication

Enable automatic replication by using the Replication Policy window of the Distributed File System console. To set replication policy, select one of your Dfs shared folders as the *initial master* (master copy), which then replicates its contents to the other Dfs shared folders in the set of Dfs shared folders. Replication occurs as part of Active Directory replication.

To set replication policy, perform the following steps:

1. Open Distributed File System.
2. Right-click a Dfs root or Dfs link, and then click **Replication Policy**.
3. In the list of shared folders, click a Dfs shared folder that you want to use as the master folder for replication.

   By default, the first Dfs folder that you create becomes the master folder for replication. If you want to change this default, click **Initial Master**.

   After you have set a master for replication, the **Initial Master** button no longer appears when you subsequently display this window. This is because you only set a master once to initiate replication; from then on, the Dfs shared folders replicate to one another whenever data in one of the Dfs shared folders changes.

4. Click all of the replicas that will participate in replication, and then click **Enable**.
5. To prevent a replica from participating in replication—for example when you do not want Dfs replication to create network traffic—select the replica, and then click **Disable**.

Checking the Status of a Dfs Replicas

Delivery Tip
Demonstrate how to check the status of replicas.

Point out the green check marks and cross marks that appear after status check. Tell students what these marks mean.

You can perform periodic status checks of Dfs replicas to ensure that replica sets are still valid for Dfs shared folders and that the replicas that you assigned are being referenced properly by Dfs. When you perform these status checks on replica sets, the results indicate one of the following conditions:

- The replica was found and is accessible. This indicates that everything is functioning correctly.
- The replica was found but is not accessible. This means that NTFS permissions or shared folder permissions may be not be configured properly.
- The replica was not found. This means that the shared folder is not available, for example, because the computer hosting it is not running.

To check status of a Dfs shared folder, perform the following steps:

1. Open Distributed File System.
2. In Distributed File System, right-click the Dfs root or Dfs link whose replication status you want to check, and then click **Check Status**.

Lab B: Configuring Domain-based Dfs

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create replicas, add Dfs links, and remove replicas and Dfs links.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a Dfs root replica.
- Create a Dfs link.

Prerequisites

Before working on this lab, you must have:

- Knowledge about how Microsoft Windows 2000 uses shared folder and NTFS file system permissions to secure access to network resources.
- The knowledge and skills to share folders.
- Knowledge about the purpose of Dfs, including how Dfs provides fault tolerance.

Lab Setup

To complete this lab, you need:

- A computer running Windows 2000 Advanced Server that is configured as a member server of the nwtraders.msft domain.
- A folder, C:\Moc\Win2152b\Labfiles\Lab07\Site Reports, shared as Reports.

Estimated time to complete this lab: 30 minutes

Exercise 1
Create a New Root Replica

Scenario

Your corporation wants to distribute reports to each office in the corporation using Dfs. The Corporate office has created a Dfs root called Corporate Reports. You must create a Dfs root replica on your server to provide fault tolerance.

Goal

In this exercise, you will create a Domain-based Dfs root replica.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with password of **domain** and attempt to create a new root replica of \\nwtraders.msft\corporate data. As part of the Dfs wizard, create a new shared folder on your server, named Corpdata, for the share point on your server to host the Dfs root.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Distributed File System from the **Administrative Tools** menu. **c.** In Distributed File System, in the console tree, right-click **Distributed File System**, and then click **Display an Existing Dfs Root**. **d.** On the **Display an Existing Dfs Root** page, expand **nwtraders.msft**, expand **Domain Dfs roots**, click **Corporate Data**, and then click **OK**. **e.** In Distributed File System, in the console tree, right-click **\\nwtraders.msft\Corporate Data**, and then click **New Root Replica**. **f.** On the **Specify the Host Server for the Dfs Root** page, verify that your server's FQDN is listed, and then click **Next**. **g.** On the **Specify the Dfs Root Share** page, click **Create a new share**. **h.** In the **Path to share** box, type **c:\moc\Win2152b\Labfiles\lab07\corpdata** **i.** In the **Share name** box, type *Server* **Dfs Replica** (where *Server* is your assigned computer name), and then click **Finish**. *A message appears indicating that the share does not exist.* **j.** Click **Yes** to create the folder. *A message appears indicating there is a network error.* **k.** Click **OK** to close the error message, click **Cancel** to close the New Dfs Root wizard, and then close Distributed File System.

Tasks	Detailed Steps
What permissions does a user account need in order to create a domain-based Dfs? **The user account must have domain-wide administrative rights. To gain these rights, a user account must be a member of an administrative group such as the Domain Admins group.**	
2. Logged on as Admin*x*, use the secondary logon, DAdmin@nwtraders.msft with a password of **domain**, to create a new root replica of \\nwtraders.msft\corporate data. Create a new shared folder on your server named Corpdata for the share point on your server to host the Dfs root. Configure your root replica to participate in automatic replication.	**a.** Click **Start**, point to **Programs**, point to **Administrative Tools**, hold the SHIFT key and right-click **Distributed File System**, and then click **Run as**. **b.** In the **Run as Other User** box, verify that **Run the program as the following user** is selected. **c.** In the **User name** box, type **DAdmin** **d.** In the **Password** box, type **domain** **e.** In the **Domain** box, type **nwtraders.msft** and then click **OK**. **f.** In Distributed File System, in the console tree, right-click **Distributed File System**, and then click **Display an Existing Dfs Root**. **g.** In the **Display an Existing Dfs Root** dialog box, expand **nwtraders.msft**, expand **Domain Dfs roots**, click **Corporate Data**, and then click **OK**. **h.** In Distributed File System, in the console tree, right-click **\\nwtraders.msft\Corporate Data**, and then click **New Root Replica**. **i.** On the **Specify the Host Server for the Dfs Root** page, verify that your server's FQDN is listed, and then click **Next**. **j.** On the **Specify the Dfs Root Share** page, verify that **Use an existing share** is selected, click *Server* **Dfs Replica** (where *Server* is your assigned computer name) if necessary, and then click **Finish**. *In the details pane of Distributed File System, your server is listed as a root replica.*
Wait for the instructor before proceeding. The instructor must configure the initial replication settings before you continue on with this exercise.	
2. (*continued*)	**k.** In Distributed File System, in the console tree, right-click **\\nwtraders.msft\Corporate Data**, and then click **Replication Policy**. **l.** On the **Replication Policy** page, click your server's shared folder entry, click **Enable**, and then click **OK**.
Note: In task 1, you created the shared folder on your server using the administrative rights associated with the Admin*x* user account, but you could not create the Dfs root replica using that account. In task 2, you did not have to create the share point on your server because you created the shared folder in task 1.	
2. (*continued*)	**m.** Minimize Distributed File System.

Tasks	Detailed Steps
3. View the data in the \\nwtraders.msft\corporate data folder, and then verify that the shared folder you created on your server has the same data.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\nwtraders.msft\corporate data** and then click **OK**. *A number of folders are listed in the Dfs shared folder.* **c.** Click **Start**, and then click **Run**. **d.** In the **Open** box, type \\S*erver*\S*erver* **Dfs Replica** (where S*erver* is your assigned computer name), and then click **OK**.
Is the content of the \\nwtraders.msft\corporate data share the same as the content of the *server**server* Dfs Replica share? Why? **Yes. Replication of the domain-based Dfs has occurred.**	
3. (*continued*)	**e.** Close the two shared folder windows.

Exercise 2
Adding a Dfs Link to an Existing Dfs Root

Scenario

To provide the entire corporation with a single share point for viewing corporate reports and remote office reports, you must create a Dfs link for your site under the corporate Dfs root.

Goal

In this exercise, you will create a Dfs Link under the \\nwtraders.msft\Corporate Data Dfs root.

Tasks	Detailed Steps
1. Create a Dfs link under \\nwtraders.msft\Corporate Data named *Server* Reports (where *Server* is your assigned computer name).	**a.** Restore Distributed File System. **b.** In the console tree, right-click **\\nwtraders.msft\Corporate Data**, and then click **New Dfs Link**. **c.** In the **Create a New Dfs Link** dialog box, under **Link name**, type *Server* **Reports** (where *Server* is your assigned computer name), and then click **Browse**. **d.** In the **Browse for Folder** dialog box, expand **Entire Network**, expand **Microsoft Windows Network**, expand **nwtraders**, expand *Server* (where *Server* is your assigned computer name), click **Reports**, and then click **OK**. **e.** In the **Create a New Dfs Link** dialog box, click **OK**. *The link appears under **Corporate Data** in the console tree.* **f.** Minimize Distributed File System.
2. View the data in the *nwtraders*.msft\Corporate Data Dfs share.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\nwtraders.msft\corporate data** and then click **OK**.
Why does your Dfs link show up as a folder when you open \\nwtraders.msft\Corporate Data? Is the Dfs link fault-tolerant? **Your Dfs link shows up as a folder under the root so that the client who connects to the Dfs shared folder sees one connection point with a number of subfolders. The Dfs link is not fault-tolerant, but a link replica could be created on a different server to provide fault tolerance for the Dfs link.**	
2. (*continued*)	**c.** Close the Corporate Data window.

Exercise 3
Removing a Dfs Link and Dfs Root Replica

Scenario

Your corporation has decided to use an Exchange mail server distribution list to provide access to corporate reports. You must remove the Dfs link, and then remove the Dfs root replica.

Goal

In this exercise, you will remove the Dfs link that you created, and then remove the Dfs root replica that you created.

Tasks	Detailed Steps
1. Remove the Dfs link for your server.	**a.** Restore Distributed File System. **b.** In Distributed File System, in the console tree, expand **\\nwtraders.msft\Corporate Data** if necessary, right-click *Server* **Reports** (where *Server* is your assigned computer name), and then click **Remove Dfs Link**. **c.** In the **Distributed file system** message, click **Yes** to proceed. *The Dfs link for your server is removed from the console tree.*
2. Remove the Dfs root replica for your server.	**a.** In Distributed File System, in the details pane, right-click *Server**Server* **Dfs Replica**, and then click **Remove Replica**. **b.** In the **Distributed file system** message, click **Yes** to proceed. *Your server is removed from the details pane.* **c.** Close any open windows, and then log off.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to Shared Folders
- Creating Shared Folders
- Combining NTFS and Shared Folder Permissions
- Using Administrative Shared Folders
- Publishing a Shared Folder in Active Directory
- Configuring Shared Folders by Using Dfs

**********ILLEGAL FOR NON-TRAINER USE**********

1. When a folder is shared, which folders and files within that folder does a user with the Read permission have access to by default?

   A user with the Read permission has access to all folders and files in the shared folder. However, the user cannot change any files or folders.

2. What is the best way to secure files and folders that you share on NTFS partitions?

   Put the files that you want to share in a shared folder and retain the default shared folder permission (the Everyone group with the Full Control permission). Then grant the appropriate NTFS permissions to users and groups for the files and folders within the shared folder.

3. The information that users in your corporation need is distributed throughout the network on various servers. This forces users to remember the names of all of the servers and shared folders on the entire network. What could you do to solve this problem?

   Install Dfs on one computer and create links that point to all of the shared folders.

4. A user attempts to connect to another computer by using the UNC name \\server\c$ to gain access to all of the files and folders on the C: partition, but is denied access. The user knows that the C$ shared folder is automatically created by default. How could you explain the user's inability to gain access to that shared folder?

   The user does not have administrative privileges on the computer that they are trying to access. A hidden shared folder is created at the root of each defined partition, but is only accessible by users with administrative privileges.

5. You have shared and can access several folders on the server you administer, but when you attempt to locate them by searching Active Directory Users and Computers, they are not found. What could the problem be? How could you resolve it?

   You have not published the files in Active Directory. To do this, you must open Active Directory Users and Computers, right-click the domain in which you want to publish the shared folder, point to New, and then click Shared Folder. You must then provide a shared folder name and the path (UNC name) to publish a shared folder.

6. When users gain access to a Dfs link, how will they know that Dfs redirects their requests to a different physical folder?

   Users do not notice that the request is redirected. Dfs is completely transparent to users.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 8: Monitoring and Optimizing Performance in Windows 2000

Contents

Overview	1
Monitoring Event Logs	2
Using Task Manager to Monitor System Resources	11
Lab A: Using Task Manager and Event Viewer	17
Using System Monitor to Monitor System Performance	27
Using Alerts	33
Lab B: Monitoring System Performance	35
Optimizing Performance	42
Review	53

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware.

Instructor Notes

Presentation:
45 Minutes

Labs:
60 Minutes

This module provides students with the skills and knowledge necessary to monitor how their computers are performing. This includes using logs, setting up mechanisms to obtain data, and monitoring systems to optimize performance.

At the end of this module, students will be able to:

- Monitor event logs to monitor information about system operations.
- Use Task Manager to monitor system resources.
- Use System Monitor to monitor system performance.
- Use alerts to notify a user or an administrator when certain system criteria are met or exceeded.
- Optimize performance by identifying the counters to monitor.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft® PowerPoint® file 2152B_08.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Monitoring Event Logs

  First, present an overview of the different types of event logs and the type of data that each log provides. Then, present information on the different types of application and system events that Microsoft Windows® 2000 logs. Next, present information on viewing event logs. Show the students an event log. Mention to students that they can search for an event or events. After viewing logs, present how to limit the size of log files. Emphasize that if security is high in their networks, they may want to archive log files. Finally, present the tasks for managing event logs. Demonstrate how to archive an event log and show students where to manually clear logs.

- Using Task Manager to Monitor System Resources

  When beginning this topic, ensure that students understand what a process is. Then, present information on monitoring programs by using the **Application** tab. Make sure you have a process running on the instructor computer that you can use to demonstrate ending a process. Next, present information on monitoring processes by using the **Processes** tab. Make sure students know what an address space is. Finally, present information on monitoring performance by using the **Performance** tab. Demonstrate how to view process time in kernel mode.

- Using System Monitor to Monitor System Performance

  First, present information on System Monitor objects, instances, and counters, and then explain how they are interrelated. Emphasize that System Monitor objects are not related in any way to the Active Directory™ directory service objects. Then, demonstrate how to add counter displays. Mention to the students that counters are always gathering data, and that adding a counter is adding the display of the data that the counter gathered. Next, present the different ways to view counter data, such as in histogram, report, or chart view.

- Using Alerts

  First, present information on using alerts. Mention to students they can use alerts to warn a user or administrators when certain criteria are met or exceeded. In addition, mention the different types of alerts that can be set. Demonstrate setting an alert.

- Optimizing Performance

  First, present the performance optimization process. Emphasize that the process of performance analysis is not a perfect science, but an evolving process. Then, present information on examining memory performance. This includes establishing a baseline, using counters, and examining page files. Next, present information on examining processor performance. If time permits, show the counters % Processor Time and Processor Queue Length in System Monitor. Then, present information on examining disk performance, including the counters to view. Finally, present information on examining network performance. Mention that Performance Monitor allows you to monitor the performance of network objects on servers and that Network Monitor allows you to monitor the network data stream.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Windows 2000.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

To prepare student computers for the labs in this module, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

- Performing the labs in this module introduces no configuration changes.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about monitoring and optimizing system performance in Windows 2000.

- **Monitoring Event Logs**
- **Using Task Manager to Monitor System Resources**
- **Using System Monitor to Monitor System Performance**
- **Using Alerts**
- **Optimizing Performance**

**********ILLEGAL FOR NON-TRAINER USE**********

As an administrator, you monitor system resources in order to evaluate the workload of your computer, observe changes and trends in resource usage, test configuration changes, and diagnose problems.

Microsoft® Windows® 2000 includes tools for monitoring system resources. Task Manager presents a snapshot of programs and processes that are running on your computer and provides a summary of the computer's processor and memory usage. System Monitor and Performance Logs and Alerts provide detailed data about the resources used by specific components of the operating system and computer.

At the end of this module, you will be able to:

- Monitor event logs to monitor information about system operations.
- Use Task Manager to monitor system resources.
- Use System Monitor to monitor system performance.
- Use alerts to notify a user or an administrator when certain system criteria are met or exceeded.
- Identify counters to monitor for optimizing performance.

◆ Monitoring Event Logs

Topic Objective
To identify the topics related to monitoring Event Logs.

Lead-in
You can monitor a variety of activities and events in Windows 2000.

- Introduction to Event Logs
- Types of System and Application Events
- Viewing Event Logs
- Limiting the Size of Log Files
- Managing Event Logs

**********ILLEGAL FOR NON-TRAINER USE**********

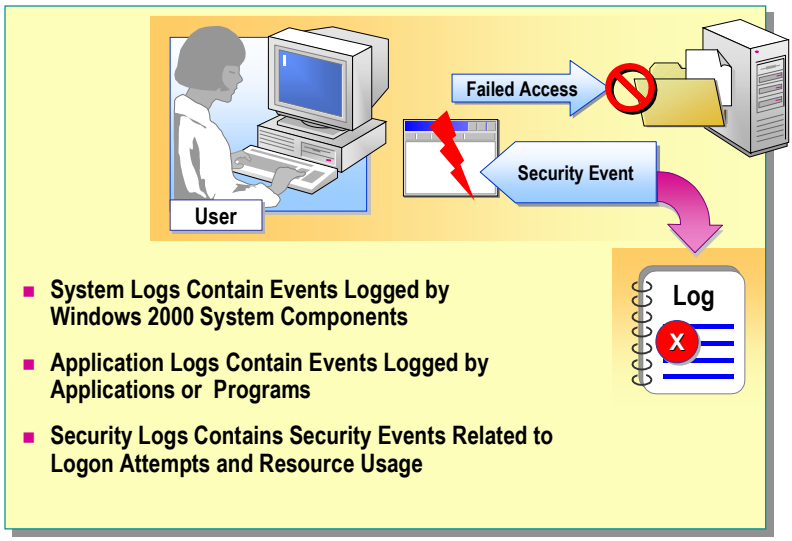
Events are user actions that are recorded based on an Audit policy, or any significant occurrence in Windows 2000 or in an application. Monitor events to identify and track security events, resource use, or system and application errors. Security events, based on an Audit policy, are recorded in the security log. System events automatically configured by Windows 2000 are recorded in the system log. Applications events determined by the application developer are recorded in the application log.

After events are recorded in these logs, view and analyze the logs to detect activities and events that require administrative consideration. Based on your analysis of the logs, you may need to resolve security violations, address system problems, or reallocate resources. You may also need to recommend changes in Audit policy, audit settings, security settings, application configuration, or system configuration.

Introduction to Event Logs

Topic Objective
To illustrate an example of the actions associated with events and event logs.

Lead-in
Event logs enable you to monitor information about hardware, software, system problems, and security.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Windows 2000 records events in three types of logs: the system log, the application log, and the security log.

Explain that depending on the services that run on your server, you may see additional logs.

Event logs enable you to monitor information about hardware, software, system problems, and security. You view these logs to detect activities and events that require your attention. Logs can also be used to provide a history of events.

Windows 2000 records events in three types of logs:

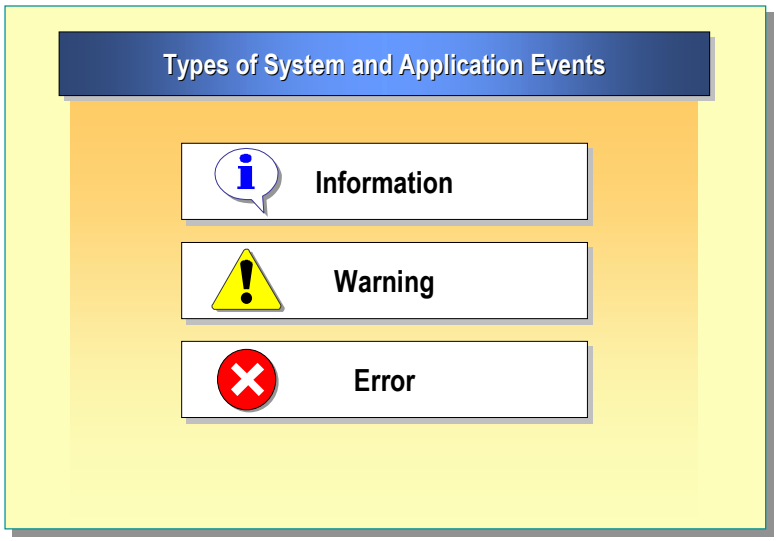
- *The system log*. This log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows 2000.
- *The application log*. This log contains events logged by applications or programs. For example, a database program records a file error in the application log. The program developer decides which events to record. Dr. Watson application logs are also viewable in this log. Dr. Watson for Windows 2000 is a program error debugger. When an application exception (or program error) occurs, Dr. Watson generates a log file (Drwtsn32.log).
- *The security log*. This log records security events such as valid and invalid logon attempts in addition to events related to resource use, such as creating, opening, or deleting files. An administrator specifies what events are recorded in the security log. For example, if you have enabled log on auditing, all attempts to log on to the system are recorded in the security log.

Note All users can view application and system logs, but security logs are accessible only to system administrators.

Types of System and Application Events

Topic Objective
To illustrate the types of system and application events.

Lead-in
Types of system and application events are information, warnings, and errors.



**********ILLEGAL FOR NON-TRAINER USE**********

There are three types of system and application events: Information, Warning, and Error. Each event contains detailed information such as the type of event and the service associated with the event. Use event information to accurately identify the event and take appropriate action. System events are generated by Windows 2000 and recorded in system logs. Application events are generated by applications and recorded in application logs. System and application developers determine the system and application events that are recorded.

Mention to the students the description of each type of event.

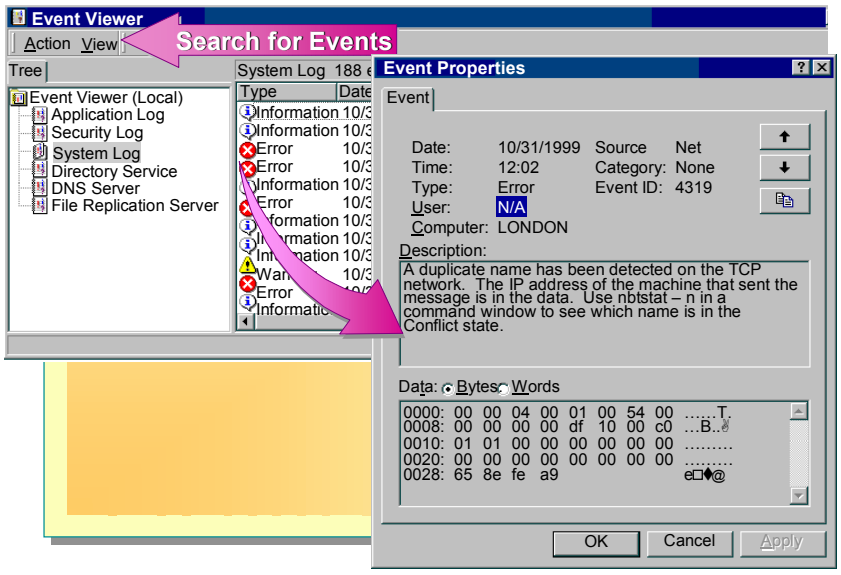
The types of system and application events are described in the following table.

Type of event	Description
Information	The successful operation of an application, driver, or service. For example, when a significant service, such as the Event Log service, starts successfully, Windows 2000 will log an Information event.
Warning	An event that is not necessarily significant but may indicate a future problem with system operations. For example, when disk space is low, Windows 2000 will log a warning. A virus detection program may log an error when a virus is detected.
Error	A significant problem with system operations, such as loss of data or loss of functionality. For example, if a service fails to load during startup, Windows 2000 will log an error.

Viewing Event Logs

Topic Objective
To illustrate the interface for viewing event logs.

Lead-in
Use Event Viewer to view the event logs, which you can use to monitor information about hardware, software, system problems, and security events.



**********ILLEGAL FOR NON-TRAINER USE**********

System and application events are logged in their associated log files sequentially, from most recent to oldest. The log files contain a lot of information about each event that occurs. Monitor information about hardware, software, system problems, and security events by viewing these event logs in Event Viewer. To facilitate viewing, search for specific events.

Viewing a Log Locally

Delivery Tip
Demonstrate Event Viewer. Select a log to view and point out the event properties in the log.

Use Event Viewer to view detailed information about each event in a log. To open Event Viewer, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**. Select the log that you want to view in the console tree of Event Viewer. In the details pane, Event Viewer displays a list of log entries and summary information for each entry. To view the more detailed information about an event, double-click the event.

Note In addition to viewing a log locally, you can view a log for a remote computer. To view a log on a remote computer, in Event Viewer, right-click **Event Viewer (Local)**. On the **Context** menu, click **Connect** to another computer. Select the domain in which the computer exists, and then select the computer to which you want to connect.

Examining Event Properties

In addition to the date, time, and event ID, you can view the properties of an event log that are described in the following table.

Property	Description
Source	Displays the Windows 2000 system component, application, or security event that generated the log.
Category	Defines the event, as set by the source, so that the programmer can further define the event as it occurs.
Type	Displays the type of event: Error, Warning, or Information.
User	Displays the user name if the event is attributed to a specific user.
Computer	Displays the exact name of the computer where the logged event occurred.
Description	Displays a text description of the event. Text descriptions are created by the source of the event.
Data	Displays binary data generated by the event. This information is best interpreted by someone familiar with the source application.

Delivery Tip
Demonstrate searching for a specific event or for a group of events.

Locating Events

Search for specific events in Event Viewer to help you determine trends or research events. Perform the following types of searches:

- Search for specific events by using the **Find** command on the **View** menu. For example, if a particular event seems related to system problems, search the event log to find other instances of the same event to judge the frequency of an error.
- Search for a group of events by filtering the log. For example, if you suspect a hardware component is the origin of system problems, filter the system log to show only those events generated by that component. To use the filter feature, right-click **Security Log**, **System Log**, or **Application Log**, click **View**, and then click **Filter**.

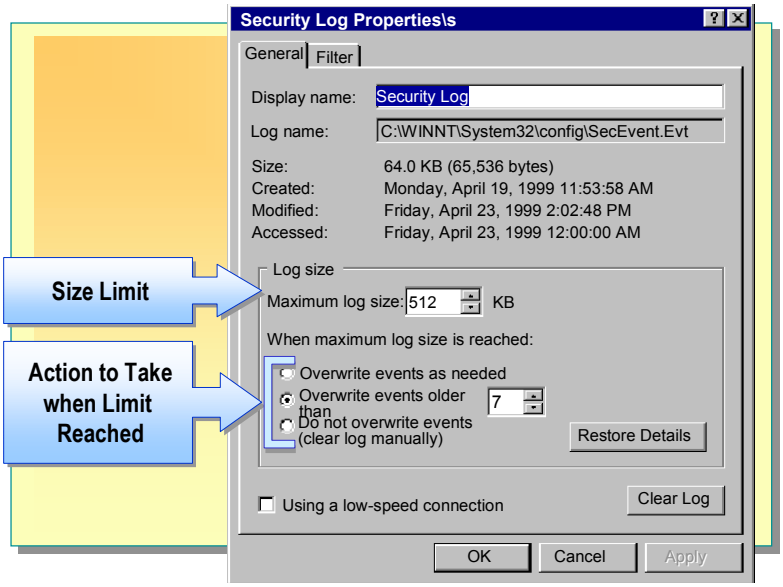
  The log properties you can use to filter out specific events are described in the following table.

Property	Description
Event types	The type of event to view.
Event source	The application or component driver that logged the event.
Category	The category of the event, such as a logon or log off attempt.
Event ID	An event number to identify the event. This number helps product support representatives to track events.
User	A user logon name.
Computer	A computer name.
From: **To:**	The range of events to view from first to last, or a specific date and time.

Limiting the Size of Log Files

Topic Objective
To illustrate the interface for limiting the size of event log files.

Lead-in
You can control the size of the logs and specify the action to take when a log becomes full.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
If your security needs are high, you will want to archive old event entries instead of overwriting them.

Limit the size of event logs if hard disk space is a problem and select a method to overwrite older log event entries with new log entries. Overwriting older event logs is called *event log wrapping*. When you enable an **Event log wrapping** option, you lose old entries. If your security needs are high or you want to keep a history of events, you can choose to archive old event entries instead of overwriting them.

To configure the size of logs, select the log in Event Viewer, and then display the **Properties** dialog box for the log. In the **Properties** dialog box for each type of event log, you can control:

- The size of each log, which can range from 64 kilobytes (KB) to 4 gigabytes (GB). The default size is 512 KB.
- The action that Windows 2000 takes when a log is full. You can configure the **Event log wrapping** options described in the following table.

Option	Description
Overwrite events as needed	You may lose information if the log becomes full before you archive it. However, the setting requires no maintenance. Choose this option when you review the log frequently, so that you will review events before they are overwritten. Or, choose this option when security is low.
Overwrite events older than *x* days	Enter the number of days. You may lose information if the log becomes full before you review or archive it, but you will only lose information older than the days you specified. Choose this option when you review the log every three to five days.

(continued)

Option	Description
Do not overwrite events (clear log manually)	This option requires you to clear the log manually. When a log becomes full, Windows 2000 will stop recording events in the log. However, Windows 2000 does not overwrite any security log entries. Choose this option when security is very high and you do not want to lose any logged events.

Be sure to mention the Caution to the students.

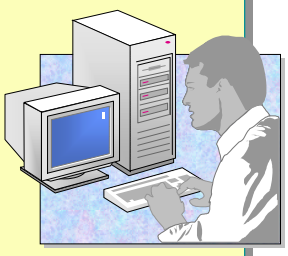
Caution If you click the **Do not overwrite events (clear log manually)** option, you must periodically archive and clear the log manually. When the log is full, Windows 2000 displays a status message indicating the log is full. In addition, Windows 2000 can be configured to shut down when the security log is full. This prevents someone from overwriting the security logs to hide activities that may compromise the security of your network. It is also important to configure a log file size that is large enough to accommodate the log files until they are archived and cleared.

Managing Event Logs

Topic Objective
To identify some of the tasks for managing event logs.

Lead-in
You archive logs to maintain a history of logged events and compare logs from different times to track trends.

- **Archive Event Logs to:**
  - Track trends to determine resource usage
  - Track unauthorized use of resources
  - Keep records when required by law
- **Select a File Format to View Archived Logs in Other Applications**
  - Log-file format (.evt)
  - Text-file format (.txt)
  - Comma-delimited text-file format (.csv)
- **Clear Event Logs When You Choose Not to Overwrite The Logs**



**********ILLEGAL FOR NON-TRAINER USE**********

There are a variety of tasks you perform when you manage event logs. You can archive event logs including determining the format they are saved in. In some instances you must manually clear the logs.

Archiving Event Logs

Delivery Tip
Demonstrate how to archive a log, view a log, and clear archived logs.

You archive logs to maintain a history of logged events and compare logs from different times in order to track trends. Viewing trends helps you determine resource use and plan for growth. You can also use archived security logs to determine a pattern of unauthorized use of resources. Many organizations have policies for saving archived logs for a specified period of time. Some organizations, such as government agencies and banks, are required by law to save archived logs.

Mention the option available when archiving a log.

To archive a log or to view an archived log, select the log in Event Viewer. On the **Action** menu, click one of the options described in the following table.

To	Do this
Archive the log	Click **Save Log File As**, and then type a file name.
View an archived log	Point to **New**, and then click **Log View**. In the **Add Another Log View** dialog box, click **Saved**, and then provide the path to the log.

Selecting a File Format

Save event logs in other formats so that you can view log data in other applications. For example, use a spreadsheet application, such as Microsoft Excel, to manipulate data so that you can track trends easier. Save event logs in one of three file formats:

- Log-file format (.evt). Enables you to view the archived log again in Event Viewer.
- Text-file format (.txt). Enables you to view the information in an application such as a word processing program.
- Comma-delimited text-file format (.csv). Enables you to view the information in an application such as a spreadsheet or database.

Key Point
The text-file or comma-delimited text-file format of an event log does not contain the binary data normally contained in an event. This means some information is lost when saving to a file using these types of formats.

Important Logs saved in text-file or comma-delimited text-file format do not retain the binary data contained within the event. This binary data may contain additional information to aid you in troubleshooting.

Manually Clearing an Event Log

If you select the **Do not overwrite events (clear log manually)** option in the **Properties** dialog box of an active log, you must periodically clear the log when the log reaches a certain size or when a message notifies you that the log is full.

Delivery Tip
Open the interface and show the students where to manually clear an event log, but *do not* clear the log.

To clear an event log, perform the following steps:

1. In the console tree, click the log you want to clear.
2. On the **Action** menu, click **Clear all Events**.
3. Click **Yes** to save the log before clearing it.

   -Or-

   Click **No** to permanently discard the current event records and start recording new events.

◆ Using Task Manager to Monitor System Resources

Topic Objective
To identify topics related to monitoring system resources using Task Manager.

Lead-in
Task Manager provides information about programs and processes running on a computer.

- **Monitoring Programs**
- **Monitoring Processes**
- **Monitoring Performance**

**********ILLEGAL FOR NON-TRAINER USE**********

Ensure that students can define a process.

Task Manager provides real-time information about applications currently running on your system, the processes and memory usage or other data about those processes, and statistics on memory and processor performance.

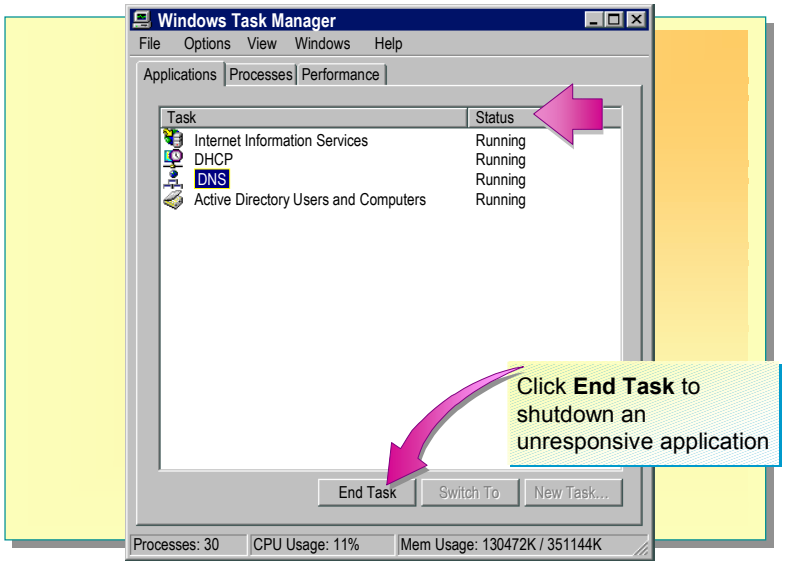
For example, you can use Task Manager to identify an application or process that is using a disproportionate amount of system resources. In addition, the Task Manager status bar provides you with measurements of a system or program activity.

Important A process is a program running in the foreground or background in reserved memory space that performs a specific task. A process can be part of an application, and an application can have many processes. Winword.exe and Services.exe are examples of processes.

Monitoring Programs

Topic Objective
To illustrate the interface for monitoring programs using the Task Manager.

Lead-in
You use the Applications tab to view the status of programs running on a computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain that the Application tab only lists applications that are running in the current user's security context.

Use the **Applications** tab of Task Manager to view the status of applications running on the computer and to identify the process associated with an application. In addition, use this tab to shut down an unresponsive application.

On the **Application** tab, you can perform the following tasks:

- View all applications that are presently running and the status of each application. The status is either Running or Not Responding.
- End an unresponsive application. To shut down an unresponsive application, press CTRL+ALT+DELETE, click **Task Manager**, click the **Applications** tab, click the program that is not responding, and then click **End Task**.

Caution Any data entered or changes made in that application and not saved will be lost.

- Identifying a process associated with an application. To identify the process associated with an application, select the application for which you want to identify processes, right-click the application, and then click **Go To Process**. The **Processes** tab appears and the associated process is highlighted.

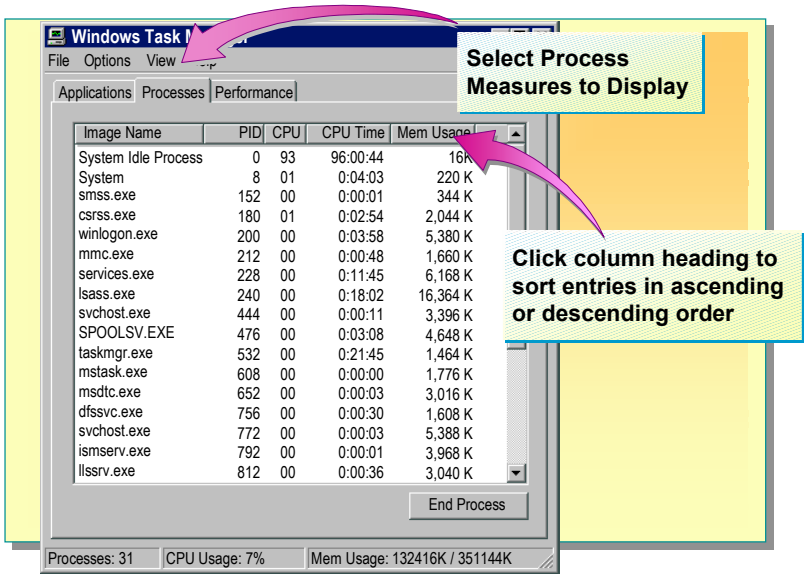
Delivery Tips
Demonstrate ending an application. You will need to have an application running that you can delete.

Then demonstrate identifying the process associated with an application.

Monitoring Processes

Topic Objective
To illustrate the interface for monitoring processes in the Task Manager.

Lead-in
You use the **Processes** tab to view information about the processes and programs currently running on your system.



**********ILLEGAL FOR NON-TRAINER USE**********

Ensure that students know what an address space is.

Use the **Processes** tab to view a list of running processes and their *measures*. Measures are measurements of a process, such as total processor time or the amount of memory in use. The list that appears on the **Processes** tab includes all processes that run in their own address space, including all applications and system services. Both the user and the system can initialize a process, but you can only end a process that is initialized by a user.

Viewing Process Measures

Explain that 23 process measures are available in Task Manager. The measures shown in the table are the most commonly used.

Some of the process measures you can view on the **Processes** tab in Task Manager are described in the following table.

Property	Description
CPU	The current percentage of the CPU time used by the process. If the operating system is not running a specific process, it runs **System Idle Process**, which is a percentage of time that the computer is not processing other tasks. On a system with low utilization, **System Idle Process** may approach 100 percent.
CPU Time	The total processor time, in seconds, used by the process since it was started.
Mem Usage	The amount of main memory, in kilobytes, used by the process.
I/O Read Bytes	The number of bytes read in input/output (I/O) operations generated by a process, including file, network, and device I/Os.
I/O Write Bytes	The number of bytes written in I/O operations generated by a process, including file, network, and device I/Os.

To display other properties, click **View**, and then click **Select Columns**. Select the items you want to appear as column headings, and then click **OK**.

Mention that by sorting the processes an administrator can determine high-usage processes.

Using Process Measures to Identify Resource Use

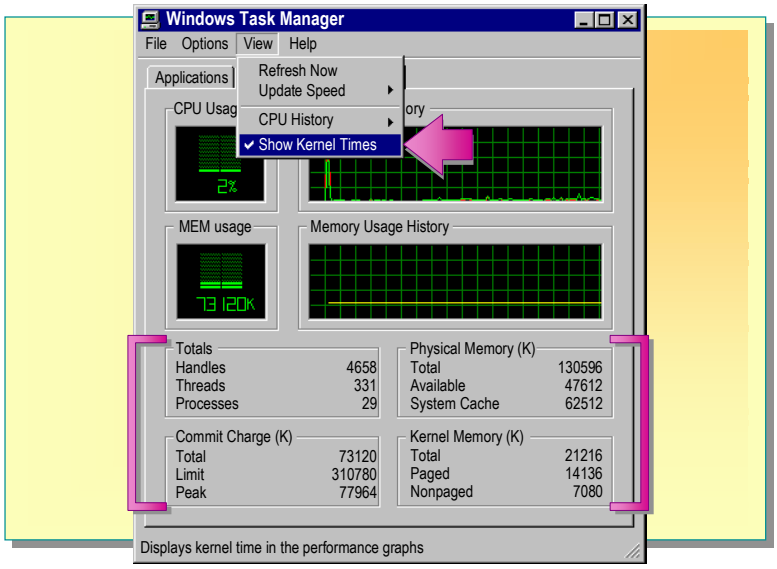
Use the **Process** tab in Task Manager to identify the resource use of a program. After you identify the applications that are using the most processor time, move some of these applications to another computer to distribute the workload. Sort column entries ascending or descending order to identify high usage.

For example, to identify the high-processor use by an application, click the **CPU** column. The first time you click the column, it sorts the applications in ascending order of usage. Clicking again sorts the applications in descending order of CPU usage. You can only sort by one column at a time.

Monitoring Performance

Topic Objective
To illustrate the interface for monitoring performance in Task Manager.

Lead-in
The **Performance** tab displays a dynamic overview of your computer's current performance.



**********ILLEGAL FOR NON-TRAINER USE**********

To monitor the current performance of your computer, you use the **Performance** tab. This tab displays a dynamic overview of the computer's current performance, including a graph and numeric display of processor and memory usage.

This table is an overview of the measures on the **Performance** tab. Briefly describe some of the process measures you can view. Do not go into too much detail.

Explain that virtual memory and page files will be discussed later in the module.

Viewing Process Measures

Some of the process measures you can view on the **Performance** tab in Task Manager are described in the following table.

Process measures	Description
Totals	The number of handles, threads, and processes running on the computer. A *handle* is a variable that is used to access a device or object such as a file, window or dialog box. A *thread* is unit of execution with a process.
Physical Memory	**Total**: Amount of physical RAM, in kilobytes, installed in the computer. **Available**: Amount of physical memory, in kilobytes, available to processes. **System Cache**: Amount of physical memory, in kilobytes, released to the file cache on demand.

(continued)

Process measures	Description
Commit Charge	**Total**: Size of virtual memory, in kilobytes, in use by all processes. *Virtual memory* is disk space that is used by the operating system to act as RAM memory. **Limit**: Amount of virtual memory, in kilobytes, that can be committed to all processes without enlarging the paging file. The *page file* moves pages of data back and forth between physical memory and the hard disk. **Peak**: Maximum amount of virtual memory, in kilobytes, used in the session. The commit peak can exceed the commit limit if virtual memory is expanded.
Kernel Memory	**Total**: Sum of paged and nonpaged memory, in kilobytes. **Paged**: Size of the paged pool, in kilobytes, allocated to the operating system. **Nonpaged**: Size of the nonpaged pool, in kilobytes, allocated to the operating system.

Using Performance Measures to View Processor Time

Delivery Tip
Demonstrate how to view processor time in kernel mode.

Use the **Performance** tab in Task Manager to identify the amount of system resources the operating system or an application is using and to view the percentage of processor time that is being used by the kernel mode. The *kernel* is the core of an operating system that manages memory, files, and peripheral devices; maintains the time and date; launches applications; and allocates system resources.

To view the percentage of processor time that is in kernel mode, on the **View** menu, click **Show Kernel Times**.

The processor time in kernel mode appears in red in the graphs. This is a measure of the time that applications are using operating system services. The remaining time, shown in green, is known as user mode. This is a measure of the time that is spent running threads within the application code.

Lab A: Using Task Manager and Event Viewer

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will use Task Manager and Event Viewer, including managing event logs.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Monitor application performance by using Task Manager.
- Shut down applications by using Task Manager.
- Review computer activity by using Event Viewer.
- Manage event logs.
- Find information in event logs.

Prerequisites

Before working on this lab, you must have:

- Knowledge about file security in Windows 2000.
- Knowledge about monitoring security in Windows 2000.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Server configured as a member server in the nwtraders.msft domain.
- A user account in the domain named Admin*x* (where *x* is your assigned student number).
- A user account in the domain that does not have administrative privileges. If this user account does not exist, create it now.

Estimated time to complete this lab: 30 minutes

Exercise 1
Monitoring Applications by Using Task Manager

Scenario

You are managing a server running Windows 2000. Your job responsibilities include monitoring the server for performance and security breaches. You are concerned because the performance of your server has recently declined. You suspect that one of the applications that is running on your server uses a disproportionate amount of system resources. You need to find out which application is causing the problems so that you can take corrective action.

Goal

In this exercise, you will run several programs on your computer and then use Task Manager to determine which system resources the programs that are running on your computer are using. You will then use Task Manager to stop a program.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with a password of **domain**, and then run Lab08a1.cmd in the C:\MOC\Win2152b\Labfiles\Lab08 folder.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab08 folder, and then double-click **Lab08a1.cmd** to start several programs. **c.** Close Windows Explorer.
2. Use Task Manager to determine which application uses system resources heavily and which system resources it uses.	**a.** Press CTRL+ALT+DELETE, and then click **Task Manager**. **b.** On the **Applications** tab, review the programs that are running.
Does the list contain any operating system processes? Why or why not? **No. The list contains no operating system process because the Applications tab only lists processes that are running in the current user's security context.**	
2. (*continued*)	**c.** Click the **Performance** tab.

Tasks	Detailed Steps
Which system resources are used heavily? **CPU usage is at or near 100 percent.**	
2. (*continued*)	**d.** Click the **Processes** tab.
Which process is displaying the highest current CPU usage? Does this indicate a problem? **App1-5 has the highest CPU usage. This could indicate a problem because this program's CPU usage is preventing other programs from gaining processor time.**	
Which process has used the most CPU time since your computer was started? Does this indicate a problem? Why or why not? **The System Idle Process has used the most CPU time. This does not indicate a problem because the time that is displayed for the System Idle process indicates that the computer's processor was not busy.**	
2. (*continued*)	**e.** On the **View** menu, click **Select Columns**. **f.** In the **Select Columns** dialog box, select the **I/O Read Bytes** and **I/O Write Bytes** check boxes, and then click **OK**. **g.** Drag the border of the Windows Task Manager window right until you can see all columns.

Tasks	Detailed Steps
Does App1-5 place a heavy load on the hard disk? **App1-5 does not place a heavy load on the hard disk.**	
3. Close the programs App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe, and App1-5.exe by using Task Manager.	**a.** Click **App1-5.exe**, and then click **End Process**. **b.** In the **Task Manager Warning** dialog box, read the warning, and then click **Yes**. **c.** Shut down App1-1.exe, App1-2.exe, App1-3.exe, and App1-4.exe by using Task Manager, and then close Task Manager.

Exercise 2
Reviewing Computer Activity by Using Event Viewer

Scenario

To ensure that your computer is running without problems, you regularly use Event Viewer to review system activity during the last week. Also, your company's security policy requires you to review and archive your computer's system logs weekly.

Goal

In this exercise, you will review the Windows 2000 log files, configure log file archiving, and archive a log file.

Tasks	Detailed Steps
1. Use Event Viewer to determine the last time your computer was started.	**a.** Open Event Viewer from the **Administrative Tools** menu. **b.** In the console tree, click **System Log** if necessary. **c.** In the details pane, find the most recent event with eventlog as its source, and then double-click the event.
Note: Windows 2000 automatically starts the event log service each time that the computer starts. The time that the event log service started is the approximate time that your computer started.	
1. (*continued*)	**d.** Click **OK** to close the **Event Properties** dialog box. **e.** Review the types of events in each of the event logs. **f.** Do not close Event Viewer.

Exercise 3
Archiving the Application Log

Scenario

Your company's security policy requires you to review and archive the application log weekly.

Goal

In this exercise, you will archive your computer's application log.

Tasks	Detailed Steps
1. Save the Application Log file as *yyyy-mm-dd*.evt (where *yyyy* are the current year, *mm* is the first two letters of the current month, and *dd* is the current date) in the C:\MOC\Win2152b\Labfiles\Lab08 folder, and then clear the Application Log.	**a.** In Event Viewer, in the console tree, click **Application Log**. **b.** On the **Action** menu, click **Save Log File As**. **c.** In the **Save "Application Log" As** dialog box, in the **Save in** box, navigate to the C:\MOC\Win2152b\Labfiles\Lab08 folder, and then save the Application Log file as *yyyy-mm-dd*.evt (where *yyyy* is the current year, *mm* is the current month, and *dd* is the current day). **d.** On the **Action** menu, click **Clear all Events**. **e.** In the **Event Viewer** message, click **No** to clear the events without saving them.

Exercise 4
Searching for Specific Events in a Saved Event Log File

Scenario

Your company's security department suspects that there have been security breaches in your network in the past. They have requested that you review archived security logs to provide possible evidence for such actions. The security department requires information about any cases of unauthorized users attempting to gain access to files in the Projects folder.

Goal

In this exercise, you will filter for specific events and the search the Security Log for instances of access to the Projects folder.

Tasks	Detailed Steps
1. Open the saved security log file, C:\MOC\Win2152b\Labfiles\Lab08\Lab08A.evt, and then view the first entries.	**a.** In the console tree, right-click **Event Viewer (Local)**, and then click **Open Log File**. **b.** In the **Open** dialog box, in the **Look in** box, navigate to the C:\MOC\Win2152b\Labfiles\Lab08 folder if necessary, and then click **Lab08A.evt**. **c.** In the **Log Type** box, click **Security**, and then click **Open**. **d.** Double-click the first event in the log. **e.** View the information in the security event, and then click the down arrow to move to the next event.
Is examining each event the most efficient way to look for specific events? **No. Because of the high number of events that you will have in the logs, you will need some way to filter out the events that do not concern you during the present search.**	
1. (*continued*)	**f.** Click **Cancel** to close the **Event Properties** dialog box.
2. Filter the log entries so that only failure events appear, and then sort the entries by category.	**a.** In the console tree, right-click **Saved Security Log**, point to **View**, and then click **Filter**. **b.** In the **Saved Security Log Properties** dialog box, under **Event types**, clear all of the check boxes except for the **Failure audit** check box, and then click **OK**. **c.** Click the **Category** column heading to sort the log entries.

(*continued*)

Tasks	Detailed Steps
3. Search the saved security log for events that indicate an unauthorized attempt to access the E:\Projects folder. Determine which user attempted to access the folder and whether this was a one-time attempt.	**a.** Right-click **Saved Security Log**, point to **View,** and then click **Find**. **b.** In the **Find in local Saved Security Log** dialog box, under **Event Types**, clear all of the check boxes except for the **Failure audit** check box. **c.** In the **Event ID** box, type **560**
Note: An event ID of 560 indicates a failure to access an object, such as a file or directory.	
3. (*continued*)	**d.** In the **Description** box, type **e:\projects** and then click **Find Next** to search through the events. *The next event that meets the search criteria is highlighted. Because this log was saved on a computer that does not belong to your network, Windows 2000 cannot resolve the security identifier (SID) to a user name. Therefore, the User column displays the SID.* **e.** Reposition the **Find in local Saved Security Log** dialog box if necessary, and then in Event Viewer, double-click the highlighted event to open it.
Based on the information in the description section of the event, what is the Primary User Name of the user that was attempting to access the folder? **User1.**	
3. (*continued*)	**f.** Click **Cancel** to close the **Event Properties** dialog box. **g.** Right-click **Saved Security Log**, point to **View**, and then click **All Records**. **h.** Right-click **Saved Security Log**, point to **View**, and then click **Find**. **i.** In the **Find in local Saved Security Log** dialog box, under **Event** types, clear all of the check boxes except for the **Failure audit** check box. **j.** In the **Event ID** box, verify that **560** appears. **k.** In the **Description** box, type **User1** and then click **Find Next**. **l.** Click **Find Next** repeatedly until the **Event Viewer** message appears, advising you that you have reached the end of the event log. **m.** In the **Event Viewer** dialog box, click **No** to discontinue searching from the beginning of the log.

(*continued*)

Tasks	Detailed Steps
Was this a one-time attempt or a repeated attempt? **User1 attempted to access the folder several times because there are several events logged.**	
4. Search for events that indicate that User1 was able to access the E:\Projects folder.	**a.** In the **Find in local Saved Security Log** dialog box, under **Event types**, clear all of the check boxes, except for the **Success audit** check box. **b.** In the **Event ID** box, verify that **560** appears. **c.** In the **Description** box, verify that **User1** appears, and then click **Find Next**. **d.** Double-click the highlighted event to open it. **e.** View the details of the event to become more familiar with the information available in each event that is recorded, and then click **OK** to close the **Event Properties** dialog box. **f.** Click **Close** to close the **Find in local Saved Security Log** dialog box.

Exercise 5
Saving a Security Log File in an Alternate File Format

Scenario

Your company's security department requested a record of a recent security breach on one of your servers. They requested that you supply this information in a comma-delimited text file, so that they can import the information into Microsoft Excel for further analysis.

Goal

In this exercise, you will save the previously saved security log file as a comma-delimited text file.

Tasks	Detailed Steps
1. Save the Lab08A.evt security log in comma-delimited format as C:\MOC\Win2152b\Labfiles\Lab08\Seclog.csv, and then use Notepad to view this file.	**a.** In the console tree, right-click **Saved Security Log**, and then click **Save Log File As**. **b.** In the **Save "Saved Security Log" As** dialog box, in the **Look in** box, navigate to the C:\MOC\Win2152b\Labfiles\Lab08 folder if necessary, and then in the **File name** box, type **Seclog** **c.** In the **Save as type** box, click **CSV (Comma delimited) (*.csv)**, and then click **Save**. **d.** Close Event Viewer. **e.** Click **Start**, and then click **Run**. **f.** In the **Open** dialog box, type **Notepad.exe C:\MOC\Win2152b\Labfiles\Lab08\Seclog.csv** and then click **OK**. **g.** Maximize Notepad. **h.** On the **Edit** menu, click **Find**. **i.** In the **Find what** box, type **e:\projects** and then click **Find Next**. **j.** In the **Find** dialog box, click **Cancel**. **k.** Close Notepad, and then log off.

◆ Using System Monitor to Monitor System Performance

Topic Objective
To identify the topics related to using System Monitor to monitor system resources.

Lead-in
If you need more detail than is provided by Task Manager, you can use System Monitor to obtain more comprehensive information on your computer or other computers on your network.

- **Objects, Instances, and Counters**
- **Adding Counters**
- **Viewing Counter Data**

**********ILLEGAL FOR NON-TRAINER USE**********

If you need more detail than is provided by Task Manager, you can use System Monitor to obtain more comprehensive information about your computer or other computers on the network. Use System Monitor in Performance in Microsoft Management Console (MMC) to collect and view real-time or logged data about memory, disk, processor, and network activity. Use this information to diagnose how the system and applications are functioning to ensure that you are optimizing the system. For example, you can determine if your system is low on disk space.

System Monitor information can be viewed in graph, histogram (bar chart), or report form. Graphs, histograms, and reports can be viewed in a browser and printed when performance data is saved as a Hypertext Markup Language (HTML) file.

Objects, Instances, and Counters

Topic Objective
To illustrate objects, counters, and instances in System Monitor.

Lead-in
Understanding how objects, instances, and counters are related to each other, is critical to efficiently using System Monitor.

- **Objects In System Monitor Are Major Components or Subsystems of the Computer System**
- **Instances Are Multiples of the Same Object**
- **Counters:**
  - Are Measurements of different aspects of objects
  - Continually gather data on objects
  - Provide data on all instances of an object
  - Can be selected to displayed in System Monitor

**********ILLEGAL FOR NON-TRAINER USE**********

Provide the definition for objects, instances, and counters.

Ensure that students know that the objects in System Monitor are not the same as objects in Active Directory.

Understanding how objects, instance, and counters are related to each other, is critical to efficiently using System Monitor. They are:

- *Objects*. In System Monitor, objects are major components or subsystems of the computer system. They can be hardware, such as the hard disk, or software such as a process. There are a fixed number of objects in Windows 2000.

  Important The objects in System Monitor are not the same as the objects in the Active Directory™ directory service and have no connection.

- *Instances*. Instances are multiples of the same object type. For example, if a system has multiple processors, the Processor object type will have multiple instances.
- *Counters*. Counters gather data on different aspects of objects. For example, for the Process object, counters gather data on the processor time and the user time. Counters are built in to the operating system and continually capture data, whether it is visible in System Monitor or not. If an object type has multiple instances, counters track statistics for each instance or the total of all instances.

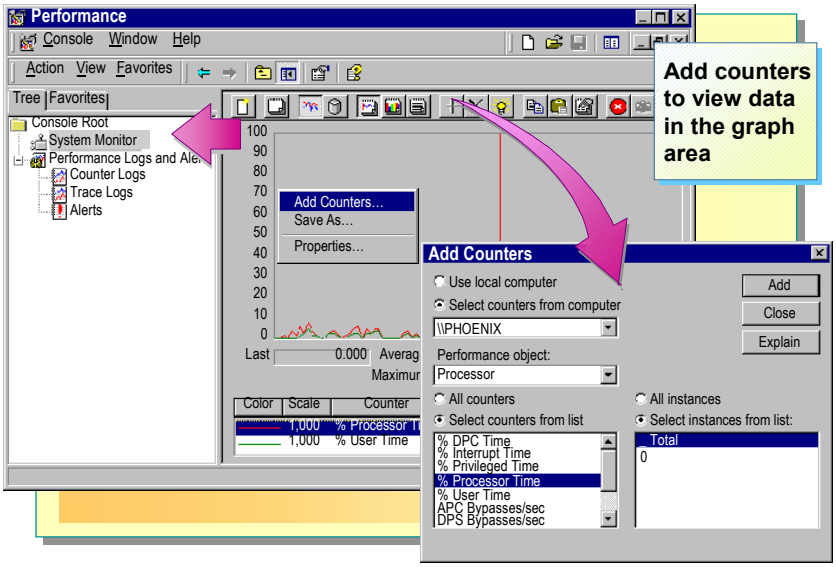
  In System Monitor, you can specify which counters are to be displayed.

  Note The process measurements in Task Manager are counters, but you have no control over what is displayed.

Adding Counters

Topic Objective
To illustrate the interface for monitoring performance in Windows 2000.

Lead-in
The Performance console hosts two tools: System Monitor and Performance Logs and Alerts.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Open Performance and add a counter as you describe the System Monitor. Point out that each object has several counters and select an object for which there are at least two instances.

Because counters continually gather data on system performance, when you add counters, you are adding their displays in System Monitor. This allows you to monitor system performance.

Note Performance in Microsoft Management Console (MMC) hosts two components: System Monitor and Performance Logs and Alerts.

To add counters in System Monitor, perform the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Performance**.

   When you start Performance for the first time, a blank System Monitor graph appears.

2. Right-click the System Monitor details pane, and then click **Add Counters**.
3. In the **Performance object** list, select an object to monitor.

   The objects that are available are based on the services and applications installed on the local computer. You can choose several counters for each object. The following table describes core objects in Windows 2000 System Monitor.

Explain that there are more than 350 counters available in System Monitor. For a list of available counters, see the Server Operations Guide section of the *Microsoft Windows 2000 Server Resource Kit*.

Object name	Description
Cache	Area of physical memory that holds recently used data.
Memory	RAM used to store code and data.
Objects	Certain system software objects.
Paging File	File used to back up virtual memory allocations.

(continued)

Object name	Description
Physical Disk	Hardware disk unit (spindle or redundant array of independent disks [RAID] device).
Process	Software object that represents a running program.
Processor	Hardware unit that executes program instructions.
Server	Service that responds to data requests from clients on the network.
System	Counters that apply to all system hardware and software.
Thread	The part of a process that uses the processor.

After you select an object, the counters associated with that object will appear in the list.

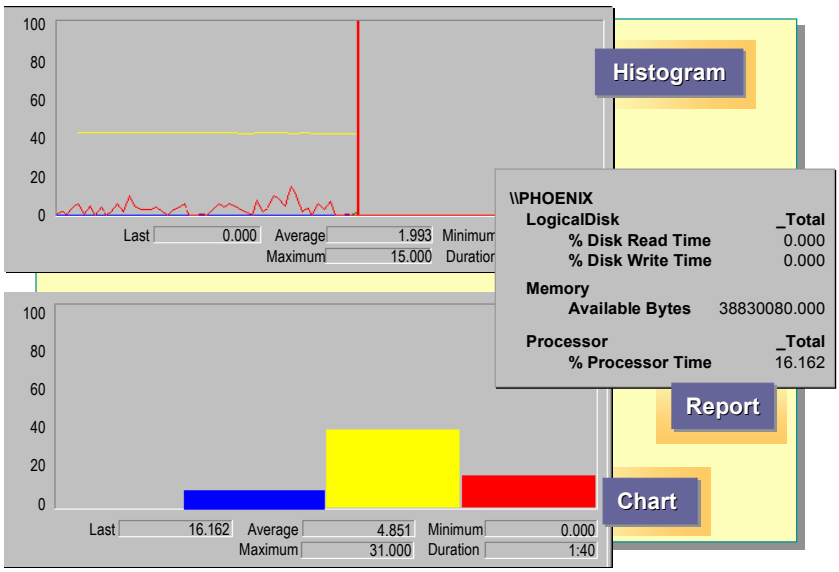
Note Click **Explain** to view a description of the counters listed in the **Add Counters** dialog box.

4. Click **All counters** or **Select counters from list** to choose individual counters.
5. If an object has instances, click **All instances** or **Select instances from list** to choose individual instances.
6. Click **Add**, and then click **Close** to close the **Add Counters** dialog box.

Viewing Counter Data

Topic Objective
To illustrate the three ways you can view counter data.

Lead-in
After you add counters, you can view the data of your counter in three different ways.



**********ILLEGAL FOR NON-TRAINER USE**********

After you add counters, you can view the data of your counters in real time. Display this data in three different ways:

Key Points
An administrator can view counter data in one of three different ways: histogram, report, or chart.

- *Histogram*. Displays data in a bar chart. This view is useful for simplifying graphs with multiple counters.
- *Report*. Displays numerical data in columns. This view is useful for collecting data that you can export into a spreadsheet, such as Excel.
- *Chart*. Displays data in a line graph. This view is useful for monitoring real time data or data logged over time.

Change and customize display settings by right-clicking the System Monitor details pane, and then clicking **Properties**. For information about specific settings that you can change, see the Server Operations Guide portion of the *Windows 2000 Server Resource Kit*.

Mention the Tip and that an administrator can save performance data as an HTML file.

Tip If you have several counters, it may be difficult to discern data from a specific counter. To accentuate the line or bar for a selected counter with white (default) or black (for light backgrounds), click **Highlight** on the toolbar or press CTRL+H.

Save performance data as an HTML file, and then open the HTML file from Microsoft Internet Explorer or another Web browser. You can also print the data from the browser. To save data as an HTML file, right-click the details pane of System Monitor, and then type a file name for the HTML file.

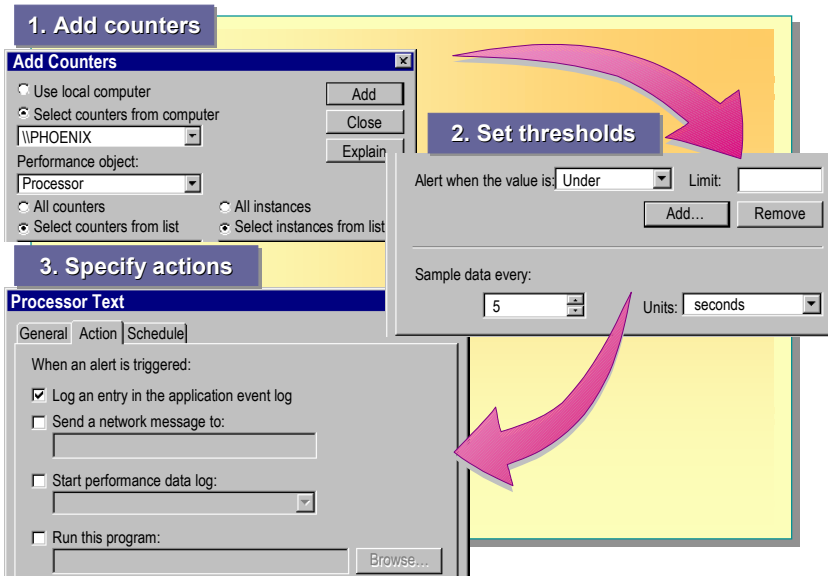
Note In addition to viewing counter data live, you can log the data in Performance Logs and Alerts in Performance and view the data later. There are two types of logs. Counter logs record data about hardware resources and system services based on performance over time. Counter logs are useful for tracking trends. Trace logs collect event traces that measure performance statistics associated with events such as disk and file I/O. An event starts the logging of counter data.

For more information about Counter and Trace logs and how to set them up, see Windows 2000 online Help. Search for Performance Logs and Alerts.

Using Alerts

Topic Objective
To illustrate the process for setting alerts.

Lead-in
Setting an alert is a three-step process.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
You can use alerts to warn a user or support professional when certain criteria are met or exceeded.

Use alerts to notify a user or an administrator when indications go beyond a set criteria. In addition, you can use performance logs to collect data on hardware resources, system services, and performance.

Alerts

Alerts are useful if you are not actively monitoring a particular counter but want to be notified when it exceeds or falls below a specified value so that you can investigate and determine the cause of the change. For example, you can set an alert when the percentage of disk space used exceeds 80 percent, or the number of failed logon attempts exceeds a specified number. There are three tasks involved in setting an alert. They are:

1. Select counters to track a specific system activity.
2. Set a threshold value for that activity.
3. Specify an action to take when the threshold is exceeded or falls below a specific value:
   - Send a network message.
   - Run a program.
   - Start a log.

Delivery Tip
Demonstrate setting an alert.

Note To run Performance Logs and Alerts, you must have the right to start or otherwise configure services on the system. Administrators have this right by default.

Setting an Alert

Use Performance Logs and Alerts in the Performance console to set an alert. To set an alert, perform the following steps:

1. In the console tree, double-click **Performance Logs and Alerts**, and then click **Alerts**.
2. In the details pane, right-click **New Alert Setting**, and then provide a name for the alert.
3. On the **General** tab, enter a brief description of the alert setting file in the **Comment** box.
4. Click **Add** to specify objects, counters, instances, and updating information in the **Add Counters** dialog box.
5. After adding counters, specify properties for the sample interval and alert threshold on the **General** tab.
6. On the **Action** tab, ensure that **Log an entry in the application event log** is selected. You can also specify a network message be sent to the computer that triggers the alert.
7. On the **Schedule** tab, define the start and stop parameters for the log under **Start scan** and **Stop scan**, and then click **OK**.

Lab B: Monitoring System Performance

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will monitor system performance, including setting performance alerts and using counters.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Monitor System Performance by using System Monitor.
- Set and review performance alerts.
- Create and view performance logs.

Prerequisites

Before working on this lab, you must have:

- Knowledge about the main hardware components of a computer that is running Windows 2000.
- Experience using Internet Explorer.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- A user account in the domain named Admin*x* (where *x* is your assigned student number).
- A user account in the domain that does not have administrative privileges. If this user account does not exist, create it now.
- A printer that is called Color Printer.

Estimated time to complete this lab: 30 minutes

Exercise 1
Monitoring Performance by Using System Monitor

Scenario

As part of your job responsibilities you need to ensure that your server is running efficiently and that you are alerted early to any problems that users may be experiencing. You also need to investigate problems that users are reporting. You are concerned about the impact that disk defragmentation has on your computer's performance. You want to know what the impact is so that you can decide whether you need to schedule disk defragmentation for times when users do not access your server.

Goal

In this exercise, you will run System Monitor and configure it with several counters that represent processor, memory, and disk usage.

Tasks	Detailed Steps
1. Log on as Admin*x* (where *x* is your assigned student number), open Performance from the **Administrative Tools** menu, and then add the counters Processor\% Processor Time, Memory\Available Bytes, PhysicalDisk\% Disk Read Time, and PhysicalDisk\% Disk Write Time.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Performance from the **Administrative Tools** menu. **c.** In the console tree, verify that **System Monitor** is selected. **d.** Right-click an open area of the details pane, and then click **Add Counters**. *Under **Select counters from list**, the % Processor Time counter for the Processor object is selected by default. This it is the most commonly used counter for monitoring.* **e.** In the **Add Counters** dialog box, click **Explain**, and then read the explanation of the % Processor Time counter. **f.** Under **Select instances from list**, ensure that **_Total** is selected, and then click **Add**. **g.** In the **Performance object** box, click **Memory**, under **Select counters from list**, click **Available Bytes**, and then click **Add**. **h.** In the **Performance object** box, click **PhysicalDisk**, under **Select counters from list**, click **% Disk Read Time**, and then click **Add**. **i.** Under **Select counters from list**, click **% Disk Write Time**, and then click **Add**. **j.** Click **Close** to close the **Add Counters** dialog box, and then minimize Performance.
2. Use System Monitor to view the effects of performing a disk fragmentation analysis on your computer.	**a.** Open Computer Management from the **Administrative Tools** menu. **b.** In the console tree, under **Storage**, click **Disk Defragmenter**. **c.** In the details pane, click **Analyze**. **d.** When the disk defragmentation analysis is complete, click **Close** to close the **Analysis Complete** message.

Tasks	Detailed Steps
2. (*continued*)	**e.** Close Computer Management, and then restore Performance. **f.** In the details pane, click the **Freeze Display** button, which shows a red circle with a white X. **g.** At the bottom of the details pane, under **Counter**, verify that **% Processor Time** is selected. **h.** Hold down the CTRL key, and then press H to highlight the currently selected counter. **i.** Use the down and up arrow keys on your keyboard to view other counters.

Which system resources did Disk Defragmenter primarily use?

Disk Defragmenter used %Processor Time and %Disk Read Time. There was also some disk write activity.

2. (*continued*)	**j.** At the bottom of the details pane, under **Object**, right-click **Memory**, and then click **Properties**. **k.** In the **System Monitor Properties** dialog box, on the **Data** tab, under **Counters**, verify that *server***Memory****Available Bytes** (where *server* is your assigned computer name) is selected. **l.** In the **Scale** box, click the smallest value available, and then click **OK**.

Did memory use fluctuate much while Disk Defragmenter was running?

No.

2. (*continued*)	**m.** Right-click an open area of the details pane, and then click **Save As**. **n.** In the **Save As** dialog box, in the **Save in** box, navigate to the Desktop. **o.** In the **File name** box, type **System Overview** and then click **Save**. **p.** Minimize Performance. **q.** On the desktop, double-click **System Overview.htm**. **r.** View the performance information in the Web page, and then close Internet Explorer.

Exercise 2
Setting Performance Alerts

Scenario

You want to be able to take corrective action whenever there are problems with your printer. To accomplish this, you configure your computer to alert you when there are too many documents that are waiting to be printed. A large number of documents in the print queue usually indicate a problem with the printer.

Goal

In this exercise, you will configure a performance alert to notify you when the number of documents in the print queue exceeds five.

Tasks	Detailed Steps
1. Set the Color Printer printer offline.	**a.** Click **Start**, point to **Settings**, and then click **Printers**. **b.** In the Printers system folder, right-click **Color Printer**, and then click **Use Printer Offline**. **c.** Close the Printers system folder.
2. Set an alert that sends a message to your computer whenever processor utilization exceeds 90 percent and that records the occurrence of such events in the event log.	**a.** Restore Performance. **b.** In the console tree, expand **Performance Logs and Alerts**, right-click **Alerts**, and then click **New Alert Settings**. **c.** In the **New Alert Settings** dialog box, type **Print Queue** and then click **OK**. **d.** In the **Print Queue** dialog box, in the **Comment** box, type **More than 5 documents in the print queue** and then click **Add**. **e.** In the **Select Counters** dialog box, in the **Performance object** box, click **Print Queue**, and then under **Select counters from list**, verify that **Jobs** is selected. **f.** Under **Select instances from list**, click **Color Printer**. **g.** Click **Add**, and then click **Close**. **h.** In the **Alert when the value is** box, click **Over**, and then in the **Limit** box, type **5** **i.** Under **Sample data entry**, in the **Interval** box, type **10** and then verify that **seconds** appears in the **Units** box. **j.** On the **Action** tab, verify that the **Log an entry in the application event log** check box is selected. **k.** Select the **Send a network message to** check box, and then type *Server* (where *Server* is your assigned computer name). **l.** On the **Schedule** tab, under **Start scan**, verify that **At** is selected, and then click **OK**. **m.** Minimize Performance.

Tasks	Detailed Steps
3. Trigger the alert that you configured by previewing an OpenGL screen saver. Then review the Application log for alerts.	**a.** Open Notepad, print the blank document to the Color Printer six times, and then close Notepad. *A **Messenger Service** dialog box notifies you that the number of jobs is over the limit value.* **b.** Restore Performance. **c.** In the console tree, click **Alerts**, in the details pane right-click **Print Queue**, click **Stop**, and then minimize Performance. **d.** Close any open **Messenger Service** messages. **e.** Open Computer Management from the **Administrative Tools** menu. **f.** Under **System Tools**, expand **Event Viewer**, and then click **Application**. **g.** In the details pane, double-click an event with SysmonLog as the source. **h.** In the **Event Properties** dialog box, read the description of the event, and then click **OK**. **i.** Close Computer Management.

Exercise 3
Recording System Performance By Using Counter Logs

Scenario

As part of your job responsibilities, you need to monitor the performance of your server. Lately, you have been getting reports from your users stating that your server's performance is often very slow. You cannot reproduce this when you are reviewing performance data by using System Monitor. You decided to create a counter log that records the performance of several system components. The counter log includes data for an extended period.

Goal

In this exercise, you will create a counter log and review data from the log.

Tasks	Detailed Steps
1. Create a counter log that is using the same settings that you saved when using System Monitor earlier in this lab, and then start logging.	**a.** Restore Performance. **b.** In the console tree, right-click **Counter Logs**, and then click **New Log Settings From**. **c.** In the **Open** dialog box, in the **Look in** box, navigate to the desktop, click **System Overview**, and then click **Open**. **d.** In the **Performance Logs and Alerts** dialog box, click **OK**. **e.** In the **New Log Settings** dialog box, type **Long-term monitoring** and then click **OK**. **f.** In the **Long-term monitoring** dialog box, under **Counters**, confirm that all the counters that you added to System Monitor earlier in this lab appear. **g.** Confirm that the **Interval** box displays 1, and that the **Units** box displays seconds. **h.** Click **OK**. **i.** In the **Long-term monitoring** message, click **Yes** to create the Perflogs folder. **j.** In the console tree, click on **Counter Logs**, in the details pane, right-click **Long-term monitoring**, and then click **Start**. **k.** Minimize Performance.
2. Create System Activity by temporarily configuring an OpenGL screen saver.	**a.** Right-click the desktop, and then click **Properties**. **b.** On the **Screen Saver** tab, in the **Screen Saver** box, click **3D Pipes (OpenGL)**, and then click **Preview**. **c.** Do not move your mouse or touch your keyboard for approximately 10 seconds, and then move the mouse to stop the screen saver. **d.** Click **Cancel** to close the **Display Properties** dialog box.

Tasks	Detailed Steps
3. Stop performance logging and then view the log by using System Monitor.	**a.** Restore Performance. **b.** In the details pane, right-click **Long term monitoring**, and then click **Stop**. **c.** In the console tree, click **System Monitor**. **d.** In the details pane, click **View Log File Data**.
Note: To find the correct button, place the mouse pointer on top of each button to see a tool tip.	
3. (*continued*)	**e.** In the **Select Log File** dialog box, in the **Look in** box, navigate to the C:\Perflogs folder. **f.** Click **Long-term monitoring_000001.blg**, and then click **Open**. *System Monitor displays the performance data that you logged earlier.*
Which system resource was most heavily used during the logging period? **The processor was most heavily used.**	
Note: The OpenGL screen savers are very processor intensive. Even previewing them can cause processor usage to increase sharply. You should never configure a server to use one of these screen savers.	
3. (*continued*)	**g.** Close Performance, and then log off.

◆ Optimizing Performance

Topic Objective
To identify the topics related to optimizing performance.

Lead-in
You can optimize performance so that your operating system and applications use system resources more efficiently.

- **The Performance Optimization Process**
- **Examining Memory Performance**
- **Examining Processor Performance**
- **Examining Disk Performance**
- **Examining Network Performance**

**********ILLEGAL FOR NON-TRAINER USE**********

Define baseline and present the information in the Important.

Optimize performance so that your operating system and applications use system resources more efficiently. The level of system performance that you consider acceptable when your system is handling a typical workload and running all required services is its *baseline*. The baseline performance is a subjective standard that the administrator determines based on the typical level of performance under typical workloads and usage. The baseline can be the measure used for setting performance expectations of your users and can be included in any service agreements you may have with your organization.

To maintain your baseline, the most important resources to monitor include:

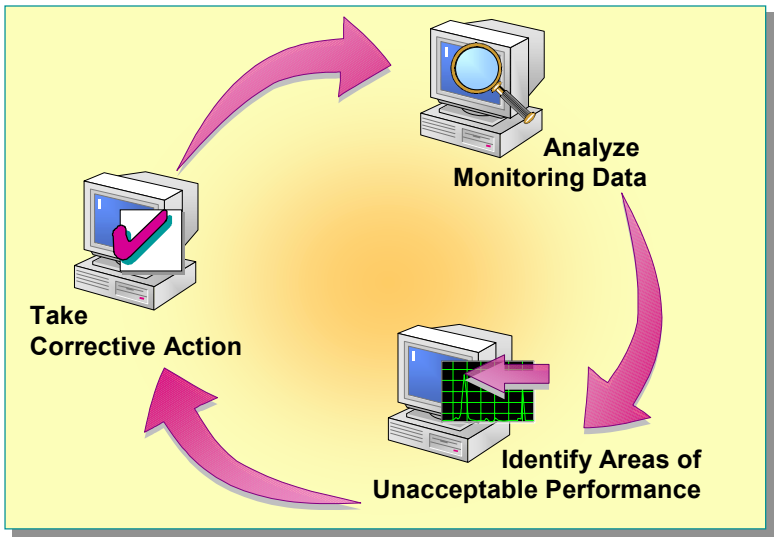
- Memory.
- Processor activity.
- Disk activity.
- Network activity.

Important There are many issues to consider when optimizing system performance. This section is intended as a quick overview. For more information about monitoring and tuning your system's memory, processor, disk systems, and network components, see the chapters on optimization under Performance Monitoring in the Server Operations Guide section of the *Microsoft Windows 2000 Server Resource Kit*.

The Performance Optimization Process

Topic Objective
To illustrate the performance optimization process.

Lead-in
Performance optimization is a constant cycle of measuring and testing, finding problems, and making changes.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Explain that the process of performance analysis is not a perfect science, but an evolving process that considers different environments.

The optimization process helps you to determine what actions to take to improve system performance in response to demands on the system. Performance optimization begins with thoughtful and organized record keeping.

The performance optimization process includes the following tasks:

- Analyzing monitoring data. Analyzing your monitoring data consists of examining counter values that are reported while your system is performing various operations. During this process you should determine:
  - Which processes are most active and which programs or threads (if any) are monopolizing a resource.
  - Whether the overuse of any hardware resource causes a decrease in system performance.
  - Whether there are residual effect of bottlenecks and other hardware resources that are underused. For example, if the system starts to run slower and the hard disk activity increases, this could indicate a hard drive problem or insufficient RAM to support the applications and operating system.

  Using this type of performance data analysis, you can understand how your system is responding to workload demands.

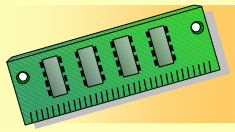
- Identifying areas of unacceptable performance. As a result of this analysis, you may find that your system performs satisfactorily at some times and unsatisfactorily at others. In general, deciding whether or not performance is acceptable is a subjective judgment that varies significantly with variations in user environments. The values you establish as the baselines for your organization are the best basis for comparison. In addition, be aware that performance varies over time and your monitoring needs to include different periods of system usage.
- Taking corrective action. Depending on the causes of these variations and the degree of difference, you may choose to take corrective action or to accept these variations and postpone tuning or upgrading resources to a later date. In some instances, the corrective action may not have enough impact to make the change worthwhile.

Examining Memory Performance

Topic Objective
To identify the topics for optimizing memory performance.

Lead-in
Memory usage is the most important factor in system performance.

- **Establish a Baseline Range for Normal Values to Help Identify Trends and Problems**
- **Use Counters to Examine Memory**
  - Monitor Pages per second
  - Monitor Available Bytes
- **Examine Page Files**
  - Indicates low memory if frequent paging
  - Check the paging file size
  - Use counters to monitor the paging file size



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Low memory conditions can slow the operation of applications and services on your computer and impact the performance of other resources in your system.

Low memory conditions can slow the operation of applications and services on your computer and impact the performance of other resources in your system.

Establishing a Baseline

Examine your physical memory usage during a normal workload to establish a baseline for physical memory usage. The baseline is usually a range of values within which physical memory usage can fluctuate and still provide acceptable performance. Use the baseline to identify trends, such as increasing physical memory demands over time, or to recognize problems that arise from a sudden change.

Delivery Tip
If time permits, show Pages/sec and Available Bytes in the System Monitor.

Using Counters to Examine Memory

All of the processing that occurs on a system occurs in memory, therefore, you must ensure that there is enough memory to support the day-to-day tasks that the system performs. The counters described in the following table are useful for examining the memory object.

Counter	Description
Pages/sec	Indicates the number of requested pages that were not immediately available in RAM and had to be read from the disk or written to the disk to make room in RAM for other pages. If your system experiences a high rate of hard page faults, the value for Pages/sec can be high.
Available bytes	Indicates how much physical memory is remaining after the working sets of running processes and the cache have been served.

If the value for Available Bytes is consistently below the system-defined threshold and the value for Pages/sec spikes continuously, it is likely that your memory configuration is insufficient for your needs.

Key Points
One of the ways you may become aware of a memory shortage is if your system is paging frequently.

Examining Paging Files

One of the ways you may become aware of a memory shortage is if your system is paging frequently.

Paging

Paging is the process of moving virtual memory back and forth between physical memory and the disk. When a computer is low on memory, paging activity increases, therefore, frequent paging indicates a memory shortage.

Increased paging activity causes more work for your disks and competes with other disk transactions that are being performed. In turn, the processor is used less or is doing unnecessary work by processing numerous interrupts due to repeated page faults. (Page faults occur when the system cannot locate requested code or data in the physical memory available to the requesting process.) In the end, applications and services become less responsive.

Note Because excessive paging can make substantial use of the hard disk, it is possible to confuse a memory shortage that causes paging with a disk bottleneck that results in paging.

Delivery Tip
Point out Pagefile.sys in Windows Explorer and compare the size of this file to the file size setting in **System** in Control Panel.

Checking the Paging File Size

To see if a paging file is approaching its upper limit, check the actual file size and compare this value to the maximum paging file size setting in **System** in Control Panel. If these two numbers are close in value, consider increasing initial paging file size or running fewer programs.

Caution If the paging file reaches its maximum size, a warning appears and the computer may stop running.

The paging file is located on the disk where you installed Windows 2000. To check the size of the paging file, view the file size shown for Pagefile.sys in Windows Explorer. If disk space is adequate, you can increase the size of the paging file. The recommended size for the paging file is equivalent to 1.5 times the amount of RAM available on your system.

Counters That Monitor the Paging File Size

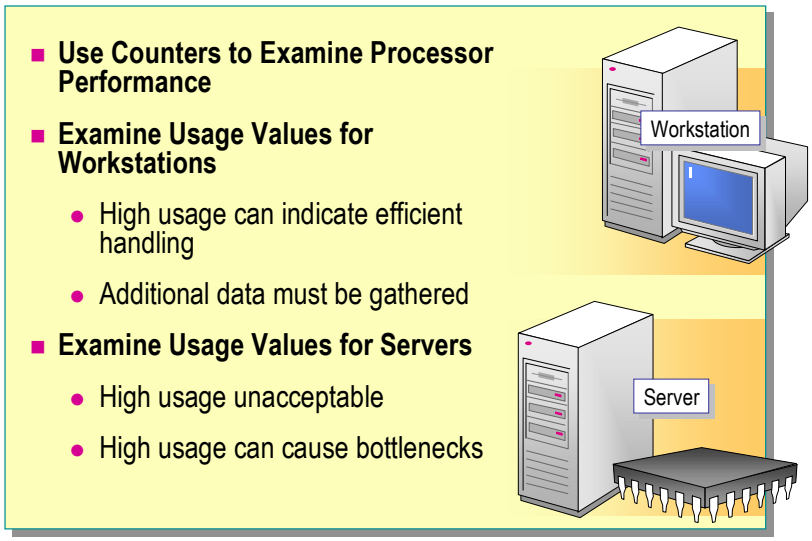
You can also use the paging file counters described in the following table to monitor the size of Pagefile.sys.

Monitor this object\counter	Then increase file size if
Paging File\ % Usage	The value is close to the maximum paging file setting.
Paging File\ % Usage Peak (bytes)	The value is close to 100 percent.

Examining Processor Performance

Topic Objective
To identify the topics related to examining processor performance.

Lead-in
When you examine processor performance, consider the role of the computer and the type of work being done.



**********ILLEGAL FOR NON-TRAINER USE**********

When you examine processor performance, consider the role of the computer and the type of work being done. Depending on what the computer is doing, high processor values could mean that the system is efficiently handling a heavy workload, or it could mean that it is struggling to keep up. However, if more than a few processes are contending for the processor's time, installing a faster processor may improve throughput.

Delivery Tip
If time permits, show % Processor Time and Processor Queue Length in System Monitor.

Using Counters to Examine Processor Performance

The counters that are useful for examining processor performance are described in the following table.

Object	Counter	Description
Processor	% Processor Time	Shows the percentage of elapsed time that a processor is busy executing a nonidle thread. A percentage of over 80 percent may indicate a bottleneck.
System	Processor Queue Length	Shows the count of threads currently in the processor queue. A queue of two or more items on a single-processor system may indicate a bottleneck.

Examining Usage Values for Workstations

If you are monitoring a workstation that is running Windows 2000, high usage values can mean that the system is efficiently handling a heavy workload. For example, if the computer is starting a new process, it may use 100 percent of the processor's time. Although this type of usage can slow the performance of other applications on that computer, you need to gather more data to determine whether the processor load is keeping other work from being done. If so, you can change the workload by moving the application to a different computer or changing the current tasks that the computer performs.

Examining Usage Values for Servers

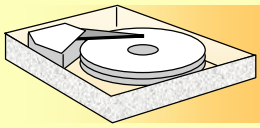
Processor values around 100 percent on a server that is processing many client requests indicate that processes are queuing up, waiting for processor time, and causing a bottleneck. A bottleneck occurs when one subsystem is so overloaded with work that the other subsystems are not fully utilized or are idle waiting for the overloaded subsystem to complete a task. Such a sustained level of processor usage is unacceptable for a server.

Examining Disk Performance

Topic Objective
To identify the topics related to examining disk performance.

Lead-in
You monitor disk activity to detect bottlenecks in the disk subsystem and help balance the workload of network servers.

- **Monitor Both Physical Disk and Logical Disk Objects to Examine Performance**
- **Use Counters to Examine Disk Activity and Determine:**
  - Percentage of unallocated disk space
  - Size of I/O operations
  - Speed data moves
  - Rates bytes transferred
  - Number of read and writes completed in a second



**********ILLEGAL FOR NON-TRAINER USE**********

Monitor disk activity to detect bottlenecks in the disk subsystem so that you can remove these bottlenecks.

Tip When monitoring disk performance, log performance data to another disk or computer so that it does not interfere with the disk you are testing.

Monitoring the PhysicalDisk and LogicalDisk Objects

Windows 2000 includes counters that monitor the activity of physical disks (including removable media drives), as well as logical partitions or volumes. The PhysicalDisk object provides counters that report physical disk activity. The LogicalDisk object provides counters that report statistics for logical disks and storage volumes. System Monitor identifies physical disks by number starting with 0 and identifies logical disks by the drive letter.

Using Counters to Examine Disk Performance

The following table provides a description of the counters for the LogicalDisk and PhysicalDisk objects that are useful for examining disk performance.

Performance object	Counter	Description
LogicalDisk	% Free Space	Reports the percentage of unallocated disk space to the total usable space on the logical volume.
LogicalDisk PhysicalDisk	Avg. Disk Bytes/Transfer	Measures the size of I/O operations. The disk is efficient if it transfers large amounts of data relatively quickly.

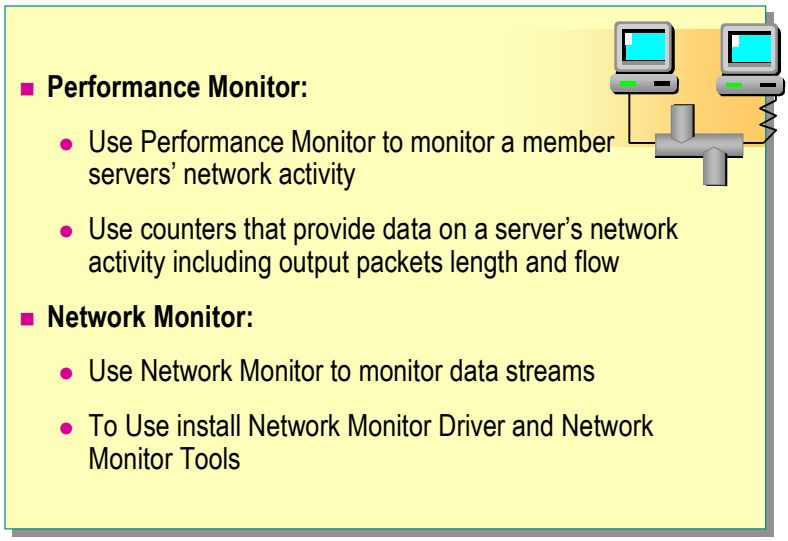
(continued)

Performance object	Counter	Description
LogicalDisk PhysicalDisk	Avg. Disk sec/Transfer	Indicates how fast data is being moved (in seconds). Measures the average time of each data transfer, regardless of the number of bytes read or written. A high value for this counter might mean that the system is retrying requests due to lengthy queuing or, less commonly, disk failures.
LogicalDisk PhysicalDisk	Disk Bytes/sec	Indicates the rate at which bytes are transferred and is the primary measure of disk throughput. The higher the number the better the performance.
LogicalDisk PhysicalDisk	Disk Transfers/sec	Indicates the number of read and writes completed per second, regardless of how much data they involve. Measures disk utilization. If value exceeds 50 (per physical disk in the case of a stripe set), then a bottleneck might be developing.

Examining Network Performance

Topic Objective
To identify the topics related to examining network performance.

Lead-in
Network activity can influence the performance not only of your network components but also of your system as a whole.



**********ILLEGAL FOR NON-TRAINER USE**********

Network activity can influence the performance not only of your network components but also of your system as a whole. After you test and optimize the client computer or server system's resources, look at the performance of the network. Windows 2000 provides two primary utilities for monitoring network performance: Performance Monitor and Network Monitor. After you capture and analyze the data, identify areas of concern, and then take corrective action.

Using Performance Monitor

Performance Monitor allows you to monitor the performance of the network objects on a server. The following table provides a description of the objects and their counters that are useful for examining the network activity of a member server.

Object	Counter	Description
Network Interface	Output Queue Length	Indicates the length of the output packet queue. The value should be low. Queues that are one or two items long constitute satisfactory performance. Longer queues mean that the adapter is waiting for the network and cannot keep pace with server requests.
Network Interface	Packets Outbound Discarded	Use this counter to determine if the network is saturated. If this counter continuously increases, it may indicate that a network is so busy that the network buffers cannot keep up with the outbound flow of packets.
Network Interface	Bytes Total/sec	Use this counter to monitor the performance of the network adapter. High values indicate a large number of successful transmissions. If the value is close to or matching the network capacity, the network may be saturated.

(*continued*)

Object	Counter	Description
Transmission Control Protocol (TCP)	Segments Received/sec Segments Retransmitted/sec Segments/sec Segments Sent/sec	Monitors activity at the transport layer.
Internet Protocol (IP)	Datagrams Forwarded/sec Datagrams Received/sec Datagrams/sec Datagrams Sent/sec	Monitors activity at the network layer.

Using Network Monitor

Use Network Monitor to monitor the network data stream, which consists of all information transferred over a network at any given time. The components of Network Monitor that you must install are:

- Network Monitor drivers, which capture the data.
- Network Monitor tools, which allow you to view the data. This information is divided into smaller parts, called frames or packets. Because frames are captured from the network, statistics about the frames are displayed in the Network Monitor Capture window.

To learn more about Network Monitor and how to install its components, see module 15, "Troubleshooting Windows 2000 Network Services," in course 2153A, *Implementing a Networking Infrastructure Using Microsoft Windows 2000*.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Monitoring Event Logs
- Using Task Manager to Monitor System Resources
- Using System Monitor to Monitor System Performance
- Using Alerts
- Optimizing Performance

**********ILLEGAL FOR NON-TRAINER USE**********

1. A user cannot connect to the e-mail server, and says that when they start their computer, a message appears indicating that at least one or more services failed to start. What event log would you look in for problem that might have occurred during startup? What type of events would you be most interested in?

   You would look in the system log on the user's computer for error messages, which are indicated by an icon with a red X.

2. A user says that Internet Explorer appears to be frozen on the screen. What tool can help the user find out if Internet Explorer is still running?

   Open Task Manager, click the Application tab, and check the status of all open applications on the user's computer. You can also end the application by using Task Manager if it is not responding to the system.

3. A user says that their system is not performing as well as it has in the past. You have used Task Manager to view processor usage and did not find any indications of a slowdown. What other tool could you use to further diagnose the user's problem?

   System Monitor. System Monitor allows you to view several counters on multiple system objects.

4. You maintain a print server that is does not have a large amount of free disk and want to be notified when the free disk space drops below a certain level. What tool could you use to alert you when the free disk space drops below a certain level?

   Use Performance Logs and Alerts to notify you when the free disk space drops below a certain level.

5. What three steps are included in the performance optimization process? Do you perform this process one time?

   The three performance optimization steps are:

   - **Analyze monitoring data**
   - **Identify areas of unacceptable performance**
   - **Take corrective action**

   Repeat this process until system performance levels are acceptable.

Microsoft® Training & Certification

Microsoft Official Curriculum

Module 9: Implementing Security in Windows 2000

Contents

Overview	1
Securing Desktops and Services by Using Security Policies	2
Lab A: Configuring Windows 2000 Security Settings	15
Auditing Access to System Resources	24
Lab B: Configuring Auditing	33
Review	42

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
60 Minutes

Labs:
60 Minutes

This module presents students with the knowledge and skills to implement security in a Microsoft® Windows® 2000 environment by using security policies and auditing.

At the end of this module, students will be able to:

- Secure desktops and services by using security policies.
- Audit access to system resources.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Course Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_09.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.

Module Strategy

Use the following strategy to present this module:

- Securing Desktops and Services by Using Security Policies

  In this topic, you will introduce the procedures for implementing security policies. Explain that the considerations behind configuring and deploying security policies will depend on the size and needs of an organization. Describe the utilities available for configuring security policy, beginning with a description of the two primary methods for implementing security policy. Explain how to create and use templates, how to analyze security configurations, and how to use the Secedit utility.

- Auditing Access to System Resources

  In this topic, you will introduce the procedures for implementing an auditing policy. Begin by explaining the purpose of auditing. Show the events Windows 2000 can audit and explain what the audit indicates. Explain how to plan an audit policy. Demonstrate how to set up an audit policy. Then, demonstrate how to set up auditing for a file.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server.*

Lab Setup

The labs in this module require each pair of student computers to be member server of the nwtraders.msft domain. To prepare the student computers to meet this requirement, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- Students create the local security template *Server* Security Template (where *Server* is the assigned server name).
- Auditing is enabled and configured on each of the student computers.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn to create and configure security policies on a computer running Windows 2000.

- **Securing Desktops and Services by Using Security Policies**
- **Auditing Access to System Resources**

**********ILLEGAL FOR NON-TRAINER USE**********

The loss of information can compromise an organization's success. Reliable security practices are essential for an organization in order to protect users' desktop computers and the network. Microsoft® Windows® 2000 provides policies and utilities to monitor security settings for a single computer or an entire enterprise. Windows 2000 also provides an auditing function that allows you to determine how resources are accessed.

At the end of this module, you will be able to:

- Secure desktops and services by using security policies.
- Audit access to system resources.

Securing Desktops and Services by Using Security Policies

Topic Objective
To introduce the topics for securing desktops and services.

Lead-in
Security policies define an organization's expectations for proper computer usage and the procedures for preventing and responding to security incidents.

- Implementing Security Policies
- Modifying Security Settings
- Using Predefined Security Templates
- Creating Custom Security Templates
- Analyzing Security
- Configuring and Analyzing Security from a Command Line

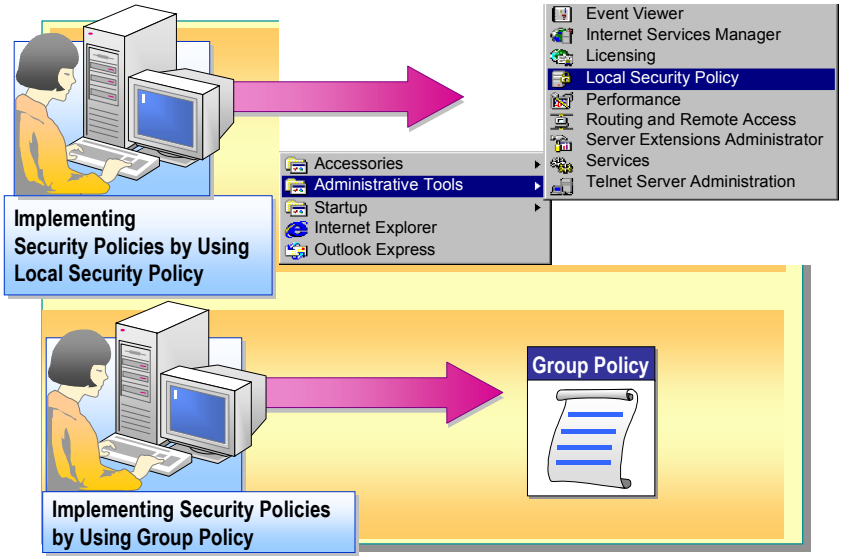
**********ILLEGAL FOR NON-TRAINER USE**********

Use security policies to enforce security in a corporate network. These security policies define an organization's expectations for proper computer usage and the procedures for preventing and responding to security incidents. Therefore, it is important that network administrators secure the desktops and services on workstations. By applying security policies, you can prevent users from damaging a computer configuration and you can protect sensitive areas of your network. The most efficient way to implement security policies is to use *security templates*. A security template is a text file that contains security settings that you can use to configure computers with consistent settings. Windows 2000 also provides security configuration tools to help you analyze and configure security settings for your computers and users.

Implementing Security Policies

Topic Objective
To identify the two methods used to implement security policy.

Lead-in
Security policy can be implemented on a per-computer basis or on the site, domain, or OU level by using Group Policy.



**********ILLEGAL FOR NON-TRAINER USE**********

Implement Security policies in two different ways: through local system policy on a single computer or through Group Policy in a domain to affect multiple computers. The method you use depends on your organization's size and security needs. Smaller organizations, or those not using the Active Directory™ directory service, are able to configure security manually on an individual basis. If your organization is large or requires a high level of security, consider using Group Policy to deploy security policy.

Explain that security policy settings will be covered next in the module.

Note Group Policy settings define components of the user's desktop environment that are managed by a system administrator. Group Policy settings are contained in a Group Policy object (GPO) and are associated with an object in Active Directory. For more information about Group Policy and Active Directory, see course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Implementing Security on a Local Computer

Implement security on a local computer that is not part of a domain by configuring a local security policy. You can configure a local security policy on the **Administrative Tools** menu.

To configure local security policy settings on computers running Windows 2000, perform the following steps:

1. Open Local Security Policy from the **Administrative Tools** menu.
2. Expand an item in the console tree to reveal a sub-area of security settings; for example, click **Account Policy**, and then click **Password Policy** to display policy settings available for passwords.
3. Click a sub-area item to display the policies in the details pane.
4. Double-click a policy listing in the detail pane to configure its settings. Each policy has unique settings available for configuration. Enter the necessary configuration settings.
5. Click **OK** to save the new settings.

Implementing Security on Multiple Computers

Key Point
Security policy settings applied locally will be overwritten by settings at the site, domain, or OU level.

Administrators of Active Directory–enabled networks can save considerable administrative time by using Group Policy to deploy security policy. Edit the security settings in a GPO for any site, domain, or organizational unit (OU). When editing a GPO, expand **Computer Configuration** or **User Configuration**, and then expand **Windows Settings** to find security policy settings.

Important Group Policy settings are applied in the following order: local settings are applied first, followed by site, domain, and then OU settings.

Modifying Security Settings

Topic Objective
To identify the security settings that you can configure.

Lead-in
You can modify security settings to establish and enforce security on your network.

Account policies	Configure password and account policies
Local policies	Configure auditing, user rights, and security options
Public key policies	Configure encrypted data recovery agents, domain roots, trusted certificate authorities, etc.
IPSec policies	Configure IP security on a network
Event log	Configures settings for application logs, system logs, and security logs
Restricted groups	Configures group memberships for security sensitive groups
System services	Configure security and startup settings for services running on a computer
Registry	Configures security on registry keys
File system	Configures security on specific file paths

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Only account policies, local policies, public key policies, and IP security policies are available when using Local Security Policy.

Also, you can assign password settings, account lockout settings, and Kerberos V5 settings only at the domain level.

The following list describes the security settings you can configure for computers by using either Local Security Policy or the Security Settings extension in Group Policy:

- *Account policies*. Account policy settings allow you to configure password policies, account lockout policies, and Kerberos version 5 protocol policies for the domain. Kerberos V5 is the primary security protocol for authentication within a domain.
- *Local policies*. Local policy settings, by definition, are local to computers. Local policies include auditing policies, the granting of user rights and permissions, and various security options that can be configured locally.

Important Do not confuse local policy settings with setting policies locally. As with all of these security areas, you can configure these settings by using Local Security Policy and by using Group Policy.

- *Public key policies*. Public key policy settings allow you to configure encrypted data recovery agents and trusted certificate authorities. Certificates are software services that provide authentication support, including secure e-mail, Web-based authentication, and smart card authentication. Public key policies are the only settings available under **User Configuration**.
- *IP security policies*. Internet Protocol (IP) security policy settings allow you to configure Internet Protocol Security (IPSec). IPSec is an industry standard for encrypting Transmission Control Protocol/Internet Protocol (TCP/IP) traffic and securing communications within an intranet and Virtual Private Networks (VPNs) across the Internet.

The following security policies can only be configured by using the Security Settings extension in Group Policy:

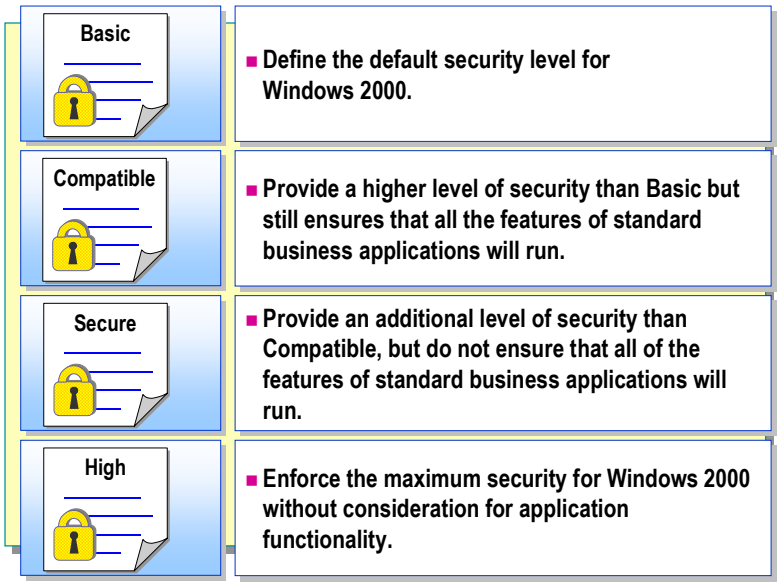
- *Event log*. Event log settings allow you to configure the size, access, and retention parameters for application logs, system logs, and security logs.
- *Restricted groups*. Restricted group settings allow you to manage the membership of built-in groups that have certain predefined capabilities, such as Administrators and Power Users, in addition to domain groups, such as Domain Admins. You can add other groups to the Restricted Group, along with their membership information. This allows you to track and manage these groups as part of security policy.

  In addition to group members, restricted group settings track and control the reverse membership of each restricted group in the Members Of column. This column displays other groups to which the restricted group must belong.
- *System services*. System service settings allow you to configure security and startup settings for services running on a computer. System service settings include critical functionality, such as network services, file and print services, telephony and fax services, and Internet or intranet services. The general settings include the service startup mode (automatic, manual, or disabled) and security on the service.
- *Registry*. Registry settings allow you to configure security on registry keys. The registry is a central hierarchical database in Windows 2000 that stores information necessary to configure the system for users, applications, and hardware devices.
- *File system*. File system settings allow you to configure security on specific file paths.

Using Predefined Security Templates

Topic Objective
To illustrate the interface for organizing and editing security templates.

Lead-in
You can use the predefined security templates in Windows 2000 to apply preconfigured security settings to a computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
The predefined security templates provided with Windows 2000 incrementally modify the default security settings. The predefined templates do *not* install the default security settings.

Create a custom security template to apply to the specific settings you want, or you can use the predefined security templates in Windows 2000 to apply preconfigured security settings to a computer. The predefined security templates provided with Windows 2000 incrementally modify the default security settings. The predefined templates do *not* install the default security settings.

Important Windows 2000 default security settings are applied only to installations of Windows 2000 on an NTFS file system partition. When computers are upgraded from Microsoft Windows NT® version 4.0, security is not modified. When Windows 2000 is installed on a FAT (file allocation table) file system, you cannot apply security to the computer.

Using Predefined Security Templates

Predefined templates can often provide a starting point from which you can customize an ideal security configuration. You should test any predefined template before using it in order to determine whether the settings adversely effect your network applications and connectivity. The predefined security templates were designed to cover common requirements for security and include templates that offer four security levels: basic, compatible, secure, and high.

Basic

Basic templates define the default security level for Windows 2000. These templates can be used as a base configuration for security analysis and should be applied to configure the upgraded computer with the new Windows 2000 default security settings.

The predefined basic security templates include the following:

- Default workstation (basicwk.inf)
- Default server (basicsv.inf)
- Default domain controller (basicdc.inf)

You can find these basic templates in the *systemroot*\security\templates folder.

Compatible

Compatible templates provide a higher level of security but still ensure that all the features of standard business applications will run. The compatibility security template is Compatible workstation or server (compatws.inf).

Secure

Secure templates provide an additional level of security, but do not include the assurance that all of the features of standard business applications will run. The predefined basic secure templates include the following:

- Secure workstation or server (securews.inf)
- Secure domain controller (securedc.inf)

High

High security templates enforce the maximum security for Windows 2000 without consideration for the functionality of applications. High security is primarily intended for testing and development of high security applications. The predefined high security templates include the following:

- Highly secure workstation or server (hisecws.inf)
- Highly secure domain controller (hisecdc.inf)

Applying a Template

You can apply a security template directly to local computer policy when a computer is not part of a domain. The system is immediately configured with the new template settings.

To apply a security template to a local computer, perform the following steps:

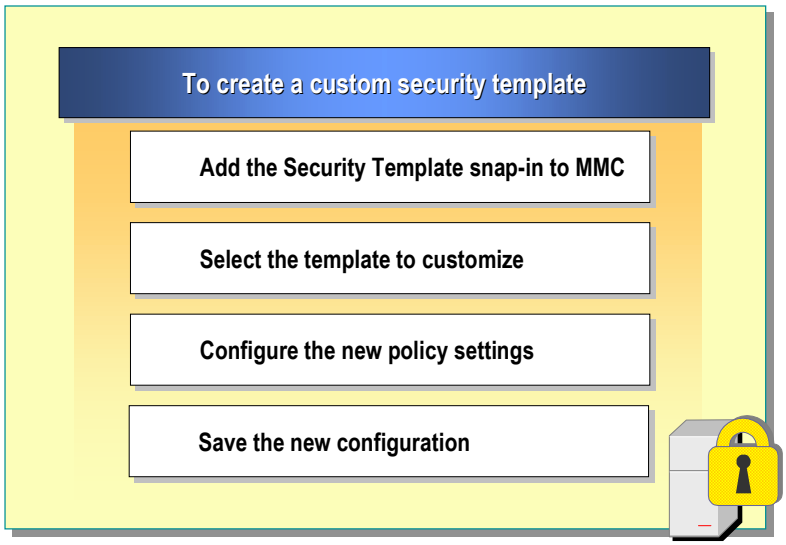
1. In Security Configuration and Analysis, right-click **Security Configuration and Analysis**.
2. Click **Open Database** to set a working database. (You only need to set a working database for a given template one time.)
3. Click **Import Template** select a security template file, and then click **Open**.
4. Right-click **Security Configuration and Analysis**, and then click **Configure System Now**.

Note In an Active Directory environment, you can import a security template to a GPO so that any computer or user accounts in the site, domain, or OU to which the Group Policy object is applied will receive the security template settings. For more information about Group Policy and Active Directory, see course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Creating Custom Security Templates

Topic Objective
To illustrate how to export a template from Local Security Policy.

Lead-in
There are two suggested methods for creating a customized policy template for your network: exporting a template from a correctly configured client computer or editing a template in Security Templates.



**********ILLEGAL FOR NON-TRAINER USE**********

If you determine that the predefined templates do not meet your security needs, create custom templates. Customize templates by using the Security Templates snap-in. After adding the Security Templates snap-in to Microsoft Management Console (MMC), either start with a new template with no settings configured, or save a copy of a predefined template and make modifications to the copy.

To modify a predefined template in Security Templates, perform the following steps:

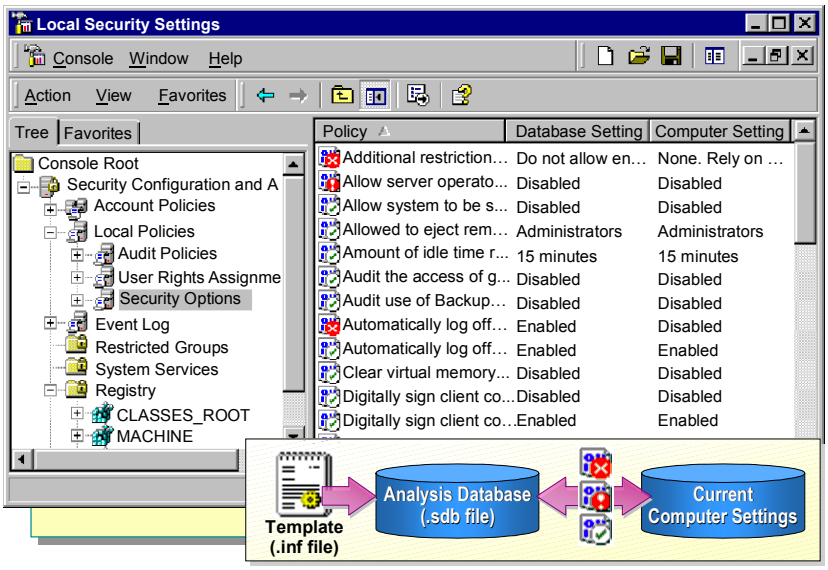
1. In Security Templates, expand the template storage location or search path. The default search path is *systemroot*\Security\Templates.
2. Right-click the template you want to copy, and then click **Save As**.
3. Enter the name of the new template, and then click **Save**. A template with the new name appears under the search path.
4. Expand the new template to select the policies you want to configure. For example, to configure the maximum password age, expand **Account Policies** and then click **Password Policy**.
5. Double-click a policy name in the details pane to configure the policy, and then click **OK** to save the configuration to the template.

   The new template is immediately available for you to import into any security configuration or GPO.

Analyzing Security

Topic Objective
To illustrate the interface used to analyze security and the concept behind its operation.

Lead-in
Security Configuration and Analysis allows you to create hypothetical scenarios to see the effect of applying a template to an existing security configuration.



**********ILLEGAL FOR NON-TRAINER USE**********

Before deploying a security template to large groups of computers, it is important to analyze the results of applying a configuration to ensure that there are no adverse effects on applications, connectivity, or security. A thorough analysis can also help you to identify security holes and deviations from standard configurations. The Security Configuration and Analysis snap-in allows you to create and review hypothetical scenarios and make adjustments to a configuration.

Security Analysis

Security Configuration and Analysis compares the security configuration of the local computer to an alternate configuration that is imported from a template (an .inf file) and stored in a separate database (an .sdb file). This allows you to ensure that computers are configured to meet your organization's security requirements.

To compare two security configurations, perform the following steps:

1. Add the Security Configuration and Analysis snap-in to MMC.
2. Right-click **Security Configuration and Analysis**, and then click **Open database**.
3. Select an existing database file or type a unique name to create a new database, and then click **Open**.
4. Existing databases already contain imported settings. If you are creating a new database, the **Import Template** dialog box appears. Select a database, and then click **Open**.

5. Right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
6. In the **Perform Analysis** dialog box, select a location for the analysis log file, and then click **OK**.

Windows 2000 then compares the two configurations and displays its progress. When processing is complete, browse the security settings tree to see the results. Discrepancies are marked with a red flag. Consistencies are marked with a green check. Settings that do not have either a red flag or a green check are not configured in the database.

Security Configuration

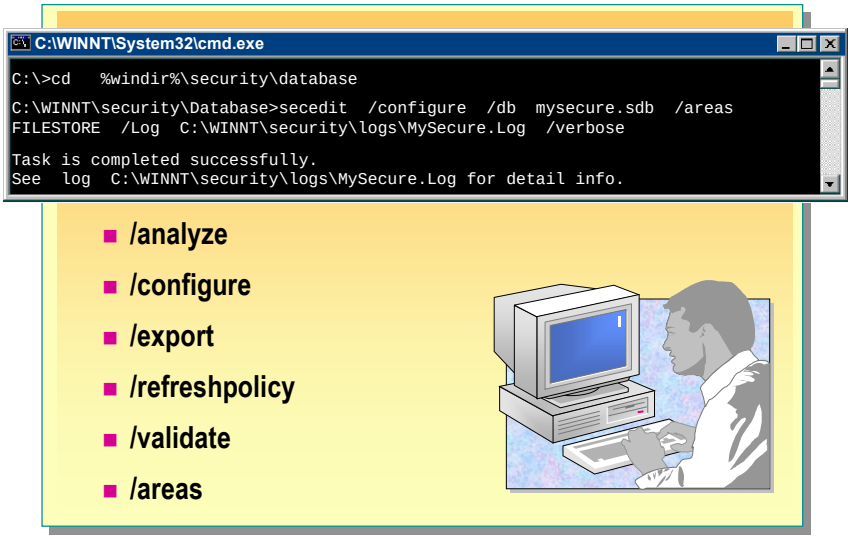
After analyzing the results, you can apply your security template to reconfigure the security of your system in the following ways:

- Eliminate discrepancies by configuring the settings in the database to match the current computer settings. To configure database settings, double-click the setting in the detail pane.
- Import another template file, merging its settings and overwriting where there is a conflict. To import another template file, right-click **Security Configuration and Analysis**, and then click **Import Template**.
- Export the current database settings to a template file. To import another template file, right-click **Security Configuration and Analysis**, and then click **Export Template**.

Configuring and Analyzing Security from a Command Line

Topic Objective
To illustrate use of the **secedit** command.

Lead-in
Command-line operation allows you to manage security policy.



**********ILLEGAL FOR NON-TRAINER USE**********

Command-line operation allows you to perform security configuration and analysis using script files as opposed to the graphical user interface (GUI). In addition, Secedit.exe, a command line utility, provides some capabilities that are not available in the graphical user interface, such as the ability to refresh a security policy.

Using the Secedit Commands

There are five high-level operations performed by Secedit.exe:

- The **/analyze**, **/configure**, and **/export** switches correspond to the same tasks available through Security Configuration and Analysis. These functions require that you specify a database to analyze with the **/db** switch. You can also specify a template to import to the database by using the **/cfg** switch. These functions also provide **/verbose** and **/quiet** modes that are not available through Security Configuration and Analysis.
- The **/refreshpolicy** switch allows you to force a Group Policy propagation event, which normally occurs whenever the computer starts, every 60 to 90 minutes thereafter, and when local security policy settings are modified by using the Security Settings extension in Group Policy. To cause a refresh in policy, regardless of whether there has been a change, add the **/enforce** switch.
- The **/validate** switch verifies the syntax of a template created by using Security Templates.

Using the /areas Switch

Also unique to Secedit.exe is the **/areas** switch, which allows you to configure or export specific areas of security settings. The areas are described in the following table.

Area	Description
securitypolicy	Local policy and domain policy for the system, including account policies, audit policies, etc.
group_mgmt	Restricted group settings for any groups specified in the security template.
user_rights	Granting user rights, including login user rights.
regkeys	Security on local registry keys.
filestore	Security on local file storage.
services	Security for all defined services.

For example, suppose you wanted to configure security on a computer using the following parameters:

- The settings to be configured are stored in the database file Mysecure.sdb.
- Only the user logon rights and local file storage security should be configured.
- You need a verbose log named Mysecure.log.
- C:\Winnt is the drive and path to the Windows folder.

To complete this configuration, you would use the following command:

secedit /configure /db mysecure.sdb /areas USER_RIGHTS FILESTORE /log c:\winnt\security\logs\Mysecure.log /verbose

---

Note To examine the full syntax for Secedit.exe, see Windows 2000 online Help.

Lab A: Configuring Windows 2000 Security Settings

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will implement security settings by using the Security Configuration Tool Set.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a security template.
- Analyze and configure a computer's security configuration by using a security template.

Prerequisites

Before working on this lab, you must have knowledge of user rights and Windows 2000 services.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- A user account in the domain named Admin*x* (where *x* is your assigned student number).
- A user account in the domain that does not have administrative privileges.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating a Security Template

Scenario

Your organization's security policy requires you to periodically review the security settings for your computers and to enforce security settings that are contained in your organization's security policy. Your organization's written security policy specifies several security restrictions that must be enforced for servers in this network. You need to configure the following security settings in the security template that you use for your server:

Only administrators are allowed to shut down the computer.

- A legal notice has to appear when any user attempts to log on, warning them that unauthorized access to this computer is not allowed.
- The user name of the last logged on user does not appear in the **Log on to Windows** dialog box to prevent unauthorized users from gathering the logon names for privileged users.
- The Telnet service must be disabled.

Goal

In this exercise, you will create an MMC console that is configured with the Security Configuration and Analysis and Security Template snap-ins. You will then create a new security template and edit this security template to configure the security settings specified in the scenario.

Tasks	Detailed Steps
1. Log on to nwtraders.msft as Student*x* (where *x* is your assigned student number) with a password of **domain** and then create an MMC console on your desktop that contains the Security Configuration and Analysis and Security Template snap-ins. Name the console Security Tools and save it on your desktop.	**a.** Log on using the following information: User name: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Click **Start**, and then click **Run**. **c.** In the **Open** dialog box, type **mmc** and then click **OK**. **d.** In the Console1 window, on the **Console** menu, click **Add/Remove Snap-in**. **e.** In the **Add/Remove Snap-in** dialog box, click **Add**. **f.** In the **Add Standalone Snap-in** dialog box, under **Available Standalone Snap-ins**, click **Security Configuration and Analysis**, click **Add**, click **Security Templates**, and then click **Add**. **g.** Click **Close** to close the **Add Standalone Snap-in** dialog box, and then click **OK** to close the **Add/Remove Snap-in** dialog box. **h.** On the **Console** menu, click **Save As**. **i.** In the **Save in** box, navigate to the desktop. **j.** In the **File name** box, type **Security Tools** and then click **Save**. **k.** Close Security Tools.

Tasks	Detailed Steps
2. Use the console that you just created to create a security template named *Server* Security Template (where *Server* is your assigned computer name).	**a.** On the desktop, right-click **Security Tools**, and then click **Run as**. **b.** In the **Run As Other User** dialog box, in the **User name** box, type **Admin***x* (where *x* is your assigned student number). **c.** In the **Password** box, type **domain** **d.** In the **Domain** box, type **nwtraders.msft** and then click **OK**. **e.** In the console tree, expand **Security Templates**, right-click **C:\WINNT\Security\Templates**, and then click **New Template**. **f.** In the **C:\WINNT\Security\Templates** dialog box, in the **Template name** box, type *Server* **Security Template** (where *Server* is your assigned computer name). **g.** In the **Description** box, type **Corporate Standard Server Settings** and then click **OK**.
3. Configure the security template to allow only the administrator to shut down the system.	**a.** In the console tree, expand **C:\WINNT\Security\Templates**, expand *Server* **Security Template** (where *Server* is your assigned computer name), and then expand **Local Policies**. **b.** Under **Local Policies**, click **User Rights Assignment**, and then in the details pane, double-click **Shut down the system**. **c.** In the **Template Security Policy Setting** dialog box, select the **Define these policy settings in the template** check box, and then click **Add**. **d.** In the **Add user or group** dialog box, click **Browse**. **e.** In the **Select Users or Groups** dialog box, in the **Look in** box, verify that your computer is selected. **f.** Under **Name**, click **Administrators**, click **Add**, and then click **OK**. **g.** Click **OK** to close the **Add user or group** dialog box, and then click **OK** to close the **Template Security Policy Setting** dialog box. *In the details pane, notice that **Administrators** appears to the right of **Shut down the system**.*
4. Configure the security template to prevent the last user name from appearing in the **Log on to Windows** dialog box.	**a.** In the console tree, click **Security Options**, and then in the details pane, double-click **Do not display last username in logon screen**. **b.** In the **Template Security Policy Setting** dialog box, select the **Define these policy settings in the template** check box, click **Enabled**, and then click **OK**. *In the details pane, notice that **Enabled** appears to the right of **Do not display last username in logon screen**.*
5. Configure the security template to display the following message to users at logon: **LEGAL NOTICE: Authorized Users Only**.	**a.** In the details pane, double-click Message text for users attempting to log on. **b.** In the **Template Security Policy Setting** dialog box, select the Define **these policy settings in the template** check box. **c.** Type **Unauthorized access is prohibited. If you are not an authorized user, do not attempt to log on** and then click **OK**.

Tasks	Detailed Steps
5. (*continued*)	**d.** In the details window, double-click **Message title for users attempting to log on**. **e.** In the **Template Security Policy Setting** dialog box, select the **Define these policy settings in the template** check box. **f.** Type **LEGAL NOTICE: Authorized Users Only** and then click **OK**. *In the details pane, notice that the message settings that you defined appear.*
6. Configure the security template to disable the Telnet service, and then save the security template.	**a.** In the console tree, click **System Services**, and then in the details pane, double-click **Telnet**. **b.** In the **Template Security Policy Setting** dialog box, select the **Define these policy settings in the template** check box. *The **Security for Telnet** dialog box appears, which can be used to modify the users and groups affected by this policy.* **c.** Click **OK** to close the dialog box. **d.** In the **Template Security Policy Setting** dialog box, under **Select service startup mode**, verify that **Disabled** is selected, and then click **OK**. *Notice that the Startup column displays **Disabled for the Telnet service**.* **e.** In the console tree, right-click *Server* **Security Template** (where *Server* is your computer name), and then click **Save**.

Exercise 2: Analyzing and Configuring a Computer's Security Configuration by Using a Security Template

Scenario

Before modifying the security settings for a computer, you want to compare the current security configuration with the settings specified in the new security template. Once you have verified that the current security settings do not comply with your organization's security requirements, you need to configure the computer by using the security template that you created. You then need to test the configured settings.

Goal

In this exercise, you will create a security database by using the security template that you created and then analyze the computer's current security configuration. You will then configure the computer by using the security template that you created and analyze your system again to verify that it complies with the security requirements. You will then verify that the new security settings enforce your organization's security policy restrictions by logging on as a domain user.

Tasks	Detailed Steps
1. Create a security configuration database.	**a.** In the console tree, click Security Configuration and Analysis. **b.** Right-click **Security Configuration and Analysis**, and then click **Open database**. **c.** In the **Open database** dialog box, in the **File name** box, type *Server* (where *Server* is your assigned computer name), and then click **Open**. **d.** In the **Import Template** dialog box, click *Server* **Security Template**, and then click **Open**. *In the details pane, Security Configuration and Analysis displays a message indicating that you may now configure or analyze your system.*
2. Analyze your computer by using the security template you created.	**a.** In the console tree, right-click Security Configuration and Analysis, and then click Analyze Computer Now. **b.** In the **Perform Analysis** dialog box, click **OK** to accept the default error log file path and start the analysis. **c.** When the analysis is complete, expand **Security Configuration and Analysis**.

Which of the following security settings were configured correctly? (Hint: Navigate to the locations below under Local Policies in the console tree to view the various settings you configured in the previous exercise. Also, incorrectly configured security settings display with a red x.)

None.

- ☐ **Local Policies\Users Rights Assignment\Shut down the system**
- ☐ **Local Policies\Security Options\Do not display last username in logon screen**
- ☐ **Local Policies\Security Options\Message text for users attempting to log on**
- ☐ **Local Policies\Security Options\Message title for users attempting to log on**
- ☐ **System Services\Telnet**

Tasks	Detailed Steps
3. Configure your system by using the template that you created in exercise 1.	**a.** In the console tree, right-click Security Configuration and Analysis, and then click Configure Computer Now. **b.** In the **Configure System** dialog box, click **OK** to accept the default log path and start the configuration. *Security Configuration Manager briefly displays the **Configuring System Security** message, which shows the progress of the configuration process, indicating which areas are being configured.*
4. Analyze your computer by using the security template you created in exercise 1.	**a.** In the console tree, right-click Security Configuration and Analysis, and then click Analyze Computer Now. **b.** In the **Perform Analysis** dialog box, click **OK** to accept the default error log file path, and then start the analysis. **c.** When the analysis is complete, expand **Security Configuration and Analysis** if necessary.

Which of the following security settings were configured correctly?

All settings are configured as specified in the security template.

- ✓ **Local Policies\Users Rights Assignment\Shutdown the system**
- ✓ **Local Policies\Security Options\Do not display last username in logon screen**
- ✓ **Local Policies\Security Options\Message text for users attempting to log on**
- ✓ **Local Policies\Security Options\Message title for users attempting to log on**
- ✓ **System Services\Telnet**

4. (*continued*)	**d.** Close Security Tools, saving the console settings, and then log off.
5. Verify that the security settings that you applied restrict users appropriately. Log on to nwtraders as Student*x* (where *x* is your student number) and the password of **domain**.	**a.** With the **Welcome to Windows** screen displayed, press CTRL+ALT+DELETE.

Does the legal notice appear with the title and message that you configured?

Yes.

Tasks	Detailed Steps
5. (*continued*)	**b.** Click **OK**.
Does the user name of the last logged on user appear in the **Log On to Windows** dialog box? **No.**	
5. (*continued*)	**c.** Log on using the following information: User name: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **d.** **Open** Computer Management from the **Administrative Tools** menu. **e.** In the console tree, expand **Services and Applications**, and then click **Services**. **f.** In the details pane, display the entry for **Telnet**.
What is the Telnet service startup type? **Disabled.**	
5. (*continued*)	**g.** Close Computer Management.

Exercise 3
Removing Group Policy

Scenario

You are about to remove a server from your network and re-install it on another network. The security policy on the other network is different than the policy for your network. You must remove your security policy before relocating the system.

Goal

In this exercise, you will remove the security setting you implemented in the previous exercise by applying the basic security template.

Tasks	Detailed Steps
1. Use the **Run As** command on the Security Tools MMC on the desktop with the user name of Admin*x* (where *x* is your assigned student number), the password of **domain** and the domain of nwtraders. Configure the system with the basicsv security template settings.	**a.** On the desktop, right-click **Security Tools**, and then click **Run as**. **b.** In the **Run As Other User** dialog box, in the **User name** box, type **Admin***x* (where *x* is your assigned student number). **c.** In the **Password** box, type **domain** **d.** In the **Domain** box, type **nwtraders.msft** and then click **OK**. **e.** In Security Tools, in the console tree, right-click **Security Configuration and Analysis**, and then click **Import Template**. **f.** In the **Import Template** dialog box, click **basicsv**, and then click **Open**. **g.** In the console tree, right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**. **h.** In the **Configure System** dialog box, click **OK** to accept the default log path and start the configuration. **i.** When the configuration is complete, close Security Tools, without saving console settings, and then log off.
2. Log on and verify that you no longer get a log on warning box and that the last user to log on appears in the User name portion of the logon window.	**a.** With the **Welcome to Windows** dialog box displayed, press CTRL+ALT+DELETE.

Tasks	Detailed Steps
	Did a warning box appear before the **Log On to Windows** dialog box appeared? Did the name of the last user to log on to the computer appear in the **User name** portion of the logon window? **No. A warning box did not appear before the Log On to Windows dialog box appeared, however, the name of the last user to log on did appear in the User name portion of the logon window.**
2. (*continued*)	**b.** Click **Cancel** to close the **Log On to Windows** dialog box.

Auditing Access to System Resources

Topic Objective
To introduce the topics related to implementing an Audit policy.

Lead-in
You can implement auditing to track specific events and to maintain security.

- Introduction to Auditing
- Selecting Events to Audit
- Planning an Audit Policy
- Setting Up an Audit Policy
- Auditing Access to Resources

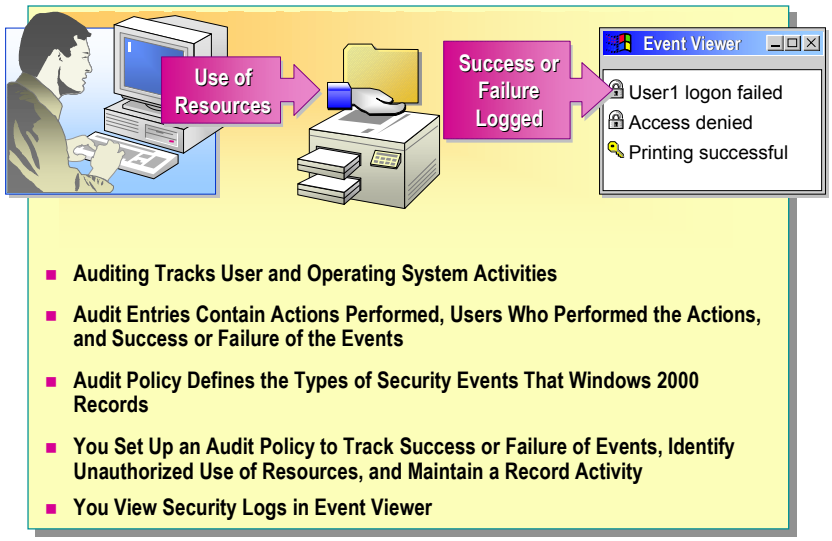
**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 allows you to track user and operating system activities on a computer. Analyze these activities to evaluate your overall security measures. Understanding how to implement auditing and monitor system events is critical for detecting an intruder's attempts to compromise data on your network.

Introduction to Auditing

Topic Objective
To explain the purpose of auditing.

Lead-in
Auditing is a feature used by administrators for monitoring network security.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Use auditing to track system events. An event shows the action that was performed, the user who performed the action, and the date and time of the action.

In Windows 2000, auditing is the process of tracking user and operating system activities (called events) on a computer. When an audited event occurs, Windows 2000 writes a record of the event to the security log.

Audit Entries

An audit entry in the security log contains the following information:

- The action that was performed.
- The user who performed the action.
- The success or failure of the event and when the event occurred.
- Additional information, such as the computer from which the action was attempted.

Audit Policy

An Audit policy defines the types of security events that Windows 2000 records in the security log on each computer. Windows 2000 writes events to the security log on the specific computer where the event occurs.

Set up an Audit policy for a computer to:

- Track the success and failure of events, such as attempts to log on, attempts by a particular user to read a specific file, changes to a user account or group membership, and changes to security settings.
- Minimize the risk of unauthorized use of resources.
- Maintain a record of user and administrator activity.

Viewing Events

Use Event Viewer to view events that Windows 2000 has recorded in the security log. You can also archive log files to track trends over time. This is useful to determine the usage of printers, access to files, or to verify attempts at unauthorized use of resources.

Selecting Events to Audit

Topic Objective
To identify the events that Windows 2000 can audit and what the event indicates.

Lead-in
To implement an Audit policy, you first select the types of events that you need Windows 2000 to audit.

Event	Example
Account Logon	Domain controller receives a request to validate a user account
Account Management	Administrator creates, changes, or deletes a user account or group
Directory Service Access	User gains access to an Active Directory object
Logon	User logs on or off a local computer
Object Access	User gains access to a file, folder, or printer
Policy Change	Change is made to the user security options, user rights, or Audit policies
Privilege Use	User exercises a right, such taking ownership of a file
Process Tracking	Application performs an action
System	User restarts or shuts down the computer

**********ILLEGAL FOR NON-TRAINER USE**********

The first step in implementing an Audit policy is to select the types of events that you want Windows 2000 to audit. The following table describes the events that Windows 2000 can audit.

Event	Example
Account Logon	An account is authenticated by a security database. When a user logs on to the local computer, the computer records the AccountLogon event. When a user logs on to a domain, the authenticating domain controller records the AccountLogon event.
Account Management	An administrator creates, changes, or deletes a user account or group. A user account is renamed, disabled, or enabled, or a password is set or changed.
Directory Service Access	A user gains access to an Active Directory object. To log this type of access, you must configure specific Active Directory objects for auditing.
Logon	A user logs on to or off a local computer, or a user makes or cancels a network connection to the computer. The event is recorded on the computer that the user accesses, independent of whether a local account or a domain account is used.
Object Access	A user gains access to a file, folder, or printer. The administrator must configure specific files, folders, or printers for auditing.
Policy Change	A change is made to the user security options (password options, account logon settings), user rights, or Audit policies.
Privilege Use	A user exercises a user right, such as changing the system time (this does not include rights that are related to logging on and logging off), or an administrator takes ownership of a file.

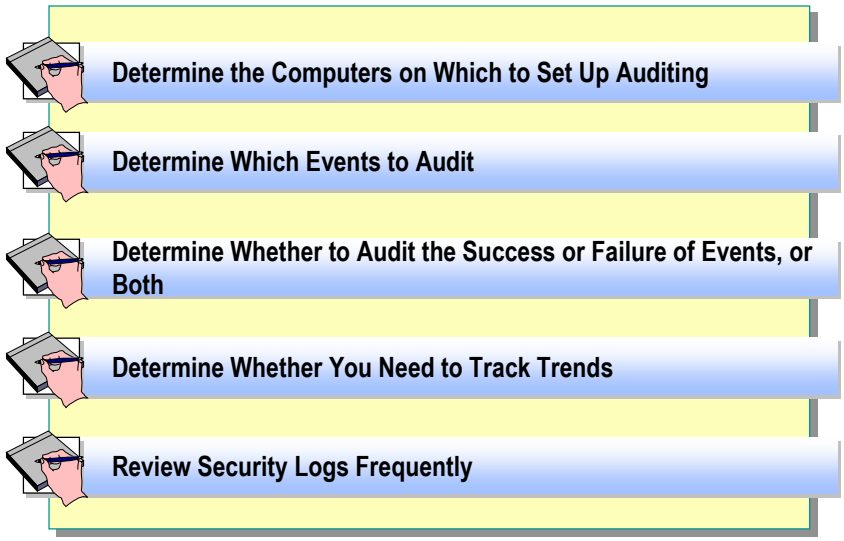
(continued)

Event	Example
Process Tracking	An application performs an action. This information is generally only useful for programmers who want to track details of application execution.
System	A user restarts or shuts down the computer, or an event has occurred that affects Windows 2000 security or the security log.

Planning an Audit Policy

Topic Objective
To explain how to plan an audit strategy and determine which events to audit.

Lead-in
Before you set up an Audit policy, you need to determine what you want to audit and whether to audit Success or Failure events.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Show students the events that Windows 2000 can audit.

Point out to students that even though Windows 2000 will track the events that are configured in security settings, it is necessary for the audit log to be reviewed regularly for that information to be of value to an organization.

Auditing too many types of events can create excess overhead. This can result in diminished system performance. It is recommended that you audit only those events that provide information that is useful to your security efforts. Use the following guidelines when planning an Audit policy:

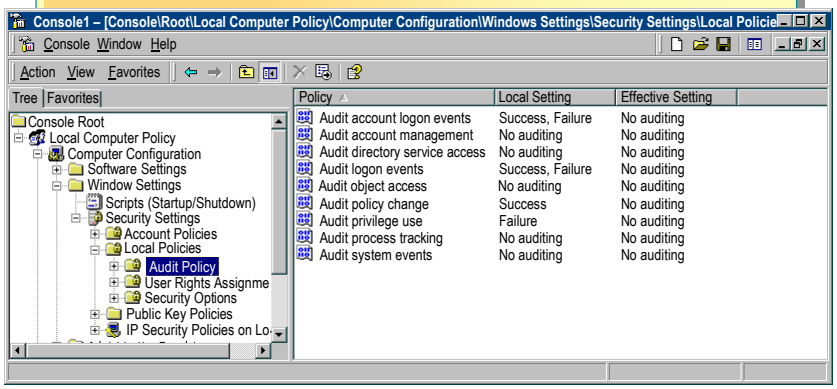
- Determine the computers on which to set up auditing. Plan what to audit for each computer because Windows 2000 records audited events on each computer separately. In this way, you can frequently audit computers used to store sensitive or critical data, but you can infrequently audit client computers that are used solely for running productivity applications.
- Determine the types of events to audit:
  - Access to files and folders
  - Users logging on and off
  - Shutting down and restarting a computer running Windows 2000 Server
  - Changes to user accounts and groups
- Determine whether to audit the success or failure of events, or both. Tracking successful events can tell you how often Windows 2000 or users gain access to specific files or printers. You can use this information for resource planning. Tracking failed events can alert you to possible security breaches.
- Determine whether you need to track trends of system usage. If so, plan to archive event logs. Some organizations are required to maintain a record of resource and data access.
- Review security logs frequently. Set a schedule and regularly review security logs. Configuring auditing alone does not alert you to security breaches.

Setting Up an Audit Policy

Topic Objective
To illustrate how to set up an Audit policy.

Lead-in
Before you set the events to audit, you must set up an Audit policy.

- **Assign Security Settings to a Single Computer by Configuring the Settings in Local Policies in Group Policy**
- **Assign Security Settings to Multiple Computers by Creating a Group Policy Object and Assigning It**



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to set up an Audit policy.

After you set an Audit policy on a single computer, you can implement auditing of file system objects, Active Directory objects, and printers. To assign audit policy to a single computer, configure the Audit Policy settings for the computer under Local Policies in Group Policy. You can also configure audit settings as part of a security template and use Security Configuration and Analysis to apply audit settings or import the template into Group Policy.

To set up an Audit policy, perform the following steps:

1. Create an MMC console and add the Group Policy snap-in. Select **Local Computer** as the Group Policy object.
2. In Local Computer Policy, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Audit Policy**.

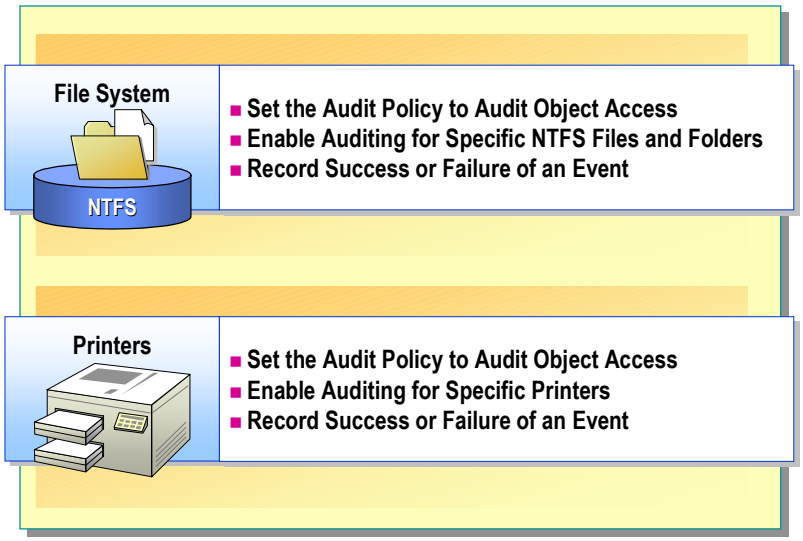
   The console displays the current Audit policy settings in the details pane.
3. Select the type of event to audit, and then click **Security** on the **Action** menu.
4. Select the **Success** or **Failure** check box, or both, and then click **OK**.

Important You need to be a member of the Administrators group to configure an Audit policy.

Auditing Access to Resources

Topic Objective
To explain the procedure for auditing access to file system, and printer objects.

Lead-in
To alert you to potential security breaches, you can set up auditing for files and folders, and printers.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to set up auditing for a file.

When auditing for security purposes, you typically audit access to file system objects and printers.

Auditing Access to File System Objects

To audit user access to the file system, perform the following tasks:

Key Point
You can only audit access to files and folders that are located on NTFS volumes.

- Set the Audit policy to audit object access, which includes files and folders.
- Enable auditing for specific files and folders and specify the types of access to audit. You can only audit access to files and folders that are located on NTFS volumes. The file allocation table (FAT) file system does not support auditing.

When you specify file system audit settings, use the following guidelines:

- Record Failure events for Read operations to determine when users are attempting to gain access to files for which they have no permissions.
- Record Success and Failure events for Delete operations when auditing confidential and archival files.
- Record Success and Failure events for Change Permissions and Take Ownership operations for confidential and personal user files. These operations may indicate that someone is attempting to modify security in order to gain access to data for which they do not currently have permissions. If an Administrator takes ownership of a user's file to assign him or herself access, this setting ensures that this event is recorded.
- Record Success and Failure events for all operations performed when auditing members of the Guests group. This should be done especially on folders and files to which Guests should not be granted access.
- Audit file and folder access on all computers containing shared data that should be secured.

Auditing Access to Printers

You can audit access to printers in order to track user access to expensive printing resources. To audit access to printers, perform the following tasks:

- Set the Audit policy to audit object access, which includes printers.
- Enable auditing for specific printers and specify the types of access to audit.

When you specify printer audit settings, use the following guidelines:

- Record Failure events for Print operations on restricted printers, such as those dedicated to printing checks.
- Record Success and Failure events for Full Control operations to maintain a log of when administrative tasks were performed on a printer.
- Record Success events for Delete operations on public printers to ensure that incomplete print jobs, or jobs that were deleted before being started, can be tracked as administrative actions rather than hardware error.
- Record Success and Failure events for Change Permissions and Take Ownership operations on restricted printers. This ensures that a record of administrative activities is retained for consultation should a discrepancy in security arise.

Lab B: Configuring Auditing

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will plan an Audit policy, configure audit settings, set up the auditing of files and printers, and create and view Security Log entries.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Plan an Audit policy.
- Configure audit settings.
- Set up auditing of files and printers.
- View security log entries.

Prerequisites

Before working on this lab, you must have:

- Knowledge about the types of audit settings available in Windows 2000.
- Experience assigning permissions on files and printers.
- Experience configuring printers.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- A user account in the domain named Admin*x* (where *x* is your assigned student number).
- A printer that is called Color Printer.
- The folder C:\MOC\Win2152b\Labfiles\Lab09, which contains a file called Bronte.txt.

Estimated time to complete this lab: 30 minutes

Exercise 1
Planning an Audit Policy

Scenario

Your organization has just completed an internal security review and has implemented several security policies that are based on the result of this review. To ensure that future security needs are identified quickly, you have identified the tasks that your network Audit policy should perform. These tasks include:

- Recording unsuccessful attempts to gain access to the network.
- Recording unauthorized access to the files that make up the Customer database.
- Tracking color printer usage for billing purposes.
- Tracking all instances of someone trying to tamper with the server hardware.
- Keeping a record of actions that an administrator performs to track unauthorized changes.

Goal

Before assigning audit settings for resources on your server, you need to determine the Audit policy settings that you will specify, including:

- Which types of events to audit.
- Whether to audit the success or failure of an event, or both.

In the following table, record your decisions for the audit settings that will satisfy the scenario.

Action to audit	Successful	Failed
Account Logon events	❑	❑
Account management	❑	❑
Directory service access	❑	❑
Logon events	❑	❑
Object access	❑	❑
Policy change	❑	❑
Privilege use	❑	❑
Process tracking	❑	❑
System events	❑	❑

Tasks	Detailed Steps

Verify that your answers from the previous table match the answers that your instructor provides. List the correct answers below, if necessary.

Account Logon events: Failed (for network access attempts).

Account Management: Successful (for administrator actions).

Directory Service Access: Nothing.

Logon: Failed (for network access attempts).

Object Access: Successful (for printer use), and Failed (for unauthorized access).

Policy Change: Successful (for administrator actions).

Privilege Use: Successful (for administrator actions and backup procedures).

Process Tracking: Nothing.

System Events: Successful and Failed (for attempts to breach the server).

Exercise 2
Configuring Audit Settings

Scenario

After you have determined your organization's Audit policy, you need to configure your server with the appropriate Audit policy settings. To do this, you need to apply the Audit policy settings to the server.

Goal

In this exercise, you will configure your computer's Audit policy and apply the settings to your computer.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with the password of **domain** and use Computer Management to configure an Audit policy that meets the requirements of your security policy.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Local Security Policy from the **Administrative Tools** menu. **c.** In the console tree, expand **Local Policies**, and then click **Audit Policy**. **d.** In the details pane, double-click each audit attribute, and in the **Local Security Policy Setting** dialog box, select the **Success** or **Failure** check box as specified in the following list. **e.** Audit account logon events - Not Configured **f.** Audit account management - Success **g.** Audit directory service access - Not Configured **h.** Audit logon events - Failure **i.** Audit object access - Success and Failure **j.** Audit policy change - Success **k.** Audit privilege use - Success **l.** Audit process tracking - Not Configured **m.** Audit System events - Success and Failure
2. Refresh the security policy for this computer immediately.	**a.** At a command prompt, type runas /user:nwtraders.msft\admin*x* "secedit /refreshpolicy machine_policy" (where *x* is your assigned student number). **b.** Press ENTER, type **domain** and then press ENTER again. *The screen flashes and a message at the command prompt indicates that the system is attempting to start the Secedit refresh.* **c.** Close the command prompt, and then close Local Security Settings.

Exercise 3
Setting Up Auditing of Files and Printers

Scenario

You have configured your computer with your organization's Audit policy settings. Next, you need to configure the audit properties for the specific files and printer for which you want to record events.

Goal

You will configure the audit settings and modify the permissions for a file. You will then configure audit settings for the printer called Color Printer.

Tasks	Detailed Steps
1. Set up auditing for the file Bronte.txt in the C:\MOC\Win2152b\Labfiles\Lab09 folder. Audit the following types of access by all users: • Create Files / Write Data • Delete • Change Permissions • Take Ownership	**a.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab09 folder, and then display the **Properties** dialog box for Bronte.txt. **b.** In the **Bronte Properties** dialog box, on the **Security** tab, click **Advanced**. **c.** In the **Access Control Settings for Bronte** dialog box, on the **Auditing** tab, click **Add**. **d.** In the **Select User, Computer, or Group** dialog box, in the **Look in** box, verify that **nwtraders.msft** appears, under **Name**, click **Everyone**, and then click **OK**. **e.** In the **Auditing Entry for Bronte** dialog box, select the **Successful** and **Failed** check boxes for each of the following events: • Create Files / Write Data • Delete • Change Permissions • Take Ownership **f.** Click **OK** to close the **Auditing Entry for Bronte** dialog box, and then click **OK** to close the **Access Control Settings for Bronte** dialog box. *Notice that the Everyone group appears under **Auditing Entries**.*
2. Change the file permissions for Bronte.txt to allow Read access to the Everyone group.	**a.** In the **Bronte Properties** dialog box, on the **Security** tab, clear the **Allow inheritable permissions from parent to propagate to this object** check box, and when prompted to copy or remove existing permissions, click **Copy**. **b.** In the **Bronte Properties** dialog box, allow the Everyone group only the Read permission. **c.** Click **OK** to close the **Bronte Properties** dialog box, and then close Windows Explorer.

(*continued*)

Tasks	Detailed Steps
3. Set up auditing of the printer called Color Printer to record all printing.	**a.** Click **Start**, point to **Settings**, and then click **Printers**. **b.** Display the **Properties** dialog box for Color Printer. **c.** On the **Security** tab, click **Advanced**. **d.** In the **Access Control Settings for Color Printer** dialog box, on the **Auditing** tab, click **Add**. **e.** In the **Select User, Computer, or Group** dialog box, under **Name**, click **Everyone**, and then click **OK**. **f.** In the **Auditing Entry for Color Printer** dialog box, select the **Successful** check box for all types of access, and then click **OK**. *Notice that the Everyone group appears under **Auditing Entries**.* **g.** Click **OK** to close the **Access Control Settings for Color Printer** dialog box. **h.** Click **OK** to close the **Color Printer Properties** dialog box, and then close the Printers system folder.

Exercise 4
Creating and Viewing Security Log Entries

Scenario

You have configured your computer with your organization's Audit policy settings and have set up auditing for file and printer objects. You want to verify that Windows 2000 records events for the actions that you want to track by performing those actions and viewing the results.

Goal

You will clear the security log for your computer. Then, you will generate events on your computer by accessing and modifying the properties of the objects that you are auditing. You will then view the security log for your computer to determine which events were recorded.

Tasks	Detailed Steps
1. Clear the security log for your computer.	**a.** Open Event Viewer from the **Administrative Tools** menu. **b.** In the console tree, right-click **Security Log**, and then click **Clear all Events**. **c.** In the **Event Viewer** message, click **No**, and then close Event Viewer.
2. Create log file entries for the local computer by viewing and attempting to change the Bronte.txt file.	**a.** In Windows Explorer, navigate to the C:\MOC\Win2152b\Labfiles\Lab09 folder, open Bronte.txt, and then close the file without changing the contents. **b.** Open Bronte.txt again, change the contents of the file, and then attempt to save the file. **c.** Close the file without saving the changes, and then close Windows Explorer.
3. Create log file entries for the local computer by changing the Color Printer priority.	**a.** Click **Start**, point to **Settings**, and then click **Printers**. **b.** Open the **Properties** dialog box for Color Printer. **c.** On the **Advanced** tab, in the **Priority** box, type **9** and then click **OK**. **d.** Close the Printers system folder.
4. Create log file entries for the local computer by restarting your computer, and attempting to log on with an incorrect password and an invalid user account. Then, log on to nwtraders as Admin*x* (where *x* is your student number) with password of **domain** and restart your computer.	**a.** Restart the computer. **b.** Attempt to log on using the following information: User name: **Starter** Password: **domain** Log on to: **nwtraders** **c.** Attempt to log on using the following information: User name: **Administrator** Password: **Windows** Log on to: *Server* (where *Server* is your assigned computer name) **d.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **e.** Restart your computer.

(*continued*)

Tasks	Detailed Steps
5. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and view the security log for your computer, and then review the events that were generated by your actions.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Event Viewer from the **Administrative Tools** menu. **c.** In the console tree, click **Security Log**. **d.** Review the log, and then use the **Filter** and **Find** commands on the **View** menu to answer the following questions:

Were Logon/Logoff events recorded? If so, were Success or Failure events recorded?

Yes. Failure events were recorded.

Were ObjectAccess events recorded for Bronte.txt? If so, were Success or Failure events recorded?

Yes. Failure events were recorded.

Were ObjectAccess events recorded for Color Printer? If so, were Success or Failure events recorded?

Yes. Success events were recorded.

(*continued*)

Tasks	Detailed Steps
Were PrivilegeUse events recorded? If so, for what event, and were Success or Failure events recorded? **Yes, for system shutdown. Success events were recorded.**	
5. (*continued*)	**e.** Close Event Viewer, and then log off.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Securing Desktops and Services by Using Security Policies
- Auditing Access to System Resources

**********ILLEGAL FOR NON-TRAINER USE**********

1. As the company administrator, you have been asked to lock down a specific computer on the network. What tool allows you to apply security settings to a computer in a single step?

   Security Configuration and Analysis.

2. An administrator asks you if there is a way to lock down a Windows 2000 Professional computer. The administrator wants to lock the computer down using the most secure method but does not want to create a template. How can the administrator accomplish this?

   By importing the Highly secure workstation or server (hisecws.inf) predefined security template into Security Configuration and Analysis.

3. You suspect that someone on the night shift is attempting to log on to the secretary's computer to access sensitive data. Where would you implement auditing and what event would you audit?

   Set up auditing on the secretary's computer and audit all successful and failed logon attempts.

4. A user attempts to set auditing on a folder on their computer and when they look at the Access Control settings for the folder, the **Audit** tab does not appear. Why is this?

   The file format must be NTFS and the user must have administrative rights on the local computer in order for the Audit tab to appear.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 10: Configuring Printing

Contents

Overview	1
Introduction to Windows 2000 Printing	2
Adding a Printer	6
Lab A: Installing Printers on a Print Server	13
Configuring a Network Printer	19
Configuring Internet Printing	25
Lab B: Installing a Client Printer and Managing Printers	29
Review	35

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

Labs:
60 Minutes

This module provides students with the knowledge and skills to set up Microsoft® Windows® 2000 printing and then manage printers after they are set up. This includes setting up and configuring Internet printing.

At the end of this module, students will be able to:

- Identify the requirements for setting up a network printer.
- Add a shared printer on a print server and set up client computers to print.
- Configure a network printer on a print server.
- Configure Internet printing.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_10.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the white paper, *File and Print Services Technical Overview*, located under **Additional Reading** on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Introduction to Windows 2000 Printing

  First, present the Windows 2000 printing terms. Ensure that the students understand the difference between print devices and printers. Then, present the requirements for configuring a network printer. Finally, present the guidelines for setting up a network printer.

- Adding a Printer

  First, present the information on adding a network printer for a local print device. Demonstrate the process using the Add Printer wizard. Then, present the information on adding and sharing a printer for a network-interface print device. Demonstrate the process using the Add Printer wizard and the Add Standard TCP/IP Printer Port wizard. Emphasize to the students that when they add a printer, if the print device is on and connected to the network, the wizard recognizes the print device. Finally, present information on setting up client computers. Emphasize that when a user at a client computer running Windows 95 or later, or Microsoft Windows NT®, connects to a printer, the client computers automatically download the appropriate printer driver.

- Configuring a Network Printer

  First, present the information on sharing an existing printer. Show the students where they would do this. Then, demonstrate how to set up a printer pool. Mention that print devices in a printer pool do not need to be identical, but they must use the same printer driver. Next, demonstrate setting up printer priorities. For this demonstration, you need at least two printers on the instructor computer. Finally, present the information on the different printer permissions. Demonstrate granting permissions.

- Configuring Internet Printing

  First, present an introduction to Internet printing. Be sure to mention the Tip on setting up a printer Web site. Then, present the information on setting up Internet printing by using a Web browser. Mention the importance of the Uniform Resource Locator (URL). Finally, show students how to manage printers by using a Web browser.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server.*

Lab Setup

The labs in this module require that the student computers be running Microsoft Windows 2000 Advanced Server configured as member servers in the wtraders.msft domain. To prepare student computers to meet this requirement, perform the following action:

- Complete lab A, "Installing Windows 2000," in module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- On the student computer, the installation of CS*x* Printer, HD*x* Printer, and ISM*x* Printer (where *x* is the assigned student number).
- On the student computer, the installation of IS Administration Printer.
- On the student computer, the creation of a 100-megabyte (MB) primary partition mounted to a new folder at the root of drive C named Spool.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn how to install and configure printers in a Windows 2000 network environment. You will also learn how to troubleshoot common printing problems that are associated with installing and configuring network printers.

- **Introduction to Windows 2000 Printing**
- **Adding a Printer**
- **Configuring a Network Printer**
- **Configuring Internet Printing**

**********ILLEGAL FOR NON-TRAINER USE**********

As a network administrator, you should set up a network-wide printing strategy that will meet the needs of users. To set up an efficient network of printers, you need to know the hardware and software requirements of network printing, how to install and configure network printers, and how to troubleshoot installation and configuration problems. Microsoft® Windows® 2000 helps you to perform these tasks more efficiently by providing the means to accomplish them and an easy-to-use interface.

At the end of this module, you will be able to:

- Identify the requirements for setting up a network printer.
- Add a shared printer on a print server and set up client computers to print.
- Configure a network printer on a print server.
- Configure Internet printing.

◆ Introduction to Windows 2000 Printing

Topic Objective
To identify the topics related to Windows 2000 printing.

Lead-in
To ensure that you successfully set up Windows 2000 printing, you should be aware of Windows 2000 printing terms, setup requirements, and follow the suggested guidelines.

- **Windows 2000 Printing Terms**
- **Requirements for Configuring a Network Printer**
- **Guidelines for Setting Up a Network Printer**

**********ILLEGAL FOR NON-TRAINER USE**********

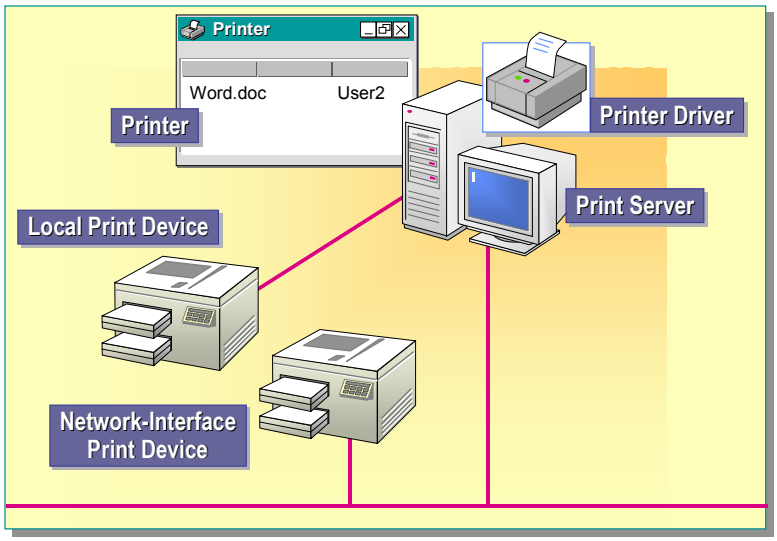
Windows 2000 makes it easy for an administrator to set up network printing and configure the print resources from a central location. You can also configure client computers running Windows 95, Windows 98, or Microsoft Windows NT® version 4.0, to print from the network print devices.

Before you set up Windows 2000 printing, you should be aware of the terms used and the recommended system requirements for setting up a print server with a network accessible print device. For best results, keep in mind certain guidelines while planning a network-printing environment.

Windows 2000 Printing Terms

Topic Objective
To identify Windows 2000 printing terms.

Lead-in
Before you set up your network accessible print device network printer, you should be familiar with certain Windows 2000 printing terms.



**********ILLEGAL FOR NON-TRAINER USE**********

Make sure that the students know what an external network adapter is. If they do not, define it.

Ensure that the students understand the difference between print devices and printers.

You should be familiar with the terms that are used to identify components and how these various components work together. The following list defines Windows 2000 printing terms:

- *Print device*. The hardware device that produces printed documents.

  Windows 2000 supports the following print devices:

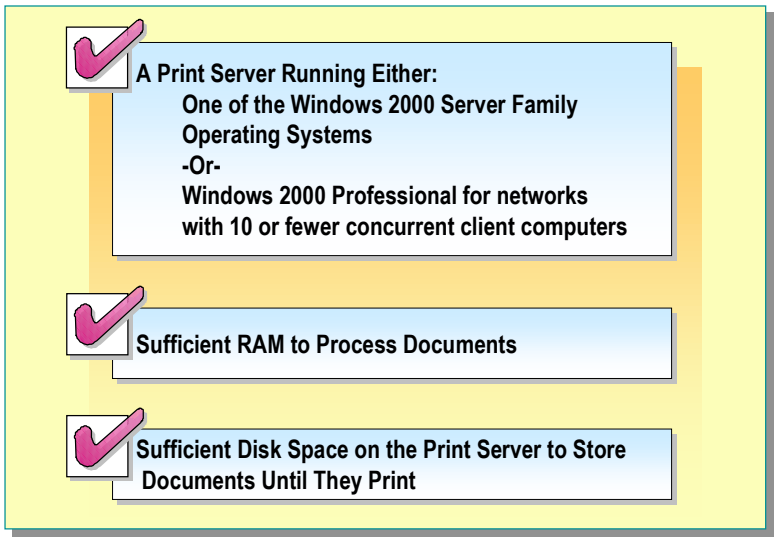
  - *Local print devices*. Print devices that are connected to a physical port on the print server.
  - *Network-interface print devices*. Print devices that are connected to a print server through the network instead of a physical port. Network-interface print devices require their own network adapters and have their own network address or they are attached to an external network adapter.
  - *Printer*. The software interface between the operating system and the print device. The printer defines when and where a document will go to reach the print device (a local port, a port for a network connection, or a file).
  - *Print server*. The computer on which the printers and client drivers are located. The print server receives and processes documents from client computers. You set up and share network printers that are associated with local- and network-interface print devices on the print servers.

- *Printer driver*. One or more files containing information that Windows 2000 requires to convert print commands into a specific printer language. This conversion makes it possible for a print device to print a document. A printer driver is specific to each print device model and the appropriate printer driver must be present on the print server.

Requirements for Configuring a Network Printer

Topic Objective
To identify the requirements for configuring network printing.

Lead-in
There are certain hardware requirements for setting up an efficient printing environment in a network.



**********ILLEGAL FOR NON-TRAINER USE**********

Make sure that students realize that a print server running Windows 2000 Professional is limited to ten concurrent connections.

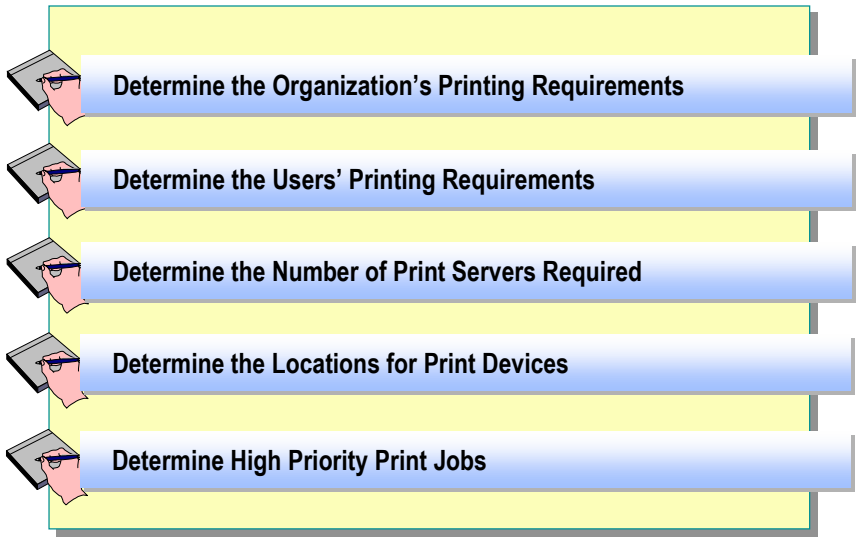
There are certain hardware requirements that are necessary for setting up an efficient printing environment. If the minimum hardware requirements are not met, network printing may be highly inefficient. Setting up printing on a Windows 2000 network requires the following:

- At least one computer to operate as the print server. If the print server is expected to manage many heavy print jobs, Microsoft recommends dedicating a server to printing. The print server can run either of the following:
  - Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server. Use one of these products when you need to support a large number of connections in addition to Macintosh, UNIX, and NetWare clients.
  - Windows 2000 Professional. Use this product when the number of concurrent connections from other computers for file and print services is limited to ten, including UNIX clients.
- Sufficient RAM to process documents. If a print server manages a large number of printers or many large documents, the server may require additional RAM beyond what Windows 2000 requires for other tasks. If a print server does not have sufficient RAM for its workload, printing performance may decline.
- Sufficient disk space on the print server to store documents. You must have enough disk space to ensure that Windows 2000 can store documents that are sent to the print server until the print server sends the documents to the print device. This is critical when documents are large or accumulate. For example, if ten users each send one large document to print at the same time, the print server must have enough disk space to hold all of the documents until the print server sends them to the print device.

Guidelines for Setting Up a Network Printer

Topic Objective
To identify strategies to consider before you set up network printing.

Lead-in
Before you set up network printing, consider these guidelines.



**********ILLEGAL FOR NON-TRAINER USE**********

Before you set up network printing, develop a printing strategy to effectively handle the printing needs of your network. This will ensure the smooth handling of print jobs. The following list provides guidelines for developing a network printing strategy:

- Determine your organization's printing requirements. This includes the number and types of print devices that are required. In addition, consider the type of workload that each print device will handle. For example, it may not be a good idea to use a print device connected locally for network printing because it may not be able to manage the workload.
- Determine user's printing requirements in each department. For example, the Billing department may have larger print jobs because they print invoices continually. A larger printing workload may require more print devices.
- Determine the number of print servers that your network requires in order to manage the number and types of printers in the network.
- Determine the location of the print devices. The printed documents should be easily accessible to the users.
- Determine which print jobs require a high priority. Executives usually need their print jobs processed quickly. Administrators can grant high priority to the people who need it.

◆ Adding a Printer

Topic Objective
To identify the tasks that an administrator must complete before users can gain access to a printer on the network.

Lead-in
After you have determined your network printing requirements, you can start adding and sharing printers.

- **Adding and Sharing a Printer for a Local Print Device**
- **Adding and Sharing a Printer for a Network-Interface Print Device**
- **Setting Up Client Computers**

**********ILLEGAL FOR NON-TRAINER USE**********

When you set up and share a print device for use on the network, you make it possible for multiple users to use the same print device. You can set up a printer for a print device that is connected directly to the print server, or you can set up a printer for a network-interface print device that is connected to the print server over the network. In larger organizations, most printers point to network-interface print devices.

When you add a printer in Windows 2000, you must also verify that client computers are properly set up so that users can print their documents to the correct print device. The appropriate client drivers need to be installed on the print server for some of the client computers to be able to download them during installation.

Adding and Sharing a Printer for a Local Print Device

Topic Objective
To introduce the options for adding and sharing a local print device.

Lead-in
The steps for adding and sharing a printer for a local and a network-interface print device are similar.

Use this option	To
Local printer	Designate where printer resides
Use the following port	Connect print device to print server
Manufacturers and **Printers**	Install correct printer driver
Printer name	Identify printer to users
Default printer	Set default printer
Shared as	Assign a share name
Location and **Comment**	Provide information about print device
Do you want to print a test page?	Verify printer installation

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate adding a local printer by using the Add Printer wizard.

When you add a shared printer, you must log on as Administrator on the print server. You can then add and share a printer by using the Add Printer wizard in the Printers system folder.

The Add Printer wizard guides you through the steps of adding a printer for a print device that is connected to the print server. The number of local print devices that you can connect to a print server through physical ports depends on your hardware configuration.

The following table describes the options that the Add Printer wizard provides for adding a printer for a local print device.

Option	Description
Local printer	This option designates that you are adding a printer to the computer at which you are sitting (the print server).
Use the following port	The port on the print server to which you attached the print device. You can also add a port. Adding a port allows you to print to non-standard hardware ports, such as a network-interface connection.
Manufacturers and **Printers**	The correct printer driver for the local print device. Enter the manufacturer and the printer model for your print device. If your print device is not in the list, you must provide a printer driver from the manufacturer or select a model that uses a similar driver.

(continued)

Option	Description
Printer name	A name that identifies the printer to the users. Use a name that is intuitive and descriptive of the print device. Some applications may not support more than 31 characters in the server and printer name combinations. This name also appears as the result of an Active Directory™ directory service search.
Default printer	The default printer for all Windows-based applications. Select this option so that users do not have to set a printer for each application. The first time that you add a printer to the print server, this option does not appear because the printer is automatically selected as the default printer.
Shared as	A share name that users (with the appropriate permission) can use to make a connection to the printer over the network. This name appears when users browse for a printer or supply a path to a printer. Ensure that the share name is compatible with the naming conventions for all client computers on the network. By default, the share name is the printer name truncated to 8.3 characters. If you use a share name that is longer than 8.3 characters, some client computers may not be able to connect.
Location and **Comment**	Information about the print device. Provide information that helps users determine if the print device fits their needs. Users can search Active Directory for the information that you enter here. Because of this search capability, you need to standardize the type of information that you enter so that users can compare printers according to the search results.
Do you want to print a test page?	Verification that you have installed the printer correctly. Click **Yes** to print a test page.

Key Points
By default a share name is truncated to 8.3 characters. If an administrator uses a longer share name, some client computers may not be able to connect.

User can search for printer on the information entered in the **Location** and **Comment** options. Therefore, this information should be standardized, so that users can make valid comparisons.

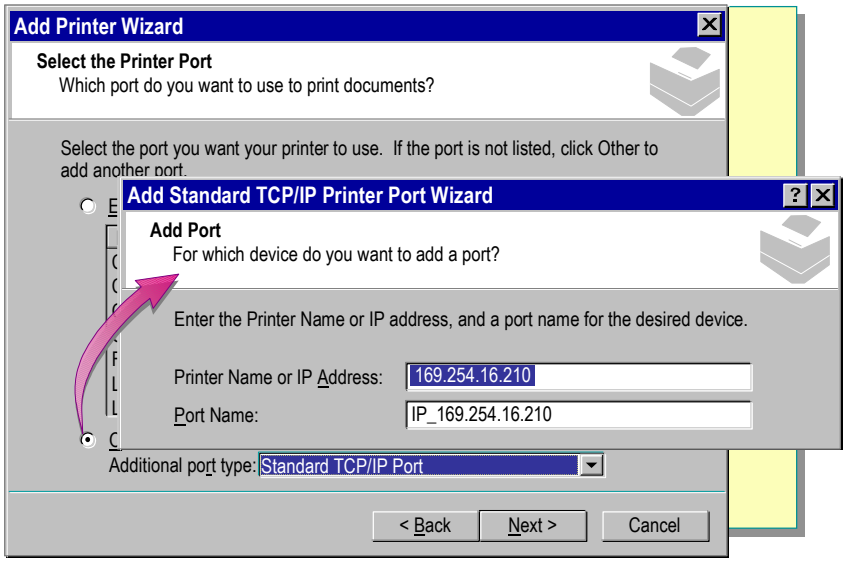
To gain access to the Add Printer wizard, click **Start**, point to **Settings**, and then click **Printers**.

Note When you add and share a network printer, Windows 2000 automatically publishes the printer in the Active Directory. Users can then search for the printer in Active Directory. In the absence of a Windows 2000 network, or if Active Directory is not installed, the shared printer would need to be searched for over the network.

Adding and Sharing a Printer for a Network-Interface Print Device

Topic Objective
To illustrate the additional information that is required to add a printer for network-interface print devices.

Lead-in
When you add network-interface print devices, you must configure a port connection.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tips
Demonstrate the steps to add and share a printer for a network-interface print device by using the Add Printer wizard and defining an IP address in the Add Standard TCP/IP Printer Port wizard.

Remind students the default Windows 2000 protocol is TCP/IP.

In larger organizations, most print devices are network-interface print devices. These print devices offer several advantages. They provide greater flexibility in where you locate your printers. In addition, network connections transfer data quicker than printer cable connections.

You can add a printer for a network-interface print device by using the Add Printer wizard. The default network protocol for Windows 2000 is Transmission Control Protocol/Internet Protocol (TCP/IP), which many network-interface print devices use. If you use TCP/IP, you must provide additional port information in the Add Standard TCP/IP Printer Port wizard.

Using the Add Printer Wizard

The following table describes the options on the Select the Printer Port page of the Add Printer wizard for adding a network-interface print device.

Option	Description
Create a new port	Starts the process of creating a new port for the print server to which the network-interface print device is connected. In this case, the new port points to the network connection of the print device.
Type	Determines the network protocol to use for the connection. The default protocol for Windows 2000 is TCP/IP.

Using the Add Standard TCP/IP Printer Port Wizard

Windows 2000 displays the Add Standard TCP/IP Printer Port wizard, if you select to add a standard TCP/IP port. The following table describes the options in the wizard that you configure when you select TCP/IP as the port type.

Option	Description
Printer Name or IP Address	Defines the network location of the print device. Provide either the TCP/IP address or the Domain Name System (DNS) name of the network-interface print device. You can obtain an IP address from your TCP/IP administrator.
Port Name	When you provide a TCP/IP address, Windows 2000 automatically supplies a suggested port name for the print device in the form IP_*IPaddress* (where *IPaddress* is the suggested port name for the print device). You can overwrite the suggested name and enter a different port name.

Key Point
To help ensure that the Add Standard TCP/IP Printer Port wizard automatically recognizes the network-interface print device, make sure the print device is on and connected to the network.

The Add Standard TCP/IP Printer Port wizard recognizes most common network-interface print devices. If it does not recognize the network-interface print device that you are configuring, you may need to provide additional information about the network-interface print device to complete the installation. To enable automatic identification, make sure that the print device is on and that it is connected to the network.

After you create the port, Windows 2000 displays it on the **Select the Printer Port** page of the Add Printer wizard. You do not have to redefine the port if you point additional printers to the same print device.

Note If your print device uses a network protocol other than TCP/IP, you must install the required network protocol before you can add a printer for this device. After you install the protocol, you can add additional ports that use the protocol. The tasks and setup information that are required to configure a printer port depend on the network protocol.

Setting Up Client Computers

Topic Objective
To identify the requirements for setting up client computers so that users can print over the network.

Lead-in
After you add and share a printer, you must ensure that users can print their documents. The tasks that you perform to do this depend on which client computers are in your network.

- **The Client Computers Running the Following Operating System Automatically Downloads the Printer Driver:**
  - Windows 95
  - Windows 98
  - Windows NT
- **Client Computers Running Other Microsoft Operating Systems Require Installation of a Printer Driver**
- **Client Computers Running Non-Microsoft Operating Systems Require Installation of:**
  - The printer driver on the client computer
  - A print service on the print server

**********ILLEGAL FOR NON-TRAINER USE**********

After you add and share a printer, you must set up client computers so that users can print their documents. Although the task of setting up client computers varies depending on which operating system is running on the client computer, all client computers require that a printer driver be installed.

Key Point
Client computers running Windows 95 or later, or Windows NT 4.0, automatically download the appropriate printer driver when they connect to the shared printer as long as there is a copy of the printer driver on the print server.

Client Computers Running Windows 95, Windows 98, or Windows NT 4.0

Users of client computers running Windows 95, Windows 98, or Windows NT 4.0, only have to make a connection to the shared printer. The client computer automatically downloads the appropriate printer driver, as long as there is a copy of the driver on the print server. You must ensure that the appropriate printer drivers are on the print server before users attempt to connect to the shared printer. In addition, if you then update the printer driver on the print server, these client computers update their local printer driver automatically the next time the client prints to this printer.

Note Printer drivers for different hardware platforms are not interchangeable. For example, if you have an Alpha-based print server and Intel-based client computers, you must add the printer drivers for both platforms on the print server.

Client Computers Running Other Microsoft Operating Systems

You must manually install a printer driver on client computers running other Microsoft operating systems (such as Microsoft Windows versions 3.1 or earlier, Microsoft MS-DOS®, and OS/2 clients) in order for them to print to a shared Windows 2000-based printer.

Mention to the students that if their networks have client computers running non-Microsoft operating, systems, in addition to manually installing printer drivers on the client computers, they need to install special services on the print server.

Client Computers Running Non-Microsoft Operating Systems

To enable users of client computers running non-Microsoft operating systems to print, you must manually install the printer driver on the client computer, and the print server must have the protocols used by the client computers and the appropriate client additional services installed. The following table lists services that are required for client computers running Macintosh, UNIX and NetWare.

Operating system	Required services
Macintosh	Services for Macintosh are included in Windows 2000 Server, but are not installed by default.
UNIX	TCP/IP Printing, which is also called the Line Printer Daemon (LPD) service, is included in Windows 2000 Server, but is not installed by default.
NetWare	File and Print Services for NetWare, an optional add-on service for Windows 2000 Server, is not included in Windows 2000 Server.

Note You can get the appropriate printer driver for a client computer from the operating system's the installation disks, or from the print device manufacturer.

Lab A: Installing Printers on a Print Server

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will add and share a printer for a local print device. To do this you do not actually need a print device connected to your computer.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Set up a print server for a print device physically attached to the print server.
- Set up a print server for a print device physically attached to the network.
- Configure print permissions.

Prerequisites

Before working on this lab, you must have:

- Knowledge of Windows 2000 printing terminology.
- Knowledge of the requirements for setting up and configuring a print device attached locally and a print device attached to the network.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- An instructor computer running Windows 2000 Advanced Server.
- Two global security groups, Customer Support and Help Desk, on the Windows 2000 Advanced Server domain controller.
- A domain user account named IS Manager*x* (where *x* is your assigned student number).

Estimated time to complete this lab: 30 minutes

Exercise 1
Configuring a Print Server for a Print Device

Scenario

As a network administrator, you need to configure a computer running Windows 2000 Advanced Server as a print server for a print device attached locally and a print device attached to the network. There is only one print device attached locally, so both the Customer Support department and the Help Desk department printers will send print jobs to this print device. The IS manager has a print device attached to the network that she also wants configured on this server.

Goal

In this exercise, you will create two printers configured for the same print device on port LPT1. Also you will create a printer for a print device using TCP/IP connected to the network. You will also configure the permissions on the printers so the proper groups and users have permission to print.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with the password of **domain**. Install a HP LaserJet 5si on port LPT1 and name the printer CS*x* (where *x* is your assigned student number), and then share the printer with the same name.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Click **Start**, point to **Settings**, and then click **Printers**. **c.** In the Printers system folder, double click **Add Printer**. **d.** On the **Welcome to the Add Printer Wizard** page, click **Next**. **e.** On the **Local or Network Printer** page, verify that **Local printer** is selected.
Note: In a production environment, you would normally let Windows automatically detect and install a Plug and Play printer. For the purposes of this lab, you will choose the manufacturer and model from a list.	
1. (*continued*)	**f.** Clear the **Automatically detect and install my Plug and Play printer** check box, and then click **Next**.
Note: The wizard prompts you to specify which port you want the printer to use. The port types available depend on the network protocols installed on the computer. For the purposes of this lab, assume that the print device that you are adding is attached directly to your computer and is using the LPT1 port.	
1. (*continued*)	**g.** On the **Select the Printer Port** page, verify that **Use the following port** is selected, click **LPT1** if necessary, and then click **Next**. **h.** On the **Add Printer Wizard** page, under **Manufacturers**, click **HP**, under **Printers**, click **HP LaserJet 5Si**, and then click **Next**. **i.** On the **Name Your Printer** page, in the **Printer name** box, type **CS***x* **Printer** (where *x* is your assigned student number), and then click **Next**.

Tasks	Detailed Steps
1. (*continued*)	**j.** On the **Printer Sharing** page, in the **Share as** box, type **CS*x* Printer** (where *x* is your assigned student number), and then click **Next**. *A warning message appears, indicating that the share name may not be accessible from some MS-DOS workstations.* **k.** Click **Yes**. **l.** On the **Location and Comment** page, in the **Location** box, type *Server* (where *Server* is your assigned computer name), in the **Comment** box type **CS*x* HP5si** (where *x* is your assigned student number), and then click **Next**.
Note: In a production environment, it is a good idea to print a test page when installing the printer on the print server for the first time. The test page includes such information as the name and location drivers, spool directory location, and any client drivers installed. For the purposes of this lab, you will not print a test page.	
1. (*continued*)	**m.** On the **Print a Test Page** page, under **Do you want to print a test page**, click **No**, and then click **Next**. **n.** On the **Completing the Add Printer Wizard** page, confirm the summary of your installation choices, and then click **Finish**. *An icon for the new printer appears in the Printers system folder.*
Why does the CS*x* printer (where *x* is your student number) display with a check mark? **Because the CS*x* printer was select as the default Windows printer during installation**.	
1. (*continued*)	**o.** Right-click **CS*x* Printer**, and then click **Pause Printing**.
Note: You are pausing the printer because the print device does not actually exist in this classroom environment, and in later exercises, you will send print jobs to the printer. If the printer is not paused, you will receive print error messages.	
2. Install another HP LaserJet 5si printer on port LPT1and name it HD*x* Printer (where *x* is your assigned student number) and share it with the same name. (This is done to create two printers for one print device.)	**a.** In the Printers system folder, double click **Add Printer**. **b.** On the **Welcome to the Add Printer Wizard** page, click **Next**.
Note: The Add Printer wizard prompts you to specify which port you want the printer to use. For this task, you are going to send print jobs to the local print device that you configured in task 1 on LPT1 port.	

Tasks	Detailed Steps
2. (*continued*)	**c.** On the **Local or Network Printer** page, verify that **Local printer** is selected, and then click **Next**. **d.** On the **Select the Printer Port** page, under **Use the following port**, click **LPT1** if necessary. *Notice that the CSx printer is configured to use this port.* **e.** Click **Next**. **f.** On the **Add Printer Wizard** page, under **Manufacturers**, verify that **HP** is selected. **g.** Under **Printers**, verify that **HP LaserJet 5Si** is selected, and then click **Next**.
Note: The **Use Existing Driver** page appears because the printer you are installing can use the drivers from a printer that has already be installed on this computer.	
2. (*continued*)	**h.** On the **Use Existing Driver** page, verify that **Keep existing driver (recommended)** is selected, and then click **Next**. **i.** On the **Name Your Printer** page, in the **Printer name** box, type **HD***x* **Printer** (where *x* is your assigned student number).
Note: The first printer installed on a computer automatically becomes the default for Windows-based programs. For printers installed subsequently, you have the option during installation to make the printer being installed the default.	
2. (*continued*)	**j.** Under **Do you want your Windows-based programs to use this printer as the default printer**, click **No**, and then click **Next**. **k.** On the **Printer Sharing** page, in the **Share as** box, type **HD***x* **Printer** (where *x* is your assigned student number), and then click **Next**. *A warning message appears, indicating the share name may not be accessible from some MS-DOS workstations.* **l.** Click **Yes**. **m.** On the **Location and Comment** page, in the **Location** box, type *Server* (where *Server* is your assigned computer name), in the **Comment** box, type **HD***x* **HP5si** (where *x* is your student number), and then click **Next**. **n.** On the **Print a Test Page** page, under **Do you want to print a test page**, verify that **No** is selected, and then click **Next**. **o.** On the **Completing the Add Printer Wizard** page, confirm the summary of your installation choices, and then click **Finish**. **p.** Right-click **HD***x* **Printer**, and then click **Pause Printing**.
3. Install a LaserJet 5si on a TCP/IP port 192.168.2.204. Name the printer ISM*x* (where *x* is your student number) and share it with the same name.	**a.** In the Printers system folder, double-click **Add Printer**. **b.** On the **Welcome to the Add Printer Wizard** page, click **Next**. **c.** On the **Local or Network Printer** page, verify that **Local printer** is selected, and then click **Next**.

Tasks	Detailed Steps
Note: This computer will manage the printer for the physical print device attached to the network the printer, and is considered local.	
3. (*continued*)	**d.** On the **Select the Printer Port** page, click **Create a new port**, in the **Type** box, click **Standard TCP/IP Port**, and then click **Next**. **e.** On the **Welcome to the Add Standard TCP/IP Printer Port Wizard** page, click **Next**. **f.** On the **Add Port** page, in the **Printer Name or IP address** box, type **192**.**168**.**2.204** and then click **Next** to accept the default port name.
Note: To connect to the print device you can type either the DNS name of the printer or the TCP/IP address of the print device.	
3. (*continued*)	**g.** On the **Additional Port Information Required** page, under **Device Type**, in the **Standard** box, click **Hewlett Packard Jet Direct**, and then click **Next**. **h.** On the **Completing the Add Standard TCP/IP Printer Port Wizard** page, confirm the summary of your installation choices, and then click **Finish**. **i.** On the **Add Printer Wizard** page, under **Manufacturers**, verify that **HP** is selected. **j.** Under **Printers**, click **HP LaserJet 6L**, and then click **Next**. **k.** On the **Name Your Printer** page, in the **Printer name** box, type **ISM***x* **Printer** (where *x* is your assigned student number), specify that this printer is not the default printer for windows-based programs, and then click **Next**. **l.** On the **Printer Sharing** page, in the **Share as** box, type **ISM***x* **Printer** (where *x* is your assigned student number), and then click **Next**. **m.** In the **Add Printer Wizard** message, click **Yes** to use this share name. **n.** On the **Location and Comment** page, in the **Location** box, type **Laser Printer on Floor** *x* (where *x* is your assigned student number), in the **Comment** box, type **ISM***x* **HP6L** and then click **Next**. **o.** On the **Print a Test Page** page, under **Do you want to print a test page**, verify that **No** is selected, and then click **Next**. **p.** On the **Completing the Add Printer Wizard** page, confirm the summary of your installation choices, and then click **Finish**. **q.** Right-click **ISM***x* **Printer**, and then click **Pause Printing**.

Tasks	Detailed Steps
4. Set up print permissions as follows (where *x* is your assigned student number): • CS*x* Printer: remove the Everyone group and add the domain user Customer Support*x*. • HDS*x* Printer: remove the Everyone group and add the domain user Help Desk*x*. • ISM*x* Printer: remove the Everyone group and add the domain user IS Manager*x*.	**a.** Display the **Properties** dialog box for the CS*x* Printer (where *x* is your assigned student number). **b.** On the **Security** tab, click **Everyone**, and then click **Remove**. **c.** Click **Add**, and then in the **Select Users**, **Computers**, **or Groups** dialog box, in the **Look in** box, verify that **nwtraders.msft** displays. **d.** Under **Name**, click **Customer Support***x* (where *x* is your assigned student number), click **Add**, and then click **OK**. **e.** Click **OK** to close the **CS***x* **Printer Properties** dialog box. **f.** Display the **Properties** dialog box for the HD*x* Printer (where *x* is your assigned student number). **g.** On the **Security** tab, click **Everyone**, and then click **Remove**. **h.** Click **Add**, and then in the **Select Users, Computers, or Groups** dialog box, in the **Look in** box, verify that **nwtraders.msft** displays. **i.** Under **Name**, click **Help Desk***x* (where *x* is your assigned student number), click **Add**, and then click **OK**. **j.** Click **OK** to close the **HD***x* **Printer Properties** dialog box. **k.** Display the **Properties** dialog box for the ISM*x* Printer (where *x* is your assigned student number). **l.** On the **Security** tab, click **Everyone**, and then click **Remove**. **m.** Click **Add**, and then in the **Select Users, Computers, or Groups** dialog box, in the **Look in** box, verify that **nwtraders.msft** displays. **n.** Under **Name**, click **IS Manager***x*, click **Add**, and then click **OK**. **o.** Click **OK** to close the **ISM***x* **Printer Properties** dialog box. **p.** In the Printers system folder, verify that the **CS***x* **Printer**, **HD***x* **Printer**, and the **ISM***x* **Printer** icons include the share symbol. **q.** Close the Printers system folder.

◆ Configuring a Network Printer

Topic Objective
To identify common changes that an administrator would make after setting up a printer.

Lead-in
After you have set up a printer, the printing needs for your organization may require that you change some printer settings.

- **Sharing an Existing Printer**
- **Setting Up a Printer Pool**
- **Setting Printer Priorities**
- **Assigning Printer Permissions**

**********ILLEGAL FOR NON-TRAINER USE**********

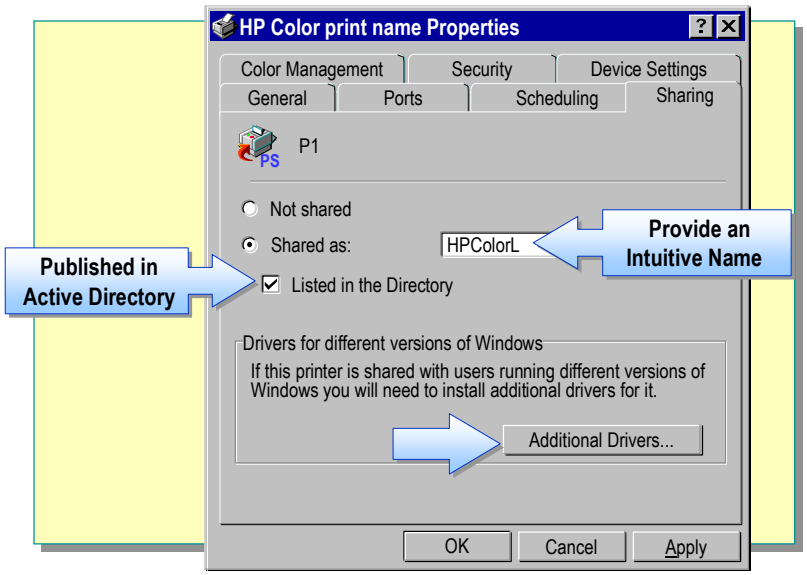
After you set up and share a printer for use on the network, user and organization printing needs may change and require you to configure printer settings so that your printing resources better fit these needs.

There are three common configuration changes. You can share an additional printer if your printing load increases. You can create a printer pool so that the printer automatically distributes print jobs to the first available print device and users do not have to search for an available printer. And you can set priorities between printers so that critical documents always print before noncritical documents.

Sharing an Existing Printer

Topic Objective
To illustrate how to share an existing printer.

Lead-in
If your network does not have enough shared printers to meet your users' printing needs, you can share an additional printer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Shows student where to share an existing printer. You can use a printer that is already shared.

If the print load increases on the shared printers and your network has an additional print device, you can share it and reduce the print load on each of the print devices.

When you share a printer on the print server:

- You must assign the printer a share name, which appears in My Network Places. Use an intuitive name to help users when they are browsing for a printer.
- You can choose to publish the printer in Active Directory if you are a member of an Active Directory network so that users can search for the printer. Publishing the printer in Active Directory enables users to search for the printer faster.
- You can add additional printer drivers for client computers running Windows 95, Windows 98, or Windows NT 4.0, on different hardware platforms.

Tip When you share an existing printer, add the additional printer drivers for client computers running Windows 95, Windows 98, or Windows NT 4.0, on different hardware platforms. Then these client computers can download the printer driver when they connect.

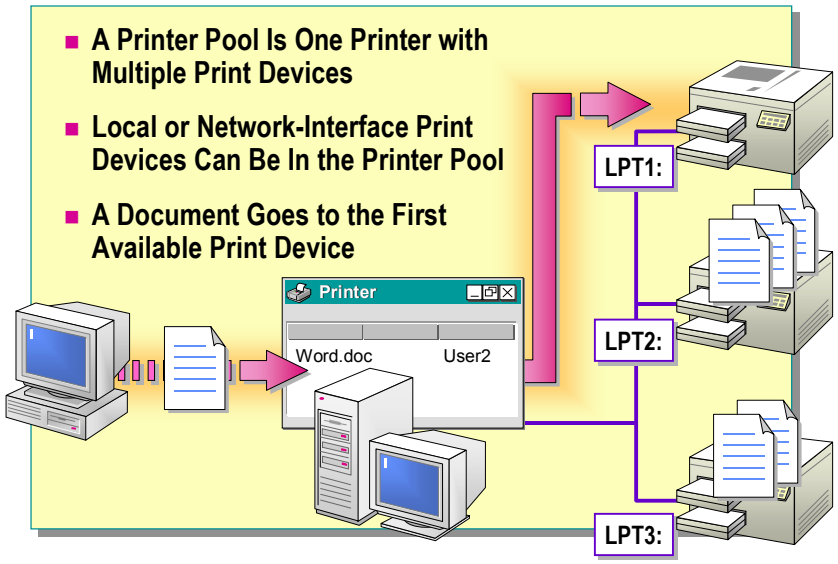
To gain access to the **Sharing** tab, right-click the icon for the printer that you want to share in the Printers folder, and then click **Sharing**.

After you have shared the printer, Windows 2000 changes the printer icon to display a hand underneath, indicating that the printer is shared.

Setting Up a Printer Pool

Topic Objective
To explain setting up printer pools.

Lead-in
You can speed up printing time for your users by using printer pools.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
The print devices in a printer pool do not need to be identical, but they must use the same printer driver.

A printer pool consists of one printer that is connected to multiple print devices through multiple ports on a print server. The print devices can be local or network-interface print devices. Print devices need not be identical, but must use the same printer driver.

When you create a printer pool, users can print documents without having to determine which print device is available because the printer checks for an available port.

Mention to the student the advantages of using printer pools and point out the Tip in their workbooks.

A printer pool has the following advantages:

- In a network with a high volume of printing, it decreases the time that documents wait on the print server.
- It simplifies administration because you can administer multiple print devices from a single printer.

Tip When you set up the print devices for a printer pool, place the print devices in the same physical area so that users can easily locate their documents.

Before you create a printer pool, make sure that you connect the print devices to the print server.

Delivery Tip
Demonstrate creating a printer pool.

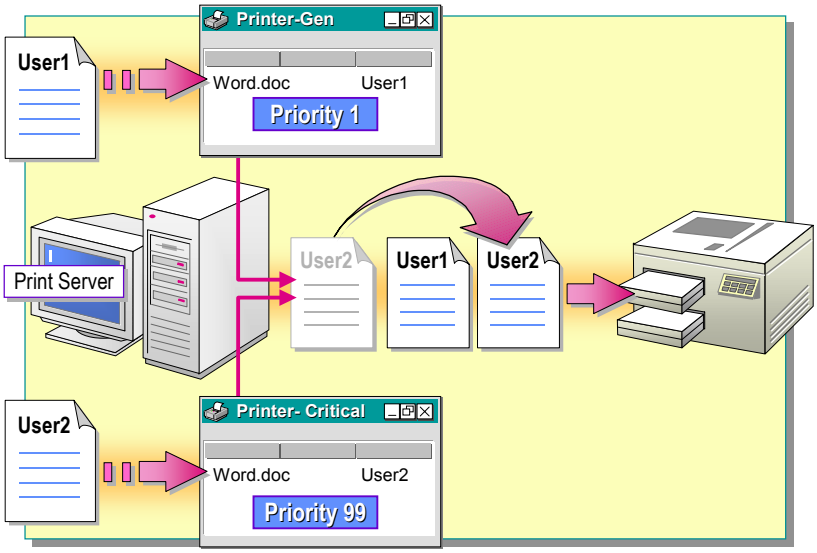
To create a printer pool, perform the following steps:

1. Open the **Properties** dialog box for the printer.
2. On the **Ports** tab, select the **Enable printer pooling** check box.
3. Select the check box for each port to which a print device is to be connected, and then click **OK**.

Setting Printer Priorities

Topic Objective
To introduce how to set priorities between printers.

Lead-in
You may need to set priorities for different groups of documents. You can do this by setting priorities for printers that are connected to the same print device.



**********ILLEGAL FOR NON-TRAINER USE**********

Set priorities between printers to prioritize documents that print to the same print device. To do this, create multiple printers pointing to the same print device. This allows users to send critical documents to a high-priority printer and noncritical documents to a lower priority printer. The documents sent to the high-priority printer will print first.

Key Point
To set priorities between printers, an administrator must point two or more printers to the same print device and then set a priority for each printer.

To set priorities between printers, perform the following tasks:

1. Point two or more printers to the same print device (the same port). The port can be either a physical port on the print server or a port that points to a network-interface print device.
2. Set a different priority for each printer that is connected to the print device, and then have different groups of users print to different printers. You can also have users send high-priority documents to the printer with higher priority and low-priority documents to the printer with lower priority.

Notice that in the preceding illustration, User1 sends documents to a printer with the lowest priority of 1, while User2 sends documents to a printer with the highest priority of 99. In this example, User2's documents will print before User1's documents.

Delivery Tip
Demonstrate setting priorities. You must have at least two existing printers in the Printers folder on the instructor computer.

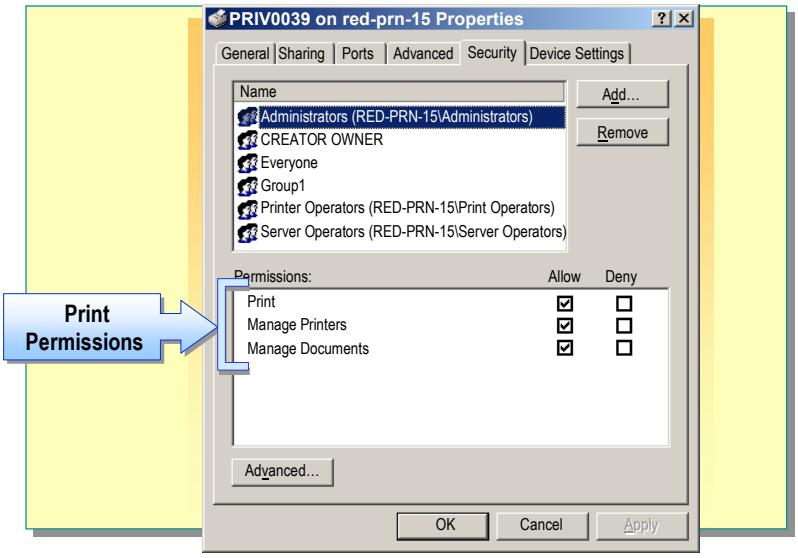
To set the priority for a printer, perform the following steps:

1. Open the **Properties** dialog box for the printer.
2. On the **Advanced** tab, change the priority in the **Priority** spin box, and then click **OK**.

Assigning Printer Permissions

Topic Objective
To illustrate how to assign printer permissions.

Lead-in
You should modify the default Print permission granted to the Everyone group, unless you want everyone to have access to the printer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the steps for changing printer permissions.

Tell the students that they can change, add, and remove printer permissions for users and groups.

Explain to students that before they assign a new permission, they need to think about how it will affect network security.

Mention that by default, the Everyone group has the Print permission. Make sure that students know what the Everyone group is.

There are three levels of printer permissions: Print, Manage Documents, and Manage Printer. The following table lists the capabilities of the different permission levels.

Capabilities of print permissions	Print permission	Manage Documents permission	Manage Printer permission
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
Pause, restart, and delete all documents		X	X
Share a printer			X
Change printer properties			X
Delete printers			X
Change printer permissions			X

By default, administrators on a server, and print operators and server operators on a domain controller have the Manage Printer permission. The Everyone group has the Print permission, and the owner of a document has the Manage Documents permission.

To add a user or group and assign print permissions, perform the following steps:

1. In the Printers folder, right-click the icon for the printer for which you want to change permissions, and then click **Properties**.
2. On the **Security** tab, in the **Properties** dialog box for the printer, click the **Everyone group**, and then click **Remove**.
3. Click the **Add** button. Select the appropriate users and groups, click **Add**, and then click **OK**.
4. On the **Security** tab, verify the permissions you want for the user or group, and then click **OK**.

◆ Configuring Internet Printing

Topic Objective
To list the topics that are related to configuring Internet printing.

Lead-in
Windows 2000 provides Internet printing, which allows you to use a Web browser to connect to and manage printers on the Internet or on an intranet. Internet printing also allows users to print directly to a URL and view print job information in HTML format.

- **Setting Up Internet Printing by Using a Web Browser**
- **Managing Printers by Using a Web Browser**

**********ILLEGAL FOR NON-TRAINER USE**********

A new feature in Windows 2000 is Internet printing: the capability to print to printers on the Internet or on an intranet by using a Web browser. By using Internet printing, you can submit print jobs to any printer on the Internet, provided you have the printer's Uniform Resource Locator (URL) and the appropriate permissions.

For example, by using Internet printing, you can send documents to print on a print device located at a company office in a different state. The benefits of this remote printing capability can also be utilized by applications such as Internet faxing. Additionally, the ability to print to a printer using a Web browser can be extended to printers located on a local area network (LAN).

In addition to sending print jobs to remote printers, Windows 2000 allows you to use a Web browser to manage printers, to print directly to a URL, and to view print job information in Hypertext Markup Language (HTML) format.

Setting Up Internet Printing by Using a Web Browser

Topic Objective
To list the guidelines for setting up Internet printing by using a Web browser.

Lead-in
You must meet certain requirements before you can use Internet printing.

- **Requirements for Printing by Using a Web Browser:**
  - The printer must be shared
  - The print server must be a computer running Windows 2000 Server and IIS, or a computer running Windows 2000 Professional and PWS
  - Internet Explorer 4.0 or later must be installed on the client computer
- **To Connect to a Printer by Using a Web Browser, You Must:**
  - Know the URL of the printer
  - Have appropriate permissions to connect to the printer
- **You Can Use the Add Printer Wizard to Connect to an Internet Printer**

**********ILLEGAL FOR NON-TRAINER USE**********

By using a Web browser, you can install printers located on the Internet or on an intranet. Internet printing uses the Internet Printing Protocol (IPP), which allows users to print directly to a URL. In addition, Windows 2000 automatically generates printer and job-related information in HTML format. Users can view the print-queue status from any Web browser, and can install printer drivers from the Web browser.

Requirements for Printing by Using a Web Browser

Before Internet printing can be operational and a print server can process print jobs that contain URLs, you must meet the following requirements:

- The printer must be shared.
- The print server must be one of the following:
  - A computer running Windows 2000 Server and Microsoft Internet Information Services (IIS).
  - A computer running Windows 2000 Professional and Microsoft Peer Web Services (PWS).
- Microsoft Internet Explorer 4.0 or later must be installed on the client computer.

Note The operating system running on the client computer determines whether the client computer will download the printer driver automatically or whether it must be installed manually.

Connecting to a Printer by Using a Web Browser

You can connect to a printer over the Internet or on an intranet by using a Web browser if you know the printer's URL and have the appropriate permissions to do so. To connect to a printer by using a Web browser:

1. Open the Web browser.
2. In the address bar, type **http://***server_name***/printers** (where *server_name* is the name of the Windows 2000 print server), and then press ENTER.
3. Click the link for the printer that you want to connect to.
4. Under **Printer Actions**, click **Connect**.

Be sure to mention the Tip to the students.

Tip It is a good idea to set up a Printers Web site for your organization. Users can browse the Web site to find their printers. They do not need to know the name of the server. For example, the Web site could display printers by their geographical location. When the users click a print device icon on the Web site, they will automatically connect to the printer on the print server.

Connecting to an Internet Printer by Using the Add Printer Wizard

You can also use the Add Printer wizard to connect to a printer on the Internet or on an intranet. To connect to a Internet printer by using the Add Printer wizard:

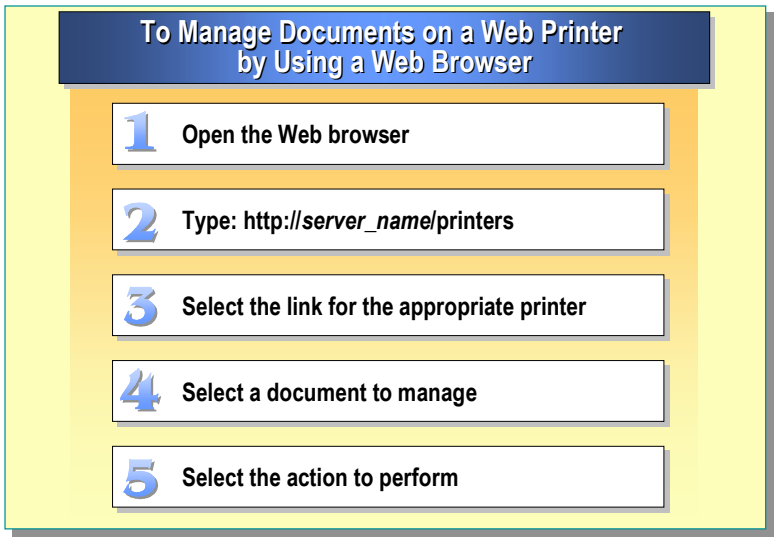
1. Click **Start**, point to **Settings**, and then click **Printers**.
2. Double-click **Add Printer**. On the **Welcome to the Add Printer Wizard** page, click **Next**.
3. Click **Network Printer**, and then click **Next**.
4. Click **Connect to a printer on the Internet or on your intranet**. In the **Address** box, type **http://***server_name***/printers/***share_name***/.printer** (where *server_name* is the name of the print server and *share_name* is the share name of the printer), and then click **Next**.
5. If prompted, type your user name and password, and then click **OK**.
6. Click **Next**, and then click **Finish**.

Note The account installing the printer must be a member of the Administrators group on the local computer.

Managing Printers by Using a Web Browser

Topic Objective
To list the steps for managing printers by using a Web browser.

Lead-in
Windows 2000 allows you to manage printers by using a Web browser. To manage a printer, you manage the documents in the print queue.



**********ILLEGAL FOR NON-TRAINER USE**********

Describe the procedure for managing documents on an Internet printer by using a Web browser.

You can manage a printer that is located on the Internet or an intranet by using any Web browser. When you manage an Internet printer, you are actually managing the documents in the print queue. Provided that you have the necessary permission, you can change the order in which documents print, pause, and resume printing, or you can delete documents from the print queue.

To manage a printer by using a Web browser:

1. Open the Web browser.
2. In the address bar, type **http://***server_name*/**printers** (where *server_name* is the name of the print server), and then press ENTER.
3. Select the link for the printer to which you want to connect.
4. Under **View**, select **Document List**, and then select a document.
5. Under **Document Actions**, click the action you wish to perform on the document.

Lab B: Installing a Client Printer and Managing Printers

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will install a printer from a Web browser and manage documents from a Web browser.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Verify the configuration for a print server that supports Internet printing.
- Install a printer from a Web browser.
- Manage documents from a Web browser.
- Set printer priorities.
- Redirect a print servers spool directory.
- Install printer drivers for Windows clients.

Prerequisites

Before working on this lab, you must have:

- Knowledge of Windows 2000 printing terminology.
- Knowledge of the requirements for installing a printer on a client computer.

Lab Setup

To complete this lab, you need the following:

- A student computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.
- An instructor computer running Windows 2000 Advanced Server as a domain controller in the nwtraders.msft domain.
- Two Hewlett-Packard printers shared on the instructor computer as Customer Support Printer and Help Desk Printer. Both printers should be paused.
- Internet Explorer must be configured to connect through a local area network.
- A local account with administrative privileges named Administrator with the password of **password**.

Estimated time to complete this lab: 30 minutes

Exercise 1
Install a Printer on a Client and Configure and Manage Printers

Scenario

The new employees of the Customer Support and Help Desk groups need to be able to install a printer from a Web browser and to manage their documents by using a Web browser. You have decided to hand out 'how to' instructions as well as give a demonstration of how to install a printer from a Web browser and how to manage documents from a browser.

The Customer Support group's documents need to print ahead of the Help Desk group's documents. The Information Services (IS) department print server needs to have the spool directory relocated. Lastly, there is a new manager in the IS department who is running Windows NT 4.0 and needs to print to the IS Manager printer.

Goal

In this exercise, you will:

- Install a printer by using Internet Explorer.
- Manage documents by using Internet Explorer.
- Change the priority on the Customer Support*x* printer.
- Redirect the print servers spool directory.
- Install drivers for Intel based Windows NT 4.0 client computers on the IS Manager printer.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with a password of **domain**. Verify that your server is properly configured to support Internet printing. Verify that IIS is installed and running and that all printers installed have been shared. Then connect to http://*server*/printers (where *server* is your assigned computer name) to view the printers.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Start Internet Services Manager from the **Administrative Tools** menu. **c.** In Internet Information Services, click *Server* (where *Server* is your assigned computer name), verify that the default Web site is running, and then close Internet Information Services. **d.** Double-click **Internet Explorer**. **e.** Complete the Internet Connection wizard, specifying to connect through a local area network; do not set up an Internet mail account. **f.** In Internet Explorer, in the **Address** box, type **http://***server*/**printers** (where *server* is your assigned computer name), and then press ENTER. **g.** On the **All Printers on** *Server* Web page (where *Server* is your computer name), verify that the three printers you installed appear and that the status of each is paused.

Tasks	Detailed Steps
2. Install the IS Administration Printer from http://London/Printers by using Internet Explorer.	**a.** In the **Address** box, type **http://London/Printers** and then press ENTER. **b.** On the **All Printers on london** page, click **IS Administration Printer**. **c.** On the **IS Administration Printer on london** page, under **Printer Actions**, click **Connect**. **d.** Click **Click here to open the printers folder on your machine**. **e.** In the **Printers** folder, right-click **IS Administration Printer on london**, and then click **Set as Default Printer**. **f.** Close the Printers system folder, and then minimize Internet Explorer.
3. Create a document named Test*x* (where *x* is your assigned student number) and print it to the IS Administration printer. Then, using Internet Explorer, cancel the document in the printer queue.	**a.** Open Windows Explorer, and then at the root of drive C, create a text document named Test*x* (where *x* is your assigned student number). **b.** Right-click **Test***x* (where *x* is your assigned student number), click **Print**, and then close Windows Explorer. **c.** Restore Internet Explorer, and then on the **View** menu, click **Refresh**. **d.** On the **IS Administration Printer on london** Web page, under **View**, click **Document List**. **e.** Click **Test***x* (where *x* is your assigned student number), and then under **Document Actions**, click **Cancel**. **f.** Verify that the Test*x* document (where *x* is your student number) does not appear in the document list, and then close Internet Explorer.
4. Set the priority on the CS*x* Printer to 99.	**a.** Click **Start**, point to **Settings**, and then click **Printers**. **b.** Display the **Properties** dialog box for the CS*x* Printer. **c.** In the **CS*x* Printer Properties** dialog box (where *x* is your assigned student number), on the **Advanced** tab, in the **Priority** box, type **99**
Note: Because both the Customer Support printer and the Help Desk printer use the same print device, the print jobs sent to the print device from the Customer Support printer will have priority over print jobs sent to the print device from the Help Desk printer.	
4. (*continued*)	**d.** Click **OK** to close the **CS*x* Printer Properties** dialog box (where *x* is your assigned student number), and then close the Printers system folder.
5. Create a 100 MB partition and mount it to a new folder titled Spool on the root of C:\. Redirect the spool directory for the print server to C:\Spool.	**a.** Open Computer Management from the **Administrative Tools** menu. **b.** Under **Storage**, click **Disk Management**. **c.** In the lower right pane, right-click the unallocated space on **Disk 0**, and then click **Create Partition**. **d.** On the **Welcome to the Create Partition wizard** page, click **Next**. **e.** On the **Select Partition Type** page, verify that **Primary partition** is selected, and then click **Next**. **f.** On the **Specify Partition Size** page, in the amount of disk space use box, type **100** and then click **Next**.
Note: In a production environment, another option for creating a designated partition might be to place the spool directory on a separate drive.	

Tasks	Detailed Steps
5. (*continued*)	**g.** On the **Assign Drive Letter or Path** page, click **Mount this volume at an empty folder that supports drive paths**, and then click **Browse**. **h.** In the **Browse for Drive Path** dialog box, verify that **C:** is selected, and then click **New Folder**. **i.** Type **Spool** as the new folder name, press ENTER, and then click **OK**. **j.** On the **Assign Drive Letter or Path** page, in the **Mount this volume at an empty folder that supports drive paths** box, verify that **C:\Spool** appears, and then click **Next**. **k.** On the **Format Partition** page, select the **Perform a Quick Format** check box, and then click **Next**. **l.** On the **Completing the Create Partition Wizard** page, click **Finish**, and then close Computer Management. **m.** Click **Start**, point to **Settings**, and then click **Printers**. **n.** In the Printers system folder, on the **File** menu, click **Server Properties**. **o.** In the **Print Server Properties** dialog box, on the **Advanced** tab, in the **Spool folder** box, type **C:\Spool** and then click **OK**. **p.** In the **Print Server Properties** message box, click **Yes** to change the spool folder.
When would you move the spool directory of a print server? **When the drive that the spool directory is on is running out of space**.	
6. Install drivers on the ISM*x* printer for Intel-based Windows NT 4.0 client computers (where *x* is your assigned student number).	**a.** Display the **Properties** dialog box for ISM*x* Printer (where *x* is your assigned student number). **b.** In the **ISM*x* Printer Properties** dialog box, on the **Sharing** tab, click **Additional Drivers**. **c.** Verify that the Windows 2000 Advanced Server compact disc is in the CD-ROM drive. **d.** In the **Additional Drivers** dialog box, select the **Intel Windows NT 4.0 or 2000** check box, and then click **OK**. **e.** Click **Close** to close the **ISM*x* Printer Properties** dialog box, close the Printers folder, and then log off.

Tasks	Detailed Steps
	What Microsoft Windows clients can automatically download printer drivers? **Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4.0, and Microsoft Windows 2000**.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to Windows 2000 Printing
- Adding a Printer
- Configuring a Network Printer
- Configuring Internet Printing

**********ILLEGAL FOR NON-TRAINER USE**********

1. In Windows 2000 printing, what is the difference between a print device and a printer?

   The print device is the physical printer, and the printer is the software interface.

2. You have been asked to create a print server for a company. They would like the print server to reside on a Windows 2000 Advanced Server. What are some factors that you should take into consideration when creating the print server?

   You should consider the number of print devices that are going to be installed on the print server, the number of users that will be printing to the printers, and the number and average size of the documents being printed. Also consider the amount of RAM and hard disk space available on the print server.

3. What port do you use when installing a network-interface printer on a TCP/IP network? What information must you supply for this port?

   Use the Add Standard TCP/IP Printer Port wizard to supply the IP address of the network-interface printer or the DNS name.

4. You have installed and shared a printer on a computer running Windows 2000 Server. What else must you do on the print server to enable client computers running Windows 95, Windows 98, or Windows NT 4.0, to connect to this printer?

   You must install the appropriate client printer drivers on the printer.

5. As the printer administrator, you need to create a print server with one print device attached to serve three departments: Sales, Accounting and Customer Support. The company has decided that the Customer Support department should be able to print their documents ahead of the other two departments. What step should you take to ensure that this happens?

   Create three printers called Sales, Accounting, and Customer Support respectively. Then, set permissions on each printer so that the corresponding department is the only department with print permissions to that printer. Finally, set the priority of the Customer Support printer higher than the priority of the other two printers.

6. A user needs to manage an Internet printer on the print server named London. What is the URL to access the printers on the print server London?

   http://london/printers

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 11: Configuring Windows 2000 for Mobile Computing

Contents

Overview	1
Configuring Hardware for Mobile Computing	2
Configuring Power Management Options for Mobile Computing	4
Lab A: Configuring Power Management Options	8
Making Files Available for Offline Use	11
Lab B: Configuring Offline Files	18
Connecting to Networks and Computers	25
Identifying Solutions to Mobile Computing Problems	29
Review	30

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

Labs:
45 Minutes

This module provides students with the knowledge and skills necessary to set up mobile users in a Microsoft® Windows® 2000 network. This includes configuring power management options for mobile users and ensuring users always have the data they need to perform their work, whether online or offline.

At the end of this module, students will be able to:

- Configure hardware for mobile computing.
- Configure power management options for mobile computing.
- Make files available offline by configuring client computers and the server.
- Connect to computers and networks remotely.
- Identify solutions to mobile computing problems.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_11.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Configuring Hardware for Mobile Computing

  Present information about hardware profiles for mobile users and why they may need to be created. Demonstrate the steps to create a new hardware profile. Mention that Windows 2000 Professional has built-in support for docking stations and ensure that students understand the term warm docking and why warm docking is beneficial to mobile users with laptops.

- Configuring Power Management Options for Mobile Computing

  First, mention that Windows 2000 Professional supports Advanced Configuration and Power Interface (ACPI) and for portable computers that use Advanced Power Management (APM). Then, present information about power schemes. Emphasize that a power scheme is a collection of settings that manages the power usage of the computer. Show students where to select a power scheme, but do not select one. Finally, present information about using the power-saving options: standby and hibernation. Mention that standby does not save the desktop state to disk and that hibernation requires an amount of free hard disk space on the boot partition equivalent to the amount of RAM.

- Making Files Available for Offline Use

  First, introduce offline files. Mention that Windows 2000 synchronizes network and local cached files when the user logs off and logs on to the network. Ensure students know what caching is. Then, present information on configuring a server, including the different caching options available. Demonstrate configuring caching. Next, present information about configuring a client computer for offline files. Demonstrate the process. Finally, present information about using Synchronization Manager to synchronize files. Demonstrate the process.

- Connecting to Networks and Computers

  First, present information about creating a dial-up connection. Mention that an administrator can either create a dial-up connection to a private network or the Internet. Demonstrate the procedures for both types of dial-up connections. Then, demonstrate how to connect to a private network through the Internet by using a virtual private network (VPN). Finally, present information on how to connect directly to another computer by using either cable or infrared connection. Mention to the students that for both types of connections, they can configure a computer to be either a host or a guest. Demonstrate the processes for both a host and guest computer.

- Identifying Solutions to Mobile Computing Problems

  Present the common problems that can arise for mobile computing. For each problem, provide a solution.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

There are no lab setup requirements that affect replication or customization. The following list describes the setup requirements for the labs in this module.

Setup Requirement for Labs A and B

The labs in this module require completion of the following:

- Install and configure the instructor computer according to the guidelines outlined in the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.
- Complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about configuring Windows 2000 for mobile computing to create a consistent working environment for mobile computer users.

- **Configuring Hardware for Mobile Computing**
- **Configuring Power Management Options for Mobile Computing**
- **Making Files Available for Offline Use**
- **Connecting to Networks and Computers**
- **Identifying Solutions to Mobile Computing Problems**

**********ILLEGAL FOR NON-TRAINER USE**********

A growing number of employees travel regularly and perform their work by using a laptop computer. Microsoft® Windows® 2000 Professional addresses the unique requirements that these mobile users have for a laptop operating system and it provides a consistent, fluid work experience for users, both while traveling and while working in the office.

Support for power management capabilities helps extend the battery life of a laptop. By making files available offline, users can work in the same files, folders, or Web sites whether they are connected or disconnected and can easily synchronize those resources. For logging on to and off of different networks or for using the same device for multiple connections, the Professional Network Connection wizard in Windows 2000 allows the user to connect to different networks in a single-step, thereby automating the user profile setup and connection process.

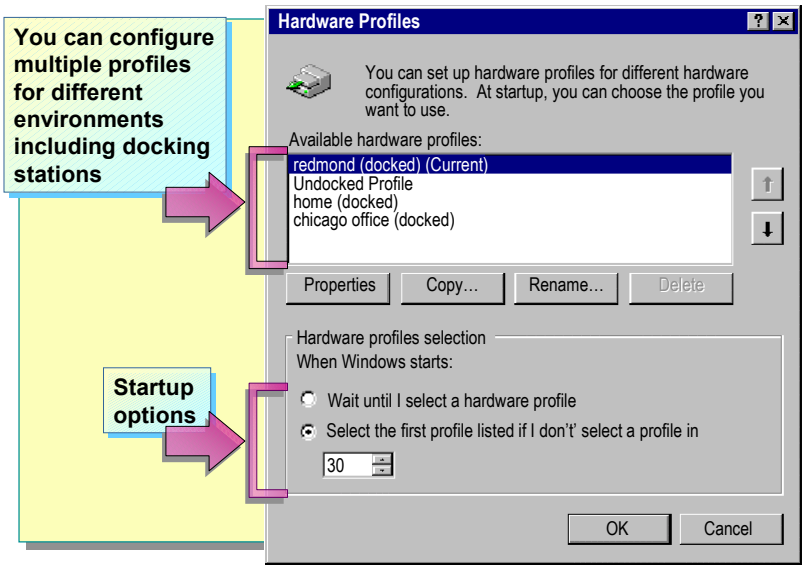
At the end of this module, you will be able to:

- Configure hardware for mobile computing.
- Configure power management options for mobile computing.
- Make files available offline by configuring client computers and the server.
- Connect to computers and networks remotely.
- Identify solutions to mobile computing problems.

Configuring Hardware for Mobile Computing

Topic Objective
To illustrate the options you can use to configure hardware for mobile computing.

Lead-in
Portable computers that are used both in a docking station and as a stand-alone computer may require advanced configuration.



**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 Professional automatically detects and installs most new and many older hardware devices. As a result, users working remotely can quickly add peripheral devices, such as, network cards or small computer system interface (SCSI) adapters in docking stations, to their computers. However, some advanced configuration may be required for portable computers that are used both in a *docking station* and as a stand-alone computer.

Note A docking station is a platform into which you can install a portable computer. Docking stations contain slots for expansion cards, bays for storage devices, and connectors for peripheral devices, such as printers and monitors. Docking stations enable users to combine the expansion capabilities of desktop computers with the mobility of portable computers.

Key Point
An administrator may need to create additional hardware profiles for laptops computers that are used stand-alone and in a docking station.

Creating a Hardware Profile for Mobile Users

Windows 2000 can automatically detect hardware on newer laptops. If Windows 2000 is unable to automatically detect the hardware for a laptop computer, you can create hardware profile to designate the devices that a portable computer loads when a user moves the computer from a docking station on the network to stand-alone use at a remote location.

Note Whether Windows 2000, running on a given laptop, detects hardware correctly depends on the version of the basic input/output system (BIOS). The system BIOS is the set of essential software routines that tests hardware at startup, starts the operating system, and supports the transfer of data among hardware devices. Consult your manufacturer or documentation for more information on hardware detection.

For example, you can create a profile named Docked for using the portable computer at a docking station with a CD-ROM drive and a network adapter. You can then create a second profile named Undocked for using the portable computer at a hotel or on an airplane with a modem and a portable printer.

Delivery Tip
Demonstrate the steps for creating a new hardware profile.

To create a new hardware profile for mobile users, perform the following steps:

1. Double-click **System** in Control Panel.
2. On the **Hardware** tab, click **Hardware Profiles**.
3. Under **Available hardware profiles**, click **Profile 1 (Current)**.

   The profile named Profile 1 (Current) provides a model for you to create new hardware profiles.
4. Click **Copy**, type a name for the new profile, and then click **OK**.
5. Select a startup option under **When Windows starts**. Select either **Wait until I select a hardware profile** or **Select the first listed if I don't select a profile in** *X* (where *X* is the amount of time to wait).
6. Restart the computer, and then select the new hardware profile at startup.
7. Double-click **System** in Control Panel. On the **Hardware** tab, click **Device Manager**. Double-click the device, and, on the **General** tab, in the drop-down list for device usage, select one of the following:
   - **Use this device (enabled)**
   - **Do not use this device in the current hardware profile (disabled)**
   - **Do not use this device in any hardware profile (disabled)**

   When the user starts the computer, the default hardware profile starts or the user can manually select a different profile. The only the device drivers that load are those that are enabled for that hardware profile are loaded.

Using Docking Stations

Explain that applications and hardware must support warm docking.

Ensure that students understand the importance of warm docking.

Windows 2000 Professional has built-in support for docking stations. Users can plug portable computers in and out of a docking station without restarting. This procedure is called *warm docking*. Warm docking is especially helpful when you are moving a portable computer from one environment to another. For example, you can move a portable computer from an office into a conference room for a presentation without restarting the computer. Users can eject their computers from docking stations by using menu commands.

To undock a portable computer, perform the following steps:

1. Click **Start**.
2. Click **Eject PC**.

   A message appears, indicating that it is safe to undock the computer. If the user has a motorized docking station, the portable computer will automatically undock.

Note Some computers have an eject button on the docking station. Pressing the eject button instead of following this procedure also undocks the laptop. For more information about the eject procedure, refer to the manufacturer's documentation.

Configuring Power Management Options for Mobile Computing

Topic Objective
To identify the topics related to configuring power management options.

Lead-in
Windows 2000 provides power management options to manage the power state of both portable and desktop computers.

- **Selecting a Power Scheme**
- **Using Power-Saving Options**

**********ILLEGAL FOR NON-TRAINER USE**********

Use **Power Options** in Control Panel to reduce the power consumption of any number of your computer devices or of your entire system. You do this by choosing a power scheme, or by adjusting the individual settings in a power scheme.

When presenting this topic, mention that Windows 2000 Professional supports both ACPI and APM. If students have questions, refer them to the white papers provided on the Student Materials compact disc.

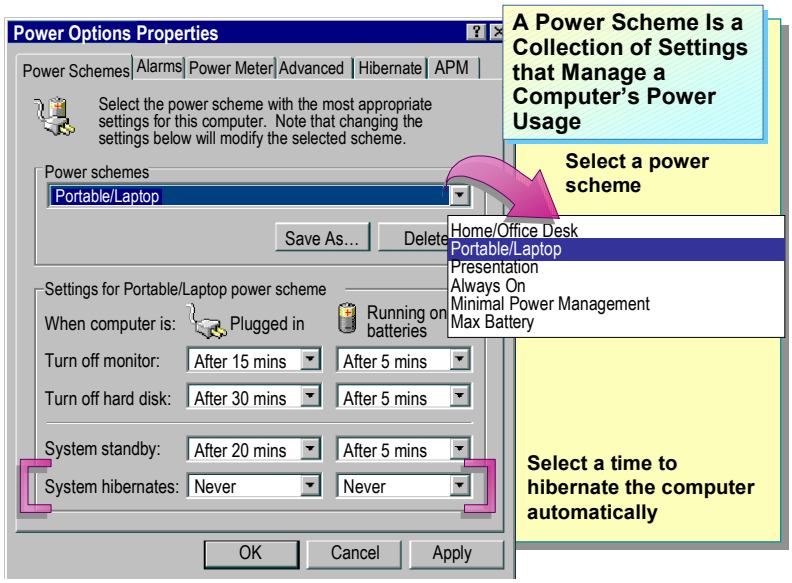
Windows 2000 Professional supports a power management technology called Advanced Configuration and Power Interface (ACPI). ACPI enables Windows 2000 to manage the power state of both portable and desktop computers in response to input from the user, applications, or device drivers. Windows 2000 Professional also includes support for portable computers that use Advanced Power Management (APM).

For more information about ACPI and APM, see the white papers, *Mobile Scenario* and *Overview of Power Management in Windows 2000*, located under **Additional Reading** on the Student Materials compact disc.

Selecting a Power Scheme

Topic Objective
To illustrate the interface for configuring power management options.

Lead-in
Windows 2000 Professional helps people make maximum use of their time out of the office by providing power management options that help conserve battery usage.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
A power scheme is a collection of settings that manages the power usage of the computer.

To reduce the power consumption of a workstation or portable computer, you can choose a *power scheme*. A power scheme is a collection of settings that manages the power usage of the computer. Power schemes provide users with the ability to choose a balance between battery life and performance that best meets their needs. Use the power schemes provided with Windows 2000 or create your own power schemes.

Delivery Tip
Show students where to select a power scheme by using **Power Options**, but do not select a new scheme.

To select a power scheme, perform the following steps:

1. Double-click **Power Options** in Control Panel.
2. Under **Power Schemes**, on the **Power Scheme** tab, select one of the power schemes described in the following table.

Explain that power scheme settings vary depending on whether the computer is a portable or a desktop. For example, the Home/Office Desk power scheme that is used for a desktop computer is similar to the Always On power scheme that is used for a portable computer.

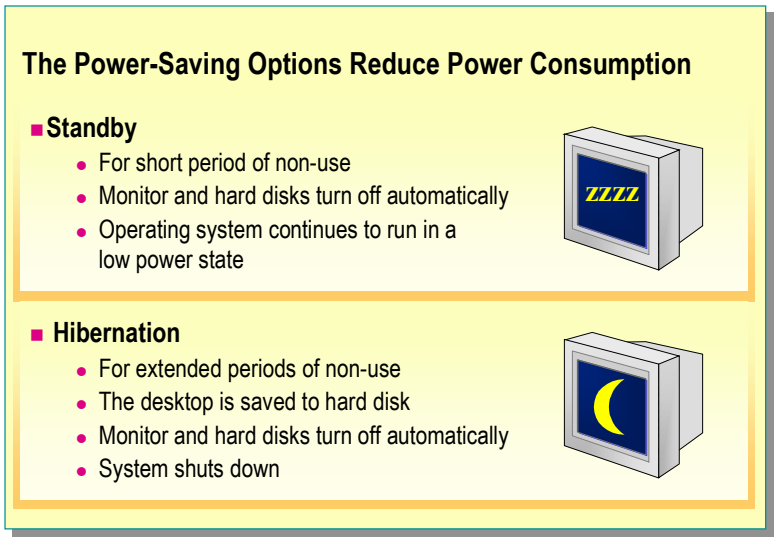
Power schemes	Description
Home/Office Desk	Maintains constant power to the hard disk and system when the computer is plugged in.
Portable/Laptop	Turns off all settings after 5 to 30 minutes of inactivity.
Presentation	Maintains constant power to the monitor when the computer is plugged in or running on batteries. Maintains constant power to the hard disk and system when the computer is plugged in.
Always On	Maintains constant power to the system when the computer is plugged in or running on batteries.
Minimal Power Management	Maintains constant power to the hard disk and system when the computer is plugged in.
Max Battery	Maintains constant power to the hard disk when the computer is plugged in.

Preset time settings appear in the **Turn off monitor** and **Turn off hard disks** lists of the **Power Schemes** tab. You can change these settings by clicking the arrow next to the list, and then clicking the time you want.

Using Power-Saving Options

Topic Objective
To identify the characteristics of the two available power-saving options.

Lead-in
You can use power options to reduce power consumption, which helps to conserve battery life on portable computers.



**********ILLEGAL FOR NON-TRAINER USE**********

You can use power options to reduce power consumption, which helps to conserve battery life on portable computers. If you plan to be away from your computer for a short time, you can put your computer on *standby*, which puts your entire operating system in a low-power state. If you plan to be away from the computer for an extended time, you can put your computer in *hibernation*.

Note To use **Power Options** in Windows 2000, you must have a computer that supports these features. Check the documentation that came with your computer to determine whether your computer supports these options.

Key Point
Standby does not save the desktop state to disk. Therefore, a power failure while a computer is in standby can cause a user to lose unsaved data.

Configuring Standby

Standby switches your entire computer to a low power state so that devices, such as the monitor and hard disks, turn off and your computer uses less power. When you log onto the computer again, your desktop is restored to the state in which you left it. If your computer supports APM, then you can configure standby.

Important Because standby does not save your desktop state to disk, a power failure while on standby can cause you to lose unsaved data.

To configure standby on a laptop, perform the following steps:

1. Double-click **Power Options** in Control Panel.
2. Under the **Power buttons**, on the **Advanced** tab, select one of the following options that determines when standby takes affect:
   - **When I close the lid of my portable computer**
   - **When I press the power button on my computer**
   - **When I press the sleep button on my computer**

Note The options that appear on the **Advanced** tab vary depending on the computer. For information about the options for your computers, such as the **Sleep** button, see the manufacturer's documentation.

3. Click **OK** or **Apply**.

Enabling Hibernation

Key Point
Hibernation requires an amount of free hard disk space on the boot partition equivalent to the amount of RAM.

Hibernation saves your desktop to the hard drive, turns off your monitor and hard disk, and then turns off your computer. When you restart your computer, your desktop is restored to the state in which you left it. However, it takes longer to bring your computer out of hibernation than out of standby.

Important Hibernation requires an amount of free hard disk space on the boot partition equivalent to the amount of RAM.

To enable hibernation, perform the following steps:

1. In the **Power Option Properties** dialog box, click the **Hibernate** tab, select the **Enable hibernate support** check box, and then click **Apply**.
2. Click the **Power Schemes** tab, and then select a time in **System hibernates**.

   The computer hibernates after it has been idle for the time period specified in **System hibernates**. To manually put a computer into hibernation, click **Start**, and then click **Shut Down**. In the **Shut Down Windows** dialog box, click **Hibernate**.

You can use your Windows password for both standby and hibernation. To password protect your computer during standby or hibernation, click the **Advanced** tab, and then click **Prompt for password when computer goes off standby**.

Note You start standby and hibernation on a desktop computer differently than on a laptop. To determine the procedures, see the manufacturer's documentation.

Lab A: Configuring Power Management Options

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create a custom power scheme and enable hibernation.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a custom power scheme.
- Enable hibernation support.

Prerequisite

Before working on this lab, you must have knowledge of the power management options in Windows 2000.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.

Estimated time to complete this lab: 15 minutes

Exercise 1
Configuring a Custom Power Scheme

Scenario

Your supervisor has asked you give a demonstration on how to create a custom power scheme with hibernation support. The supervisor has also asked you to demonstrate hibernation.

Goal

In this exercise, you will create a custom power scheme and enable hibernation. You will start Notepad, Calculator, Pinball, and Disk Defragmenter and then hibernate the computer manually. When you bring the computer out of hibernation, you will verify the effects of hibernation on an application that accesses the hard drive.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with a password of **domain**. Create a custom power scheme called Mobile User. On the Mobile User power scheme, enable support for hibernation.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Control Panel, double-click **Power Options**. **c.** In the **Power Options Properties** dialog box, on the **Hibernate** tab, select the **Enable hibernate support** check box, and then click **Apply**.
How much free disk space is required on your computer to support hibernation? How much RAM does your computer have? Are these two numbers related? **Disk space required to support hibernation: Answers will vary. Amount of RAM: Answers will vary. The amount of space for hibernation and the amount of RAM should be the same. The computer needs as much space to support hibernation, as there is RAM in the computer because hibernation saves the desktop to the hard drive.**	
1. (*continued*)	**d.** On the **Advanced** tab, select the **Always show icon on the taskbar** check box. **e.** On the **Power Schemes** tab, click **Save As**, in the **Save Scheme** dialog box, type **Mobile User** and then click **OK**. **f.** Under **Settings for Mobile User power scheme**, specify to turn off the monitor after 10 minutes and to turn off the hard disks after 15 minutes. **g.** Click **OK** to close the **Power Options Properties** dialog box, and then close Control Panel.

Tasks	Detailed Steps
2. Start Notepad, Calculator, Pinball, and run Disk Defragmenter on the C: partition. Immediately following this, hibernate the computer. Once the computer is turned off, start the computer and verify that all of the applications are as you left them.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **calc** and then click **OK**. **c.** Calculate the following (79 * 36.04)= and then leave Calculator open. **d.** Click **Start**, and then click **Run**. **e.** In the **Open** box, type **notepad** and then click **OK**. **f.** In the Notepad window, type **Windows 2000 Hibernation support** and then leave Notepad open. **g.** Click **Start** and then click **Run**. **h.** In the **Open** box, type **pinball** and then click **OK**. **i.** Leave Pinball open. **j.** Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Defragmenter**. **k.** Click the **C:** partition, and then on the **Action** menu, click **Defragment**. **l.** While Disk Defragmenter is running, click **Start**, and then click **Shut Down**. **m.** In the **Shut Down Windows** dialog box, click **Hibernate**, and then click **OK**. *Notice that the screen shows that the computer is hibernating.* **n.** Turn off the computer if necessary, and then restart the computer. *Notice the start up screen message appears, indicating that Windows is resuming.* **o.** Unlock the computer, and then verify that Calculator, Notepad, Pinball, and Disk Defragmenter are still running. **p.** Close all applications and windows, and then log off.

Making Files Available for Offline Use

Topic Objective
To identify the topics for making files available for offline use.

Lead-in
Offline files enable users who have portable computers to work with network files when they are disconnected from the network.

- Introduction to Offline Files
- Configuring a Server for Offline Files
- Configuring a Client Computer for Offline Files
- Using Synchronization Manager to Synchronize Files

**********ILLEGAL FOR NON-TRAINER USE**********

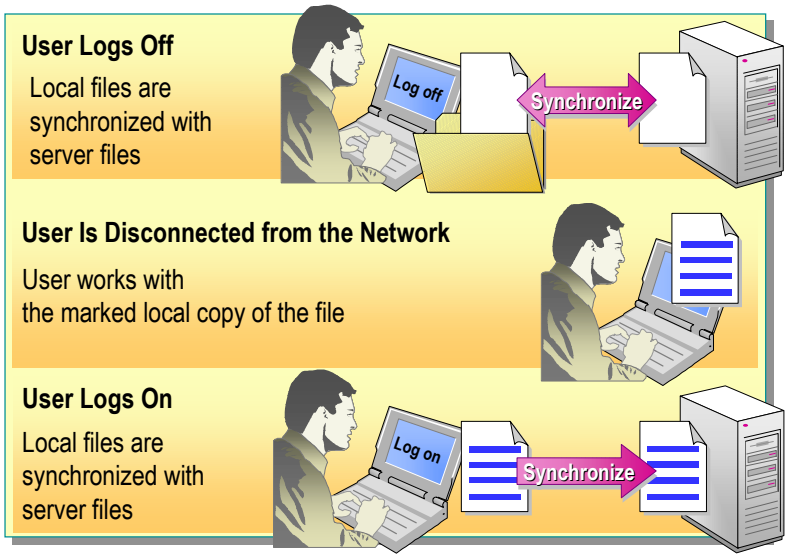
Offline files allow a user to gain access to files stored on a network shared folder when disconnected from the network. Offline files can benefit mobile users as well as network users. With offline files a user can work with a locally cached copy of the network file when disconnected from the network. When the user reconnects to the network the user can have the local cached copy of the file synchronized with the network version. This is possible because offline files are cached on local hard disks, even though the original resides on a network server.

Offline files can be managed with Synchronization Manager, which you access from the **Accessories** menu. Using Synchronization Manager, a user can configure a synchronization schedule and select options to perform synchronization when idle, when logging off, or when logging on.

Introduction to Offline Files

Topic Objective
To illustrate how offline files work for users.

Lead-in
Offline files provide users with continuous access to network files and programs, even when those users are not connected to the network.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain that users have the same access permissions to offline files and folders as they would have if they were connected to the network.

Ensure that students know what caching is.

Mention that when a user logs on to the network and both the network and cached files have changed, Windows 2000 prompts the user to choose which version to keep or allows the user to rename one of the versions and keep both files.

Once a network shared folder has been configured to support offline files, all files on the shared folder have the potential to be configured as offline files. When a user configures a file as offline the user works with the network version while connected to the network. Then, when the user disconnects from the network, the user still has continuous access to network files and programs on his or her computer.

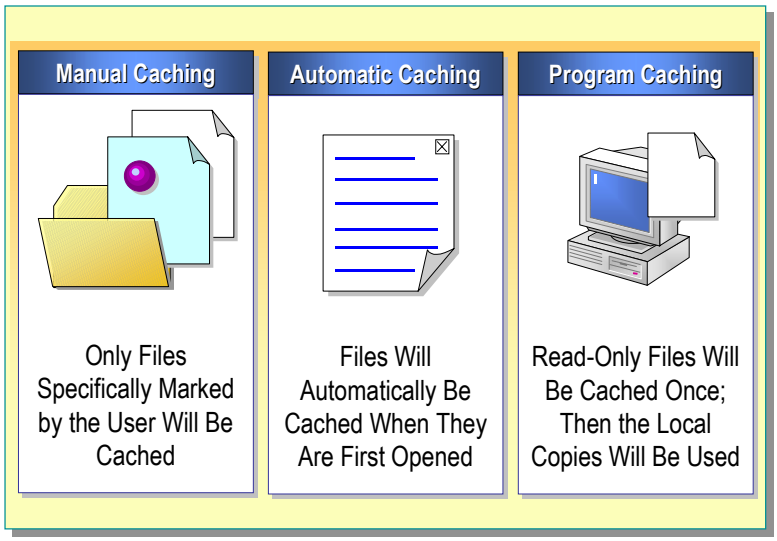
When a file or folder is marked as being available offline, while users are connected to the network they access the network version of the file. When the user disconnects from the network, the following events occur:

- When a user logs off the network, Windows 2000 synchronizes the network files with a local cached copy of the file.
- While disconnected from the network, the user has access to the local cached copy.
- When a user logs back on to the network, Windows 2000 synchronizes any offline file that has been modified by the user with the network version of the file. If the file has been modified in both locations, Windows 2000 prompts the user to choose which version of the file to keep, or the user can rename one file and keep both versions.

Configuring a Server for Offline Files

Topic Objective
To illustrate the caching options available for offline files.

Lead-in
There are three options for caching shared files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

By default, any folder that you share on a computer running Windows 2000 Server or Advanced Server is enabled for offline file use. However, you can specify what method of caching will be enabled. You can also elect to turn off caching on a shared folder.

Delivery Tip
Demonstrate how to set caching options for a shared folder.

Mention that an administrator can choose not to cache a folder.

To set caching options for a shared folder, perform the following steps:

1. In Windows Explorer, right-click the folder for which you want to set caching options for, click **Sharing**, and then click **Caching**.
2. If you do not want the contents of this folder cached, clear the **Allow caching of files in this shared folder** check box. (For example, clear this check box to disable offline file use for a public folder that many users share.)

   –Or–

   If you want to enable offline files, leave the check box selected, choose one of the following options, and then click **OK**.

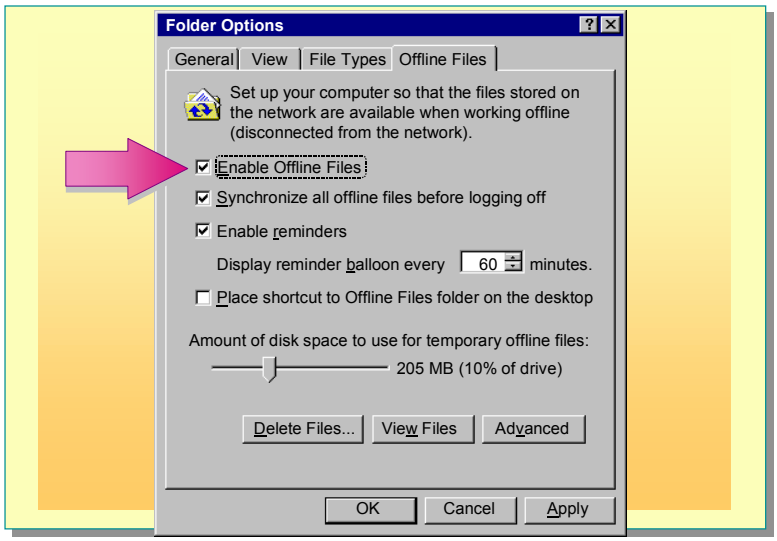
Mention the different options for caching offline files.

Option	Description
Manual caching for documents	Requires users to manually specify the documents that they want cached. Only files marked by users as being available offline will automatically be cached. This is the default setting for shared folders.
Automatic caching for documents	Automatically caches every file in the folder that is opened by the user. Older copies of files are automatically deleted to provide space for newer files. This option results in less network traffic than manual caching and is recommended for folders containing user documents.
Automatic caching for programs	Provides one-way caching for read-only files and for applications that run from the network. Files stored on the server are cached on local hard disks, but changes that users make to those files are not replicated back to the server. This prevents the user from overwriting the original file.

Configuring a Client Computer for Offline Files

Topic Objective
To illustrate the client interface for configuring offline files.

Lead-in
Before a file or folder can be made available offline to a client, the **Enable Offline Files** option must be selected.



**********ILLEGAL FOR NON-TRAINER USE**********

Individual files from a shared network folder or an entire shared network folder can be made available to use offline. By default, offline files are enabled on Windows 2000 Professional.

Before a file or folder can be made available offline to a client, the **Enable Offline Files** option must be selected on the client computer. To enable offline files on the client computer, perform the following steps:

Delivery Tip
Demonstrate how to enable offline files for a client computer.

1. In Windows Explorer, on the **Tools** menu, click **Folder Options**.
2. In the **Folder Options** dialog box, on the **Offline Files** tab, select the **Enable Offline Files** check box.

   When the computer is offline, the files and folders appear in the same directory as they did online. On the user interface, double arrows indicate an offline file.

Mention that in addition to offline files, users can make Web pages available offline.

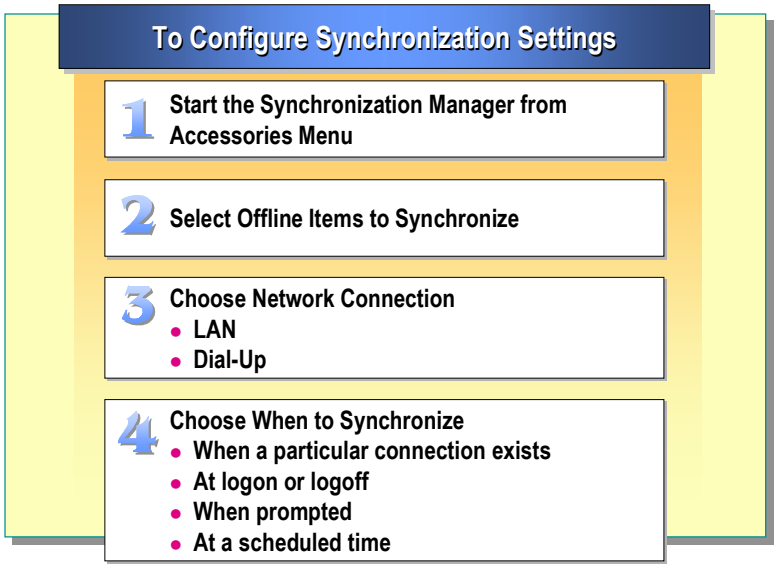
Note In addition to offline files, you can make a Web page available offline so that you can view it when you do not have a network or Internet connection.

To make the current Web page available offline, on the **Favorites** menu, click **Add to Favorites**, and then select the **Make available offline** check box. To specify a schedule for updating that page, and how much content to download, click **Customize**. Follow the instructions on your screen.

Using Synchronization Manager to Synchronize Files

Topic Objective
To identify the tasks for synchronizing files.

Lead-in
Synchronization Manager provides users with a single location for synchronizing offline resources.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
When using offline files, it is recommended that users synchronize when they log on to the network.

When you set up offline files, by default Windows 2000 automatically synchronizes offline files when a user disconnects or reconnects to the network. You can configure how these files are synchronized. To do this, use the Synchronization Manager, which, in addition to enabling you to synchronize files, enables you to synchronize other offline network resources, such as folders, e-mail, and databases, in a single location. Synchronization Manager quickly scans the system for any changes, and if it detects changes, the resources are automatically updated, which speeds up the synchronization process.

Configuring Synchronization Settings

To better manage files on the computer and on the network, you can choose when offline items are synchronized. For example, a user can save time by specifying that large database files only be synchronized when the computer is using a high-speed connection and that all personal documents stored in a specific file are synchronized every time they are connected to the corporate local area network (LAN).

To open Synchronization Manager and configure synchronization settings, perform the following steps:

Delivery Tip
Demonstrate the steps for synchronizing files. Point out the different options.

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Synchronize**.
2. In the **Items to Synchronize** dialog box, select the check boxes for the offline items that you want to synchronize.
3. Click **Setup** to display the **Synchronization Settings** dialog box and then select either a LAN or a dial-up connection.
4. To accomplish the tasks in the following table, perform the actions described in the following table.

To	Perform this action
Select files to synchronize for a particular connection	On the **On/Idle** tab, click the network connection that you want to use in the **When I am using this network connection** list, and then select the check boxes beside the offline items that you want to synchronize in the **Synchronize the following checked items** list.
Synchronize when logging on	On the **Logon/Logoff** tab, click **When I log on to my computer**.
Synchronize when logging off	On the **Logon/Logoff** tab, click **When I log off my computer**.
Prompt user before automatically synchronizing your offline items	On the **Logon/Logoff tab**, select the **Ask me before synchronizing the items** check box.
Schedule synchronization when the system is idle or for specific times	On the **Scheduled** tab, click **Add** to start the Scheduled Synchronization wizard. The wizard assists you in creating a synchronization schedule.

5. After selecting an option, click **OK**.

Lab B: Configuring Offline Files

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create offline files, configure a shared folder for offline support, and the synchronize offline files.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create offline files.
- Configure a shared folder for offline support.
- Synchronize offline files.

Prerequisite

Before working on this lab, you must have knowledge of offline files.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server in the nwtraders.msft domain.

Estimated time to complete this lab: 30 minutes

Exercise 1
Configuring a Client Computer for Offline Files

Scenario

You need to demonstrate the concept of offline files to the Human Resources manager and his staff.

Goal

In this exercise, you will:

- Create an offline file manually.
- Create a shared folder and configure caching options on the share.
- Create an offline file automatically.
- Disconnect from the network and then modify both the manual offline document and the automatic offline document.
- Configure synchronization schedules with Synchronization Manager, and then reconnect to the network and synchronize offline files.
- Verify synchronization by viewing the modifications in offline documents.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and enable offline files.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned number) Password: **domain** Log on to: **nwtraders** **b.** In Control Panel, double-click **Folder Options**. **c.** In the **Folder Options** dialog box, on the **Offline Files** tab, select the **Enable Offline Files** check box, and then click **OK**.
Note: This option is enabled by default in Windows 2000 Professional and disabled by default in Windows 2000 Server.	
1. (*continued*)	**d.** Close Control Panel.
2. Connect to the APM and ACPI Entry Level file in the path \\London\Student folders\Student*x* (where *x* is your assigned student number) and mark it as available offline.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\london\student folders** and then click **OK**. **c.** In the **Student Folders on london** dialog box, double-click **Student***x* (where *x* is your assigned student number), and then double-click **User Data**. **d.** In the **User Data** window, right-click **APM and ACPI Entry Level**, and then click **Make Available Offline**. **e.** On the **Welcome to the Offline Files Wizard** page, click **Next**. **f.** Clear the **Automatically synchronize the Offline Files when I log on and log off my computer** check box if necessary, and then click **Next**. **g.** Accept the default settings to enable reminders and not create a shortcut on the desktop, and then click **Finish**.

Tasks	Detailed Steps
Note: Synchronization occurs. Notice the offline symbol on the APM and ACPI Entry Level file.	
2. (*continued*)	**h.** Close the **User Data** window.
The first time synchronization occurs on a file, where does the offline file reside? **On the local computer's hard drive.**	
3. Using Computer Management, connect to London and share the \\London\Student folders\Student*x*\Research data folder on the London computer as Student*x* Research Data (where *x* is your assigned student number), and then configure caching as Automatic Caching for Documents.	**a.** Open Computer Management from the **Administrative Tools** menu. **b.** In the console tree, right-click **Computer Management (Local)**, and then click **Connect to another computer**. **c.** In the **Select Computer** dialog box, click **london**, and then click **OK**. **d.** In the console tree, expand **System Tools**, expand **Shared Folders**, right-click **Shares**, and then click **New File Share**. **e.** In the Create Shared Folder wizard, click **Browse**. **f.** In the **Browse For Folder** dialog box, expand **C$**, expand **moc,** expand **Win2152b,** expand **Classroom**, expand **Student Folders**, and then expand **Student***x* (where *x* is your student number). **g.** Click **Research Data**, and then click **OK**. **h.** In the Create Shared Folder wizard, in the **Share name** box, type **Student***x* **Research Data** (where *x* is your student number), and then click **Next**. **i.** Click **Customize share and folder permissions**, and then click **Custom**. **j.** In the **Customize Permissions** dialog box, click **Remove**, and then click **Add**. **k.** In the **Select Users, Computers, or Groups** dialog box, in the **Look in** box, click **Entire Directory**. **l.** Under **Name**, click **Admin***x* (where *x* is your assigned student number), click **Add**, click **Domain Admins**, click **Add**, and then click **OK**. **m.** In the **Customize Permissions** dialog box, under **Name**, click **Admin***x* (where *x* is your assigned student number), and then under **Permissions**, allow the Full Control permission. **n.** Under **Name**, click **Domain Admins**. **o.** Under **Permissions**, allow the Full Control permission, and then click **OK**.

Tasks	Detailed Steps
3. (*continued*)	**p.** In the **Create Shared Folder** wizard, click **Finish**, and then click **No** to specify not to create another shared folder. **q.** In Computer Management, under **System Tools**, under **Shared Folders**, click **Shares**. **r.** In the details pane, in the **Shared Folder** column, right-click **Student***x* **– Research Data** (where *x* is your assigned student number), and then click **Properties**. **s.** In the **Student***x* **Research Data Properties** dialog box, on the **General** tab, click **Caching**.

What four options can be set on a shared folder?

Allow caching of files in this shared folder – unchecked

Automatic Caching for Documents

Automatic Caching for Programs

Manual Caching for Documents

3. (*continued*)	**t.** In the **Caching Settings** dialog box, in the **Setting** box, click **Automatic Caching for Documents**, and then click **OK**. **u.** Click **OK** to close the **Student***x* **Research Data Properties** dialog box. **v.** Close Computer Management.
4. Connect to the Plug and Play Architecture file in the path \\London\Student*x* - Research Data (where *x* is your assigned student number). Open the file, and then close the file to create an offline file automatically.	**a.** Click **Start**, and then click **Run**. **b.** **In** the **Open** box, type **\\london\Student***x* **Research Data** (where *x* is your assigned student number), and then click **OK**. **c.** In the **Student***x* **Research Data on london** window, open Plug and Play Architecture.

Note: Because you selected the **Automatic Caching for Documents** option for the shared folder, opening the file automatically marks the file as offline.

4. (*continued*)	**d.** Close Plug and Play Architecture. **e.** Close the **Student***x* **Research Data on london** window.
5. Disconnect from the network.	**a.** In Control Panel, double-click **Network and Dial-up Connections**. **b.** Right-click **Local Area Connection**, click **Disable**, and then minimize Network and Dial-up Connections.

Note: The previous task has the same effect as physically removing the computer from the network.

Tasks	Detailed Steps
6. While disconnected from the network, try to gain access to the APM and ACPI Entry Level file using the path \\London\Student Folders\Student*x* (where *x* is your student number). In the file, type your name, and then save the file.	**a.** Click **Start**, and then click **Run**. **b.** **In** the **Open** box, type **\\london\student folders** and then click **OK**.
Note: The only folder that displays is Student*x* (where *x* is your assigned student number).	
6. (*continued*)	**c.** In the **Student folders on london** window, double-click **Student***x* (where *x* is your student number). **d.** In the **Student***x* window, double-click **User Data**. **e.** Double-click **APM and ACPI Entry Level**. **f.** In the document, type your name, save and close the document, and then close the **User Data** window. **g.** Click **Start**, and then click **Run**. **h.** In the **Open** box, type **\\london\Student***x* **Research Data** (where *x* is your assigned student number), and then click **OK**. **i.** In the **Student***x* **Research Data on london** window, double-click **Plug and Play Architecture**. **j.** In the document, type your name, and then save and close the document. **k.** Close the **Student***x* **Research Data on london** window.

Which copy did you modify in the preceding task, the original file on the network shared folder or the locally cached copy of the file?

The locally cached copy of the file.

Tasks	Detailed Steps
7. Using Synchronization Manager from the **Accessories** menu, create a synchronization schedule for the \\London\Student*x* - Research Data connection in Synchronization Manager (where *x* is your assigned student number). The schedule is weekdays at 4:00 A.M.	**a.** Click **Start**, point to **Programs**, point to **Accessories**, and then click **Synchronize**. **b.** In the **Items to Synchronize** dialog box, click **Setup**. **c.** In the **Synchronization Settings** dialog box, on the **Scheduled** tab, click **Add**. **d.** In the Scheduled Synchronization wizard, click **Next**. **e.** Under **On this connection, synchronize these items**, under **Offline Files**, select the **\\london\student*x* research data on london** check box, and then click **Next**. **f.** Under **Select time and day you want this synchronization to start**, in the **Start time** box, specify **4:00 AM**, click **Weekdays**, and then click **Next**. **g.** Under **Type a name for this scheduled synchronization**, type **Research Data Update** **h.** Click **Next**, and then click **Finish**. **i.** Click **OK** to close the **Synchronization Settings** dialog box. **j.** Click **Close** to close the **Items to Synchronize** dialog box.
8. Reconnect to the network and complete the synchronization process.	**a.** Restore Network and Dial-up Connections. **b.** Right-click **Local Area Connection**, click **Enable**, and then close Network and Dial-up Connections. **c.** In the System Tray, at the lower-right side of the desktop, click the **Offline Files Status** icon, which resembles a computer with an I symbol. **d.** In the **Offline File Status** dialog box, click **Details**, and then click **View Files**.
Note: Notice the status in the Availability column. For the Manual Offline file the status appears as **Always available offline**, while the Automatic Offline file appears as **Temporarily available offline**.	
8. (*continued*)	**e.** Close the Offline Files Folder window, and then click **OK** to close the **Offline Files Status** dialog box. *The synchronization process completes.*
9. Open the \\London\Student Folders\Student*x*\APM and ACPI Entry Level file (where *x* is your assigned student number) and verify that your name appears. Open the \\London\Student Folders\Student*x*\Plug and Play Architecture file and verify that your name appears.	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **\\london\student folders** and then click **OK**. **c.** In the Student Folders on london window, double-click **Student*x*** (where *x* is your student number). **d.** In the **Student*x*** window, double-click **User Data**. **e.** Double-click **APM and ACPI Entry Level**. **f.** Verify that your name appears in the document, close the document, and then close the **User Data** window. **g.** Click **Start**, and then click **Run**.

Tasks	Detailed Steps
9. (*continued*)	**h.** In the **Open** box, type **\\london\Student***x* **Research Data** (where *x* is your assigned student number), and then click **OK**. **i.** In the Student*x* Research Data on london window, double-click **Plug and Play Architecture**. **j.** Verify that your name appears in the document, close the document, and then close the Student*x* Research Data on london window.
When connected to the network and accessing an offline file, which file is accessed: the locally cached copy or the version of the file on the network shared folder? **The version of the file on the network shared folder.**	
10. Disable offline files.	**a.** In Control Panel, double-click **Folder Options**. **b.** In the **Folder Options** dialog box, on the **Offline Files** tab, clear the **Enable Offline Files** check box, and then click **OK**. **c.** Close Control Panel, and then log off.

Connecting to Networks and Computers

Topic Objective
To identify the topics for connecting clients to networks and other computers.

Lead-in
Windows 2000 Professional makes it easy for users to remotely connect to networks and other computers.

- Creating a Dial-up Connection
- Connecting to a Private Network Through the Internet
- Connecting Directly to Another Computer

**********ILLEGAL FOR NON-TRAINER USE**********

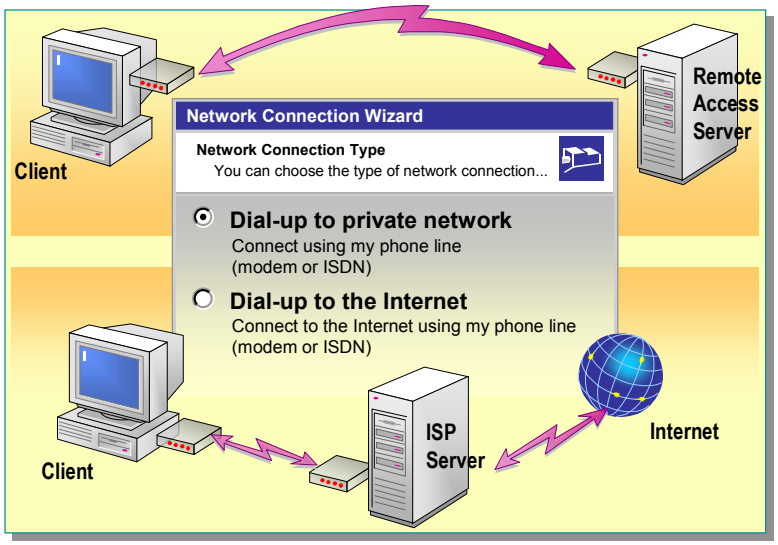
If students ask you about VPN, delay the discussion until it appears later in this section.

Windows 2000 Professional makes it easy for users to remotely connect to networks, including private networks, called virtual private networks (VPNs), over dial-up, infrared, and direct cable connections. A wizard guides you through the steps of setting up connections to different types of networks, thus eliminating the need to manually configure settings. The Network Connection wizard helps to create many types of new connections. Connection setup is also automated, eliminating the need to download and install additional services.

Creating a Dial-up Connection

Topic Objective
To illustrate the two types of dial-up connections.

Lead-in
You use the Network Connection wizard to create and configure a dial-up connection to either a private network or to an ISP.



**********ILLEGAL FOR NON-TRAINER USE**********

Before you can connect to a remote network or computer, you need to create a new connection on a client computer. Use the Network Connection wizard to create and configure a dial-up connection to either a private network or to an Internet service provider (ISP).

To create a new dial-up connection, perform the following steps on the client:

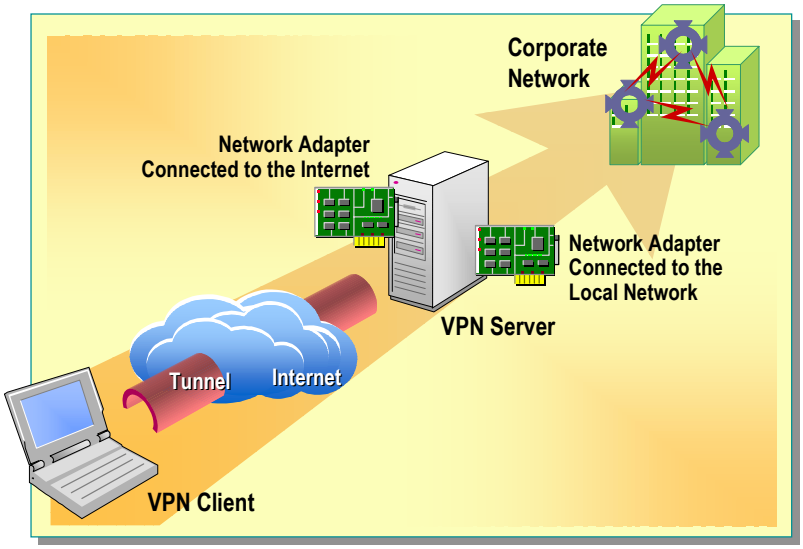
Delivery Tip
Demonstrate the steps for creating the two dial-up connections with the wizard.

1. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**.
2. In **Network and Dial-up Connections**, double-click **Make New Connection**.
3. In the Network Connection wizard, click **Next**, and then click either **Dial-up to private network** or **Dial-up to the Internet**.
4. Select one of the following:
   - If you clicked **Dial-up to private network**, select a device to use for the connection, and then click **Next**. Enter the phone number of the computer to which you are connecting, and then click **Next**. Click **Only for myself**, and then click **Next**. Type a name for the connection.
   - If you clicked **Dial-up to the Internet** and are connecting through your LAN, select **I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)**, and then click **Next**. Select **I connect through a local area network (LAN)**. You will be prompted for proxy settings and Internet mail account information.
5. Click **Finish**.

Connecting to a Private Network Through the Internet

Topic Objective
To illustrate the process of connecting to a private network through the Internet.

Lead-in
Typically users will connect to a private network by first connecting to an ISP, and then connecting to the LAN through the existing Internet connection.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain that VPNs can significantly reduce the cost of reaching remote offices and users.

You also use the Network Connection wizard to create a connection to a private network through the Internet, called a VPN. A VPN uses tunneling protocols, such as Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP), across an unsecured network to provide remote clients with access to a corporate network. VPNs can significantly reduce the cost of reaching remote offices and users by eliminating the need to use long-distance phone connections.

Delivery Tip
Demonstrate creating a VPN connection through the Internet.

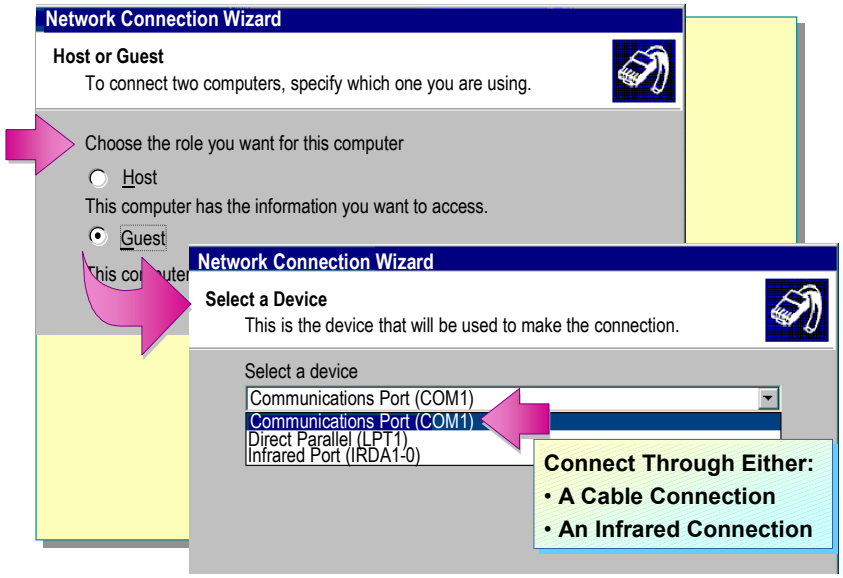
To create a new VPN connection, perform the following steps on the client:

1. In Network and Dial-up Connections, double-click **Make New Connection**, and then click **Next**.
2. In the Network Connection wizard, select **Connect to a private network through the Internet**, click **Next**, and then do one of the following:
   - If you need to establish a connection with your ISP or some other network before tunneling to your destination computer or network, click **Automatically dial this initial connection**, click a connection in the list, and then click **Next**.
   - If you do not want to automatically dial an initial connection, click **Do not dial the initial connection**, and then click **Next**.
3. Type the host name or Internet Protocol (IP) address of the computer or network to which you are connecting, and then click **Next**.
4. Click **Only for myself**, and then click **Next**.
5. Type a name for the connection, and then click **Finish**.

Connecting Directly to Another Computer

Topic Objective
To illustrate key pages in the Network Connection wizard for establishing a direct connection.

Lead-in
You also use the Network Connection wizard to create a direct (cable or infrared) connection to another computer.



**********ILLEGAL FOR NON-TRAINER USE**********

You can also use the Network Connection wizard to create a direct connection to another computer with either a cable or infrared device. A cable connection uses the standard and enhanced (ECP) parallel ports and requires Basic or Fast parallel cables. An infrared connection requires an infrared transceiver on both computers. For two devices to communicate by using infrared, the infrared transceivers must be pointed at each other, usually spaced no more than a meter apart. To create a direct connection to another computer, perform the following steps on the client:

Delivery Tip
Demonstrate the wizard for creating both a guest and host connection.

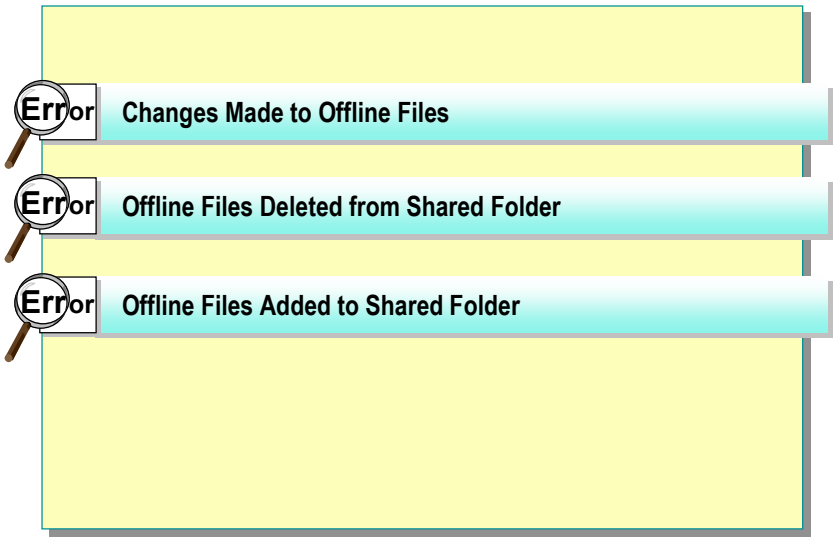
1. In Network and Dial-up Connections, double-click **Make New Connection**.
2. In the Network Connection wizard, select **Connect directly to another computer**, click **Next**, and then do one of the following:
   a. If the computer will host information that other computers will gain access to, click **Host**, and then click **Next**.
      - Choose the device for the connection, and then click **Next**.
      - Select the users that you want to allow to connect to the computer.

   b. If the computer will be used to gain access to information on another computer, click **Guest**, and then click **Next**.
      - Choose the device for the connection, and then click **Next**. The device must be the same type as the one the host is using.
      - If you want this connection to be made available to all users of this computer, click **For all users**, and then click **Next**. If you want to reserve the connection for yourself, click **Only for myself**, and then click **Next**.
3. Type a name for the connection, and then click **Finish**.

Identifying Solutions to Mobile Computing Problems

Topic Objective
To identify potential mobile computing problems and their solutions.

Lead-in
It's important to identify potential mobile computing problems and their solutions in order to maintain a reliable working environment for mobile computer users.



**********ILLEGAL FOR NON-TRAINER USE**********

The following table lists common mobile computing problems and possible solutions.

Problem	Solution
Someone else made changes to the same network file that you updated offline.	You are given a choice of saving your version, saving the one on the network, or saving both. To save both versions of the file, give your version a different file name, and both files will appear in both locations.
You change a network file while working offline but somebody else on the network deletes that file.	You can choose to save your version onto the network or delete it from your computer.
You are disconnected from the network when a new file is added to a shared network folder that you have made available offline.	The new file will be added to your computer when you reconnect and synchronize.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Configuring Hardware for Mobile Computing
- Configuring Power Management Options for Mobile Computing
- Making Files Available for Offline Use
- Connecting to a Network Remotely
- Identifying Solutions for Mobile Computing Problems

**********ILLEGAL FOR NON-TRAINER USE**********

1. A user would like to start her computer running Windows 2000 Professional with the network adapter disabled so that she can test an application without impacting the network. How can she accomplish this?

   Create a profile called Network Disabled on her computer. Restart the computer and, at startup, select the new hardware profile Network Disabled. While started in the Network Disabled hardware profile, in Device Manager, set the network adapter to disabled with this profile. Then, instruct her to select the hardware profile Network Disabled for testing the application.

2. A salesperson would like to configure her laptop so that it uses less battery power when she uses it on the road, yet still protects her desktop if power to her laptop fails. What feature can she use for this? And why?

   Configure the computer to hibernate because it saves her desktop to the hard drive thus protecting her desktop. Standby will not protect your desktop from a loss of power to the laptop because it does not save the desktop to the hard drive.

3. A salesperson would like to configure her laptop to hibernate. When she tries to enable hibernation she receives a warning that she does not have adequate disk space to enable hibernation. How much disk space does she need? How can you solve this issue?

   To enable hibernation there must be free disk space on the computer equal to or greater than the amount of RAM in the computer. She must not have free space equal, or greater than, to the amount of RAM in her computer. To solve this she must free up disk space in order to enable hibernation.

4. An administrator of a server running Microsoft Windows NT® version 4.0 wants the network clients running Windows 2000 to create offline files from the shared folders on the server running Windows NT 4.0. What must be configured in addition to sharing the folders on the server running Windows NT 4.0 to enable Windows 2000 clients to create offline files from the shared folders?

   Nothing. Clients running Windows 2000 can create offline files from shared folders located on computers running Microsoft Windows 95, Microsoft Windows 98 and Windows NT 4.0.

5. A company's mobile sales force currently uses long distance dial-up connections from their laptops running Windows 2000 Professional to connect to the company's private network. Is there a more cost effective method of connecting to the remote access server that you can present to the company? How would you implement this solution?

   Use a VPN connection. Configure the mobile sales force laptops with dial-up connections to a local ISP and then create a VPN connection using these local dial-up connections.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 12: Configuring and Managing Disks

Contents

Overview	1
Windows 2000 Disk Types	2
Creating Partitions on a Basic Disk	7
Creating Volumes on a Dynamic Disk	8
Lab A: Working with Dynamic Disks	13
Performing Common Disk Management Tasks	19
Lab B: Creating and Mounting a New Volume	29
Best Practices	33
Review	34

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware.

Instructor Notes

Presentation:
75 Minutes

Labs:
60 Minutes

This module provides students with the knowledge and skills necessary to set up and manage basic and dynamic disks, including upgrading a basic disk to a dynamic disk.

At the end of this module, students will be able to:

- Describe the different disk types in Microsoft® Windows® 2000.
- Create partitions on a basic disk.
- Create volumes on a dynamic disk.
- Perform common disk management tasks.
- Apply best practices for configuring and managing hard disks.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_12.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Windows 2000 Disk Types

  First, present information on basic disks. Emphasize that a basic disk can have only four partitions, although one partition can be a logical partition with multiple logical drives. Then, present information on dynamic disks. Emphasize to the students that they cannot create extended partitions or dynamic volumes on removable storage devices. Ensure that students know the difference between basic and dynamic disks in Windows 2000.

- Creating Partitions on a Basic Disk

  Demonstrate creating a partition on a basic disk by using the Create Partition wizard.

- Creating Volumes on a Dynamic Disk

  First, present information on upgrading a basic disk to a dynamic disk, including the upgrade results. Mention that an administrator cannot convert a dynamic disk back to a basic disk but can revert a dynamic disk back to a basic disk. Then, explain and demonstrate the process for creating and extending simple volumes. Emphasize that a volume can only be extended if it was originally created on a dynamic disk, but not if it was converted from a basic disk.

- Performing Common Disk Management Tasks

  First, present information on common disk management tasks: checking the status of hard disk and repairing and deleting hard disks. Demonstrate repairing and deleting partitions and volumes. Then, demonstrate adding new hard disks and hard disks from another computer. Mention what happens when incomplete volumes are imported.

  Next, present information on managing drive letters and drive paths. Mention that mounting a local disk to an empty folder on a local NTFS file system partition or volume is a new feature of Windows 2000. Then, demonstrate how to manage hard disks remotely, by managing a student's hard disk. Finally, show students the interface for defragmenting a hard disk. Mention that it is important to defragment a hard disk because the fragmentation of files decreases system performance when the computer must read data files from various locations.

- Best Practices

  Present the best practices for hard disk configuration issues. Discuss each issue, and the rationale behind the recommendations, in detail. Give examples of when each issue would be important to the user.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

The labs in this module require each student computer be configured as a member server of the nwtraders.msft domain. To prepare the student computers to meet this requirement, complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- Hard Disk 0 will be converted to a dynamic disk.
- A 125-megabyte (MB) volume will be created on Hard Disk 0.
- A 100-MB volume will be created on Hard Disk 0 and will mounted as C:\Mount.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about configuring and managing disks and partitions on a computer running Windows 2000.

- **Windows 2000 Disk Types**
- **Creating Partitions on a Basic Disk**
- **Creating Volumes on a Dynamic Disk**
- **Performing Common Disk Management Tasks**
- **Best Practices**

**********ILLEGAL FOR NON-TRAINER USE**********

If students have questions about dynamic disks, tell them you will discuss that topic later in this module.

One of the tasks involved in administering a computer is managing disks. Knowing what tools are available to set up and manage disks, and what capabilities are provided with Windows 2000 allows you to better manage disk drives, and configure advanced features, such as implementing a fault-tolerance feature or assigning a new partition to a folder on an existing partition rather than assigning it a new drive letter.

Microsoft® Windows® 2000 offers two disk types: basic disk and dynamic disk. Basic disk uses the partitions that are familiar to users of earlier versions of Windows and Microsoft MS-DOS®, while dynamic disks use volumes that provide more efficient use of space than partitions in computers with multiple hard disks, in addition to providing options for data redundancy. An understanding of basic and dynamic disks will allow you to configure hard disks efficiently on a Windows 2000–based computer.

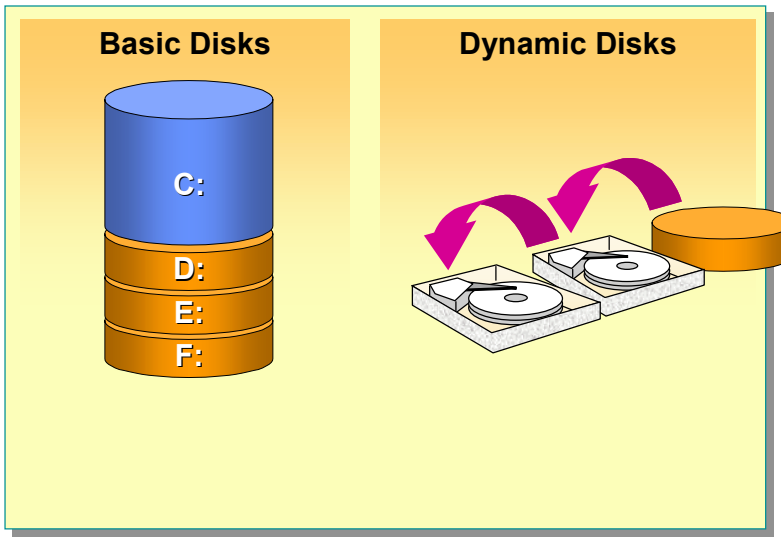
At the end of this module, you will be able to:

- Describe disk types in Windows 2000.
- Create partitions on a basic disk.
- Create volumes on a dynamic disk.
- Perform common disk management tasks.
- Apply best practices for configuring and managing hard disks.

◆ Windows 2000 Disk Types

Topic Objective
To illustrate the different disk types in Windows 2000.

Lead-in
Windows 2000 supports basic disks and dynamic disks.



**********ILLEGAL FOR NON-TRAINER USE**********

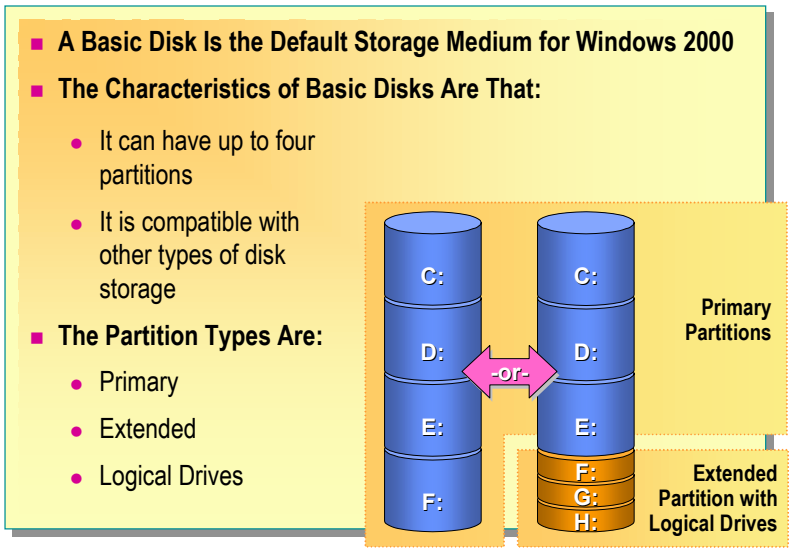
Do not present the information on basic and dynamic disks in this topic. Wait until the basic and dynamic disk topics that follow.

When you configure disks on your computer, you must decide between implementing basic disks and dynamic disks. The type of hard disk you select determines how you can use the space on the hard disk. Dynamic disks are new to Windows 2000, and provide more flexibility in how you set up your hard disk than basic disks provide. For example, you can implement fault tolerance on a dynamic disk, but not on basic disks.

Basic Disks

Topic Objective
To show the partitions on a basic disk.

Lead-in
Basic disks contain primary partitions and extended partitions with logical drives, and are compatible with disk partitions and sets in Windows NT 4.0.



**********ILLEGAL FOR NON-TRAINER USE**********

When you install a new disk, Windows 2000 recognizes it and configures it as a basic disk. Basic disks are the default storage medium for Windows 2000, and provide limited capabilities for configuring your disks. You use basic disks when you have multiple operating systems installed and need to dual boot, because Windows 2000 is the only operating system that recognizes dynamic disks.

Delivery Tip
Demonstrate to students how to access the Disk Management tool in Computer Management in Microsoft Management Console (MMC). Have students determine which type of hard drive their computers have. It should be a basic disk.

Key Points
A basic disk can have up to four partitions, but a basic disk cannot have new volume sets, stripe sets, or RAID-5 sets created on it.

An administrator can set up a basic disk to have up to four primary partitions or three primary partitions and one extended partition with logical drives.

Characteristics of a Basic Disk

The characteristics of a basic disk are the following:

- A basic disk can contain up to four partitions. A *partition* is a logical portion of a hard drive to which you assign a drive letter or a mount point. You can only create partitions on a basic disk.
- A basic disk in Windows 2000 is compatible with other types of disk storage that includes partitions, and previously existing volume sets, stripe sets and redundant array of independent disks (RAID-5) from Microsoft Windows NT® version 4.0 and other operating systems.

Important You cannot create new volume sets, stripe sets, or RAID-5 sets on a Windows 2000 basic disk. To implement these storage methods, you must upgrade to a dynamic disk. After an upgrade, Windows 2000 can, however, read previously existing versions of volume sets, stripe sets, or RAID-5 sets created on Windows NT.

Partition Types on Basic Disks

A basic disk can have four partitions, which can be made up of four primary partitions, or up to three primary partitions and one extended partition containing one or more logical drives. In Windows 2000, you can create, delete, and format basic partitions without having to restart your computer for the changes to take effect.

The following list describes the types of partitions available in Windows 2000:

- *Primary partition*. A portion of usable storage space that you create from unallocated space on a disk. Assign a drive letter to each partition.
- *Extended partition*. A portion of usable storage space you create from unallocated space on a disk when you want to create more than four storage spaces on a basic disk. You can subdivide an extended partition into logical drives. Do not assign a drive letter to an extended partition, but rather to its logical drives.
- *Logical drive*. A portion created within an extended partition. Format it and assign it a drive letter. A logical drive cannot span multiple disks.

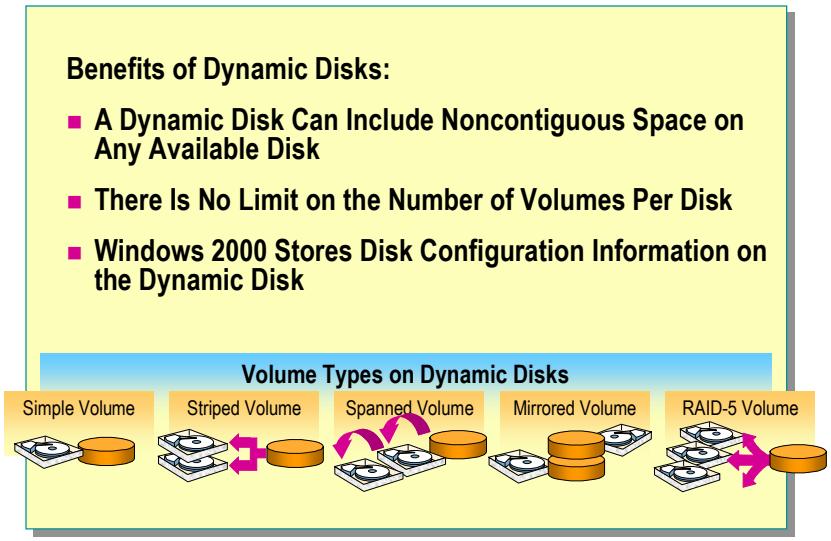
Key Point
When administrators create partitions on a disk, they should leave 1 MB of unallocated space in case they want to convert to a dynamic disk later. The conversion process needs at least 1 MB of unallocated space in order to succeed.

Important When you create partitions, you should leave a minimum of 1 megabyte (MB) of unallocated space on the disk in case you decide to convert the basic disk to a dynamic disk. The conversion process uses 1 MB of space on each dynamic disk to store a database that tracks the configuration of all dynamic disks in the computer.

Dynamic Disks

Topic Objective
To illustrate the volume types for dynamic disks, and the interface for configuring dynamic disks.

Lead-in
On a dynamic disk, storage is divided into volumes instead of partitions.



**********ILLEGAL FOR NON-TRAINER USE**********

Dynamic disks are a new form of disk storage for Windows 2000 that provide benefits and offer you a variety of volume types to set up. Create a dynamic disk by upgrading a basic disk. Dynamic disks are more efficient and provide greater capability and flexibility than basic disks. For example, with dynamic disks you can easily implement redundancy of data.

Benefits of Dynamic Disks

A disk that is converted from a basic to dynamic disk contains volumes instead of partitions. A *volume* is a logical portion of a hard drive to which you assign a drive letter or a mount point. You can only create volumes on a dynamic disk. Dynamic disks has several advantages over basic disks:

- Volumes can be extended to include noncontiguous space on any available disks.
- There is no limit to the number of volumes that you can create per disk.
- Windows 2000 stores dynamic disk configuration information on the disk, rather than in the registry or in other places where it might not be updated accurately. Windows 2000 replicates this disk configuration information to all other dynamic disks so that the failure of a single disk will not affect access to data on other disks.

Be sure to mention that a hard disk can be basic or dynamic, but not both.

A hard disk can be basic or dynamic, but not both; you cannot combine storage types on one disk. However, if your computer has multiple hard disks, you can configure each hard disk in a computer as either basic or dynamic, and therefore have both types within a single system.

Key Points
An administrator cannot create new volume sets, stripe sets, or RAID-5 sets on basic partitions in Windows 2000. An administrator can only create similar disk configuration on a dynamic disk.

Delivery Tip
Briefly discuss with students the advantages and disadvantages of each type of volume using dynamic storage.

Important You cannot create new volume sets, stripe sets, or RAID-5 sets on basic partitions in Windows 2000. You can only create these disk configurations on dynamic disks. In addition, because removable storage devices can only contain primary partitions, you cannot extend or create any dynamic volumes in these devices.

Volume Types on Dynamic Disks

You can use the following volume types on a dynamic disk:

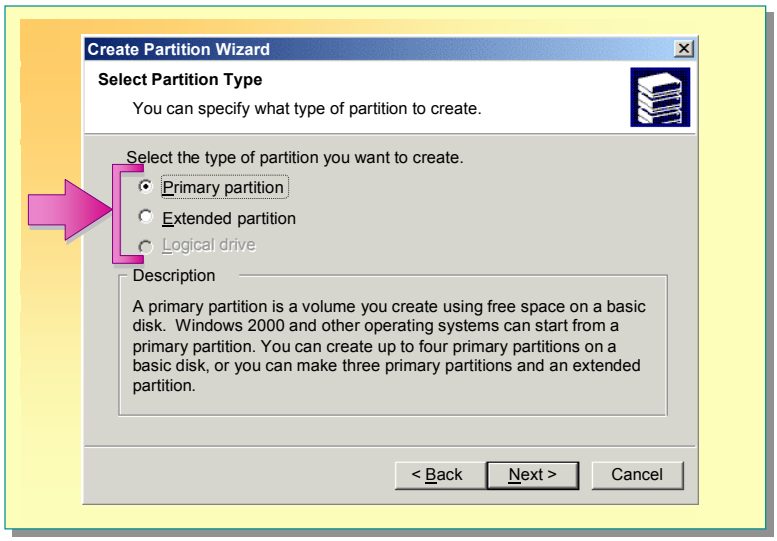
- A *simple volume* contains disk space from a single disk.
- A *striped volume* combines areas of free space from two or more disks (up to 32 hard disks) into one volume. When data is written to a striped volume, it is divided into 64-kilobyte (KB) blocks and spread equally among all disks in the array. An array is a collection of two or more disks. This process of dividing data across a set of disks improves disk performance but does not provide fault tolerance. Fault tolerance is the ability of a computer or operating system to respond to a catastrophic event, such as a hard disk failure, without loss of data.
- A *spanned volume* includes disk space from two or more disks (up to 32 disks). When data is written to a spanned volume, the portion of the spanned volume residing on the first disk is filled up first, and then data is written to the next disk in the volume. If a particular disk fails in the spanned volume, then all data stored on that disk is lost. Similar to a volume set in earlier versions of Windows NT, a spanned volume allows you to combine disk storage but does not improve disk performance. Disk performance is the speed with which the computer can access data on one or more disks.
- *Mirrored volumes* are two identical copies of a simple volume, each stored on a separate hard disk. Mirrored volumes provide fault tolerance in the event of hard disk failure.
- *RAID-5 volumes* are fault-tolerant striped volumes. Windows 2000 adds a parity stripe to each disk in the volume. Parity is a mathematical technique that adds bits to a data stream that contain redundant information, allowing reconstruction of the data stream if part of the stream is corrupted or absent. The data and the parity information are arranged so they are always on separate disks. A parity stripe block exists for each row across the disk. Windows 2000 uses the parity information in those stripes to reconstruct data when a hard disk fails. RAID-5 volumes require a minimum of three hard disks.

Note For more information on mirrored and RAID-5 volumes, see module 13, "Implementing Disaster Protection," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Creating Partitions on a Basic Disk

Topic Objective
To show the Create Partition wizard interface.

Lead-in
You should create partitions instead of dynamic volumes when the disk must also be supported by Windows NT 4.0 or earlier.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the process to create a partition on a basic disk on the instructor computer.

Basic disk storage is used by all Windows operating systems prior to Windows 2000. In a network with multiple operating systems, it is important to know how to use the Disk Management tool in Computer Management in Microsoft Management Console (MMC) to create basic disks that support earlier versions of software.

On basic disks, you can only create primary partitions, extended partitions, and logical drives. To create primary partitions on a basic disk, perform the following steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Computer Management**.
2. In Computer Management, click **Disk Management**, right-click the unallocated space on the basic disk, and then click **Create Partition**.
3. In the Create Partition wizard, click **Next**.
4. Click **Primary Partition** or **Extended Partition**, and then follow the on-screen instructions.

◆ Creating Volumes on a Dynamic Disk

Topic Objective
To describe the procedure for creating dynamic volumes.

Lead-in
When you install Windows 2000 on a computer, the disks are basic disks. You can upgrade a basic disk to a dynamic disk without loss of data.

- **Upgrading from a Basic Disk to a Dynamic Disk**
- **Creating Simple Volumes**
- **Extending Simple Volumes**

**********ILLEGAL FOR NON-TRAINER USE**********

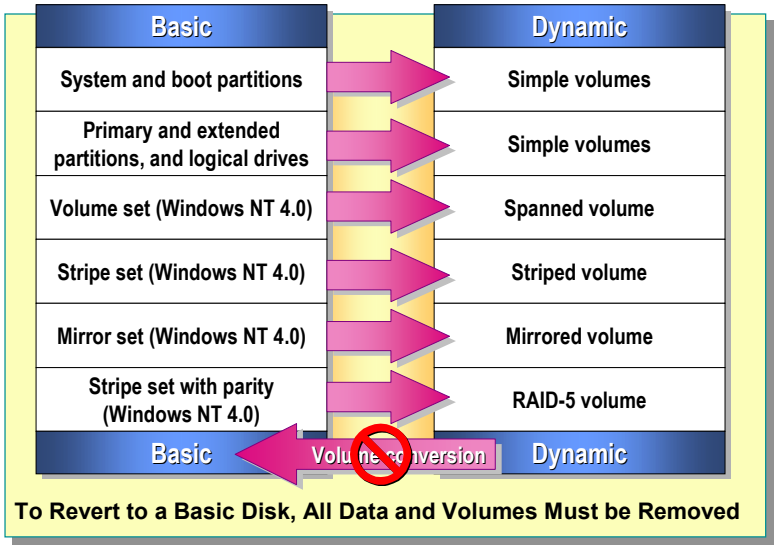
When you set up a new disk, by default, Windows 2000 creates it as a basic disk. To use a dynamic disk, you must upgrade from a basic disk to a dynamic disk. Once the upgrade process has been completed, you can create a wide range of dynamic volumes. There is no limit to the number of volumes that you can create using dynamic disks. In addition, you can also extend volumes over multiple disks. These capabilities provide you with greater control and allow you to prevent data loss due to hardware failure.

If you choose to upgrade from a basic disk to a dynamic disk, consider which volume type best suits your organization's needs for efficient use of disk space and performance.

Upgrading from a Basic to a Dynamic Disk

Topic Objective
To illustrate the upgrade from basic disk partitions and various Windows NT 4.0 sets to dynamic storage.

Lead-in
A primary partition on a basic disk becomes a simple volume when you upgrade the disk to use dynamic storage.



**********ILLEGAL FOR NON-TRAINER USE**********

Upgrade a disk from basic storage to dynamic storage at any time without losing data.

Delivery Tip
Show students Disk Management and its menu options when you right-click on a basic disk. You also may want to direct them to look at Disk Management on their own. Do not upgrade at this time.

Tip
Administrators should always backup a disk before they upgrade it to a dynamic disk.

To upgrade from a basic disk to a dynamic disk, open Disk Management, right-click the basic disk that you want to upgrade, and then click **Upgrade to Dynamic Disk**. Select the disk you want to upgrade in the **Upgrade to Dynamic Disk** dialog box. If the disk that you are upgrading contains the boot or system partition, or an active paging file, you must restart the computer to complete the upgrade process.

Tip You should always back up the data on a disk before you upgrade the storage type from basic to dynamic to ensure that you do not lose data if there are problems.

Upgrade Results

When you upgrade a basic disk to a dynamic disk, any existing partitions on the basic disk become volumes. The following table describes the results of an upgrade.

Mention the upgrade results to the students.

Basic disk organization (before upgrade)	Dynamic disk organization (after upgrade)
System and boot partitions	Simple volumes
Primary partition	Simple volume
Extended partition	Any logical drives become simple volumes and any free space becomes unallocated space

(continued)

Basic disk organization (before upgrade)	Dynamic disk organization (after upgrade)
Volume set from earlier Windows NT versions (no longer available in Windows 2000)	Spanned volume
Stripe set from earlier Windows NT versions (no longer available in Windows 2000)	Striped volume
Mirror set from earlier Windows NT versions (no longer available in Windows 2000)	Mirrored volume
Stripe set with parity from earlier Windows NT versions (no longer available in Windows 2000)	RAID-5 volume

Key Points
To successfully upgrade a basic disk to a dynamic disk, there must be at least 1 MB of unallocated space on the basic disk.

Make sure that students understand that when they revert to a basic disk from a dynamic disk, they lose all the data on the disk.

Important To upgrade a disk successfully, the disk must contain at least 1 MB of unallocated space to store disk configuration information.

Reverting to a Basic Disk

You cannot convert a dynamic disk back to a basic disk and maintain the disk structure and data you had on the dynamic disk. You can revert a dynamic disk back to a basic disk, which is setting up a clean basic disk without the data that was on the dynamic disk. Delete the data and volumes on the dynamic disk, and then recreate a basic partition from the new unallocated space.

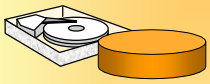
To revert a dynamic disk to a basic disk, after you delete all data and volumes on the dynamic disk, open Disk Management, right-click the dynamic disk that you want to revert, and then click **Revert To Basic Disk**.

Creating Simple Volumes

Topic Objective
To list features of simple volumes.

Lead-in
A simple volume is contained on a single disk.

A Simple Volume:



- **Contains Space on Single Disk**
- **Has less Restrictions than a Basic Disk Partition**
- **Can Use the NTFS, FAT, or FAT32 File Systems**
- **Can Be Mirrored to Provide Fault Tolerance**
- **Is Created by Using the Create Volume Wizard**

**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Although it appears similar to a basic disk partition, a simple volume does not have the size limits that a partition has.

A simple volume contains disk space on a single disk and is created from unallocated space on dynamic disk. Although a simple volume may seem similar to a partition, a simple volume does not have the size limits that a partition has, nor is there a restriction on the number of volumes that you can create on a single disk. In addition, you can add additional space to, or extend, a simple volume after you create it.

A simple volume uses the NTFS file system, file allocation table (FAT), or FAT32 file system formats. However, you can extend a simple volume only if it is formatted with NTFS.

A simple volume is not fault-tolerant; however, you can create a mirror of a simple volume, or a mirrored volume, to provide fault tolerance. For more information about mirrored and RAID-5 volumes, see module 13, "Implementing Disaster Protection," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Delivery Tip
Demonstrate the steps of this process on the instructor computer as you review the process. This process will require restarting the instructor computer unless a dynamic volume has already been created on the computer.

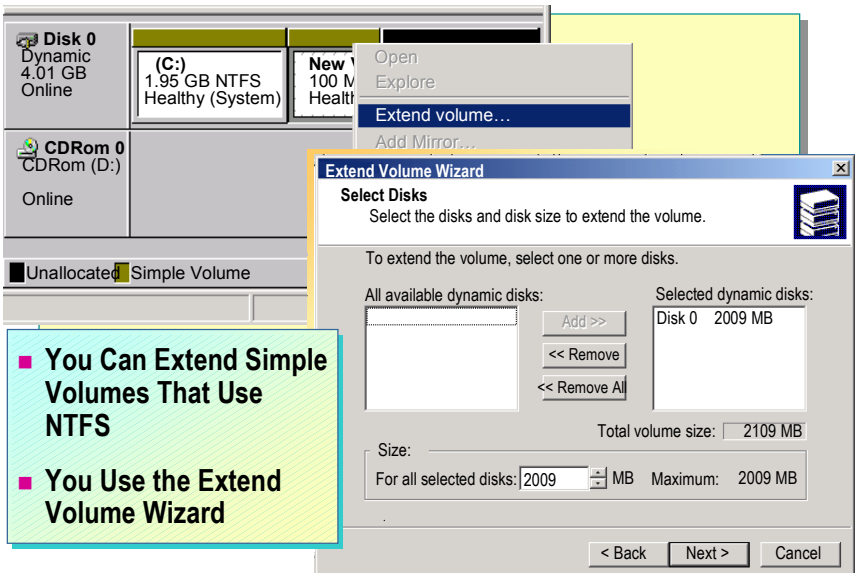
To create a simple volume, perform the following steps:

1. Open Disk Management, right-click the unallocated space on the dynamic disk where you want to create the simple volume, and then click **Create Volume**.
2. In the Create Volume wizard, click **Next**.
3. Click **Simple Volume**, and then follow the on-screen instructions.

Extending Simple Volumes

Topic Objective
To show how to extend simple volumes.

Lead-in
A simple volume can be extended to include unallocated space on the same disk.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Emphasize that a simple volume can be extended if it is formatted with NTFS.

A volume can only be extended if it was originally created on a dynamic disk and not upgraded from a partition on a basic disk.

You can extend any simple volume that is formatted with NTFS to include either contiguous or noncontiguous unallocated space from any dynamic disk. This means you can add additional hard drive space to an existing volume rather than reconfiguring all of your hard drives. Exceptions include any volume that contains system or startup files or an active paging file.

To extend a simple volume, in Disk Management, right-click the simple volume that you want to extend, click **Extend Volume**, and then follow the on-screen instructions.

Important Extending a volume can only be done on a volume that was originally created on a dynamic disk. If the volume was created first on a basic then converted to dynamic it cannot be extended.

Lab A: Working with Dynamic Disks

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will upgrade a disk, create a simple volume, and extend a volume.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Upgrade a basic disk to a dynamic disk.
- Create a new volume.
- Extend a simple volume.

Prerequisites

Before working on this lab, you must have:

- Knowledge of basic and dynamic disks.
- Knowledge of storage types on basic and dynamic disks.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server.
- A single hard disk partitioned with:
  - Drive C as the primary partition.
  - A minimum of 2 GB of unallocated disk space.

Estimated time to complete this lab: 30 minutes

Exercise 1
Upgrading a Disk

Scenario

You have a corporate policy mandating that all disks be configured as dynamic disks because some servers in your corporation implement software fault tolerance. In order to comply with corporate policy, you must convert the hard disks from basic disks to dynamic disks.

Goal

In this exercise, you will use Disk Management to upgrade a basic disk to a dynamic disk.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and upgrade disk 0, a basic disk, to a dynamic disk.	**a.** Log on using the following information: User name: **Student***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Computer Management from the **Administrative Tools** menu. **c.** In the console tree, under **Storage**, click **Disk Management**. *A message appears, indicating that you do not have the access rights to the service.* **d.** Click **OK**, and then close Computer Management. **e.** Click **Start**, point to **Programs**, point to **Administrative Tools**, right-click **Computer Management**, and then click **Run as**. **f.** In the **Run As Other User** dialog box, verify that **Run the program as the following user** is selected. **g.** In the **User name** box, type **Admin***x* (where *x* is your assigned student number). **h.** In the **Password** box, type **domain** **i.** In the **Domain** box, type **nwtraders.msft** and then click **OK**. **j.** In Computer Management, in the console tree, under **Storage**, click **Disk Management**.

What is the storage type of disk 0?

Basic.

Tasks	Detailed Steps
Is drive C a primary partition or a logical drive in an extended partition? **Primary partition.**	
1. (*continued*)	**k.** In the lower-right pane of Computer Management, right-click **Disk 0**, and then click **Upgrade to Dynamic Disk**. **l.** In the **Upgrade to Dynamic Disk** dialog box, verify that **Disk 0** is the only disk selected for upgrade, and then click **OK**. **m.** In the **Disks to Upgrade** dialog box, click **Upgrade**. *The **Disk Management** dialog box appears, indicating that you will not be able to start previous versions of Windows from any volumes on this disk.* **n.** Click **Yes**. *The **Upgrade Disks** dialog box appears, warning that the file system will be forcibly dismounted.* **o.** Click **Yes**. *The **Confirm** message box appears, informing you that you must restart the computer to complete the upgrade process.* **p.** Click **OK** to restart your computer.
2. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and confirm the upgrade of disk 0 to dynamic.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** *The **System Settings Change** dialog box appears, prompting you to restart your computer.* **b.** Click **No**. **c.** Open Computer Management from the **Administrative Tools** menu. **d.** In the console tree, under **Storage**, click **Disk Management**.
What is the storage type of Disk 0? **Dynamic.**	

Tasks	Detailed Steps
Is drive C an extended partition in a logical drive? **No. Drive C is a simple volume.**	
What has changed? **Drive 0 has been changed from a basic disk to a dynamic disk. Drive C has been changed from a primary partition to a simple volume.**	
2. (*continued*)	**e.** Leave Computer Management open.

Exercise 2
Creating a Simple Volume

Scenario

You need to create a new volume to store employee telephone extension numbers and office numbers. To do this, you will create a new volume to store the information.

Goal

In this exercise, you will create a simple 100 MB volume labeled Data.

Tasks	Detailed Steps
1. Create a simple volume with the following information: Size: 100 Volume Label: Data	**a.** In the lower-right pane of Computer Management, right-click the unallocated space on Disk 0, and then click **Create Volume**. **b.** On the **Welcome to the Create Volume Wizard** page, click **Next**. *The **Select Volume Type** page appears; notice that **Simple volume** is the only available option.* **c.** Click **Next**. **d.** On the **Select Disks** page, under **Size**, in the **For selected disk** box, type **100** and then click **Next**. **e.** On the **Assign Drive Letter or Path** page, verify that **Assign a drive letter** is selected, verify that **F** appears as the drive letter, and then click **Next**. **f.** On the **Format Volume** page, in the **Volume label** box, type **Data**, select the **Perform a Quick Format** check box, and then click **Next**. **g.** Click **Finish**. *The new volume is created and formatted.*
In the upper-right pane of Computer Management, what is the reported capacity of the volume you just created? **100 MB.**	
1. (*continued*)	**h.** Leave Computer Management open.

Exercise 3
Extending a Volume

Scenario

Your company acquired another company and the number of employees doubled. The volume you created to store employee information needs to be expanded to accommodate the data that must be added.

Goal

In this exercise, you will use Disk Management to extend an existing volume.

Tasks	Detailed Steps
1. Extend a volume using the following information: Volume to Extend: Data increase by 25 MB	**a.** In the lower-right pane of Computer Management, right-click **Data (F:)**, and then click **Extend Volume**. **b.** On the **Welcome to the Extend Volume Wizard** page, click **Next**. **c.** On the **Select Disks** page, under **Size**, in the **For all selected disks** box, type **25** and then click **Next**. **d.** Click **Finish**. *Drive F is extended to include an additional 25 MB of disk space.*
In the upper-right pane of Computer Management, what is the reported capacity of the volume you just extended? **124 MB.**	
Did you have to restart the computer to extend the volume? **No. The system is able to use the additional space without restarting the system.**	
1. (*continued*)	**e.** Close Computer Management, and then log off.

◆ Performing Common Disk Management Tasks

Topic Objective
To introduce some common disk management tasks in Windows 2000.

Lead-in
In addition to creating dynamic volumes, you use Disk Management to perform disk management tasks such as creating partitions and changing drive letters.

- **Repairing and Deleting Partitions and Volumes**
- **Adding Disks**
- **Managing Drive Letters and Paths**
- **Managing Disks Remotely**
- **Defragmenting Partitions**

**********ILLEGAL FOR NON-TRAINER USE**********

Disk management tasks are a set of tasks that you perform by using Disk Management. Disk Management provides a central location for viewing disk information and performing management tasks, such as repairing and deleting partitions and volumes. Some of the other disk management tasks that you may need to perform to meet your changing storage demands include the following:

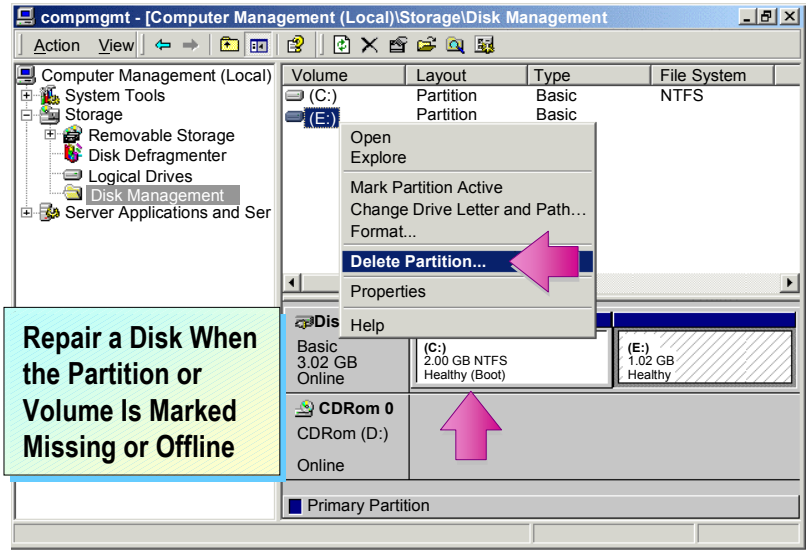
- Adding hard disks
- Changing the drive letter and path
- Managing disks remotely
- Defragmenting partitions

You will find these tasks to be a routine part of administration as you organize users' access to data and maintain computers.

Repairing and Deleting Partitions and Volumes

Topic Objective
To show the interface used to repair and delete partitions and volumes

Lead-in
Deleting and repairing partitions and volumes is one of the most common administrative tasks.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Show the interface for repairing and deleting partitions and volumes.

From time to time, you may encounter a failed disk or volume that needs to be repaired or deleted. Disk Management allows you to find disk storage problems quickly. You can view the status of a disk or volume, repair a disk if it is possible, or delete the disk if it cannot be repaired.

Disk Status

Mention to students that the actions for the disk status are covered later in the module.

View the status of a disk under the Status column in Disk Management. The following table reviews the different types of disk status and the actions to perform for each status.

Disk status	Action
Healthy (for volumes) or Online (for disks)	No action required
Failed: Incomplete Volume	Import remaining disks in set
Foreign	Import foreign disk
Failed Redundancy	Import remaining disk in set

Repairing Partitions and Volumes

If a disk goes offline due to corruption, power interruption, or disconnection, it can cause problems with the basic disk partitions and dynamic disk volumes. If this occurs, you may need to repair the partitions or volume. To repair a partition or volume, open Disk Management, right-click the partition or volume that is marked Missing or Offline, and then click **Reactivate Disk**. The disk should be marked **Online** after the disk is reactivated.

Deleting Partitions and Volumes

You can delete any basic disk partitions or dynamic disk volumes except the system partition or volume, boot partition or volume, or any partition or volume that contains an active paging file. In addition, Windows 2000 requires that you delete all of the logical drives or other volumes before you delete the extended partition or volume.

To delete a partition, open Disk Management, right-click the partition that you want to delete, and then click **Delete Partition**.

To delete a volume, open Disk Management, right-click the volume that you want to delete, and then click **Delete Volume**.

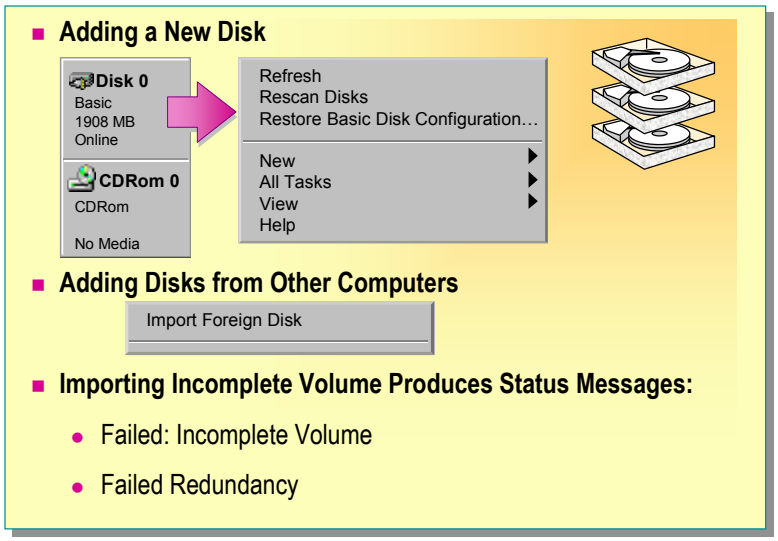
Key Point
An administrator cannot recover deleted partitions or volumes. All the data on the deleted partition or volume is lost.

Important You cannot recover deleted partitions or volumes and all data on the deleted partition or volume is lost.

Adding Disks

Topic Objective
To illustrate how to add new disks to a computer.

Lead-in
You can add new disks to a computer or move a disk from one computer to another.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
With the students, discuss reasons for adding a disk or moving a disk from one computer to another.

Ensure the students know what hot swapping means.

Key Points
If a computer supports hot swapping, the administrator does not need to shut down and restart the computer before the new disk is recognized.
An administrator should rescan a new disk that is added on a computer that supports hot swapping.

Add new disks to a computer or move a disk or group of disks from one computer to another to increase your disk storage. For example, if you are running out of network storage space for user data, you can add a hard disk.

Adding a New Disk

To add a new hard disk to a computer that supports *hot swapping* (the ability to add or remove disks without shutting down the computer), install or attach the new hard disk. Then, in Disk Management, on the **Action** menu, click **Rescan Disks**. You must use the **Rescan Disks** command every time that you add disks to a computer that supports hot swapping so that Disk Management can rescan to find and register the disk.

Note If the computer to which you are adding the disk does not support hot swapping, shut down the computer, add the disks, and then restart the computer. The new disk appears in Disk Management.

If your computer supports hot swapping, it should not be necessary to restart the computer when you add a new hard disk. However, if Disk Management is unable to detect the new disk after you click **Rescan Disks**, you will need to restart the computer.

Delivery Tip
Prompt students to suggest reasons for possible circumstances for when you would add disks from other computers.

Adding Disks from Other Computers

If you need to transfer a disk from one computer to another, in most cases, Windows 2000 automatically imports a disk that contains data. However, if Disk Manager indicates the status of a new disk as **Foreign**, you must right-click the representation of the disk, and then click **Import Foreign Disk**. The Import wizard appears to guide you through the import process.

If you move a dynamic disk from one computer to another, because dynamic storage is only supported by Windows 2000, you can only use dynamic disks on a computer running Windows 2000.

The newly imported disks are grouped according to the computer name from which they were moved. After you add the disk to the computer, when you open Disk Management, the new disk is displayed and has a status of **Foreign**. You right-click the disk, click **Import foreign disks**, and then in the **Import foreign disk** dialog box, select the appropriate disk set. The dialog box then displays any defined partitions or volumes on the added disk. Click **OK** to complete the process.

Note If you are adding multiple disks from another computer and the status of any of the disks appears as **Foreign**, right-click any of the disks, and then click **Import Foreign Disk**.

When you move a dynamic disk to your computer from another computer running Windows 2000, you can see and use any existing volumes on that disk.

Importing Incomplete Volumes

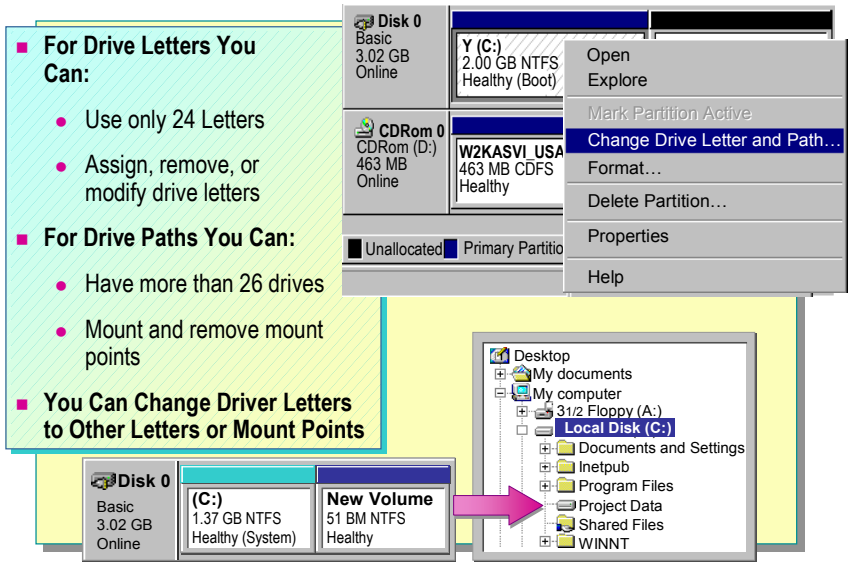
There are different ways that volumes are imported incompletely. For each way there is a different status message:

- If the status of an imported volume appears as **Failed: Incomplete Volume**, a disk that contains part of a spanned or a striped volume has been imported but the remaining portions of the spanned or striped volume have not been imported. This also applies to RAID-5 volumes if two or more disks were not imported. You must import the remaining disks to complete the volume. You will be unable to access the volume until the remaining disks are imported.
- If the status of an imported volume appears as Failed Redundancy, a mirror volume or a RAID-5 volume has been imported, but one or more volumes that contain the remaining portions of the mirror or RAID-5 volume have not been imported. You can gain access to the data on the volume, but redundancy is lost. You must import the remaining disks to complete the volume and restore the redundancy.

Managing Drive Letters and Paths

Topic Objective
To show how to manage drive paths and drive letters.

Lead-in
You can assign static drive letters to partitions, volumes, and removable devices.



**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 allows the static, or permanent, assignment of drive letters to partitions, volumes, and CD-ROM drives and to mount a drive path to a folder, which is the mount point for the volume. Use drive letters and mount points on basic and dynamic disks.

Managing Drive Letters

You can use up to 24 drive letters, from C through Z. Drive letters A and B are typically reserved for disk drives. However, if you have only one disk drive, you can override this setting and assign the letter B to a partition, volume, or CD-ROM drive. When you add a new hard disk to an existing computer, it does not affect previously assigned drive letters because it is automatically assigned a letter that is not currently in use.

Tip It is often convenient to assign drive letters to removable devices in such a way that the removable devices are listed after the permanent partitions and volumes on the computer.

To assign, change, or remove a drive letter, open Disk Management, right-click a partition, logical drive, or volume, and then click **Change Drive Letter and Path**. In the **Drive Letter and Paths** dialog box, do one of the following:

- Assign a drive letter. To assign a drive letter, click **Add**, click a drive letter, and then click **OK**.
- Remove a drive letter. To remove a drive letter, click the drive letter, and then click **Remove**.
- Modify a drive letter. To modify a drive letter, click the drive letter that you want to modify, and then click **Modify**. Click the drive letter that you want to use, and then click **OK**.

Key Point
Mounting a local disk to an empty folder on a local NTFS partition or volume is a new feature of Windows 2000. This removes the 26-drive letter limit on mounting drives for users and allows you to mount a disk using a more logical naming scheme.

Managing Drive Paths

As a new feature of Windows 2000, you can use Disk Management to mount a local disk to any empty folder on a local NTFS volume rather than to a drive letter. This is a similar to creating a shortcut that points to a disk partition or volume. Because mounted drives are not subject to the 26-drive letter limit, use them to exceed the limit.

In addition, mounting a drive to a folder allows you to use an intuitive name for the folder, such as Project Data. Users would then save their documents in the Project Data folder rather than to a drive letter. Windows 2000 ensures that drive paths retain their association to the drive so that you can add or rearrange storage devices without the drive path failing.

When you mount a local disk to an empty folder on a local partition or volume that is formatted with NTFS, Windows 2000 assigns a drive path, rather than a drive letter, to the disk.

Delivery Tip
Demonstrate this process to students by creating a folder on an existing partition or volume. Browse to the folder rather than typing the path to assist students in visualizing the connection.

Creating a New Mount Point

To create a new drive path, click **Add**, and then type the path to the empty folder or click **Browse** to locate it. When the correct path is entered, click **OK**.

If you are administering a local computer, you can browse folders on that computer to locate the folder to which you want to mount the disk. If you are administering a remote computer, browsing is disabled and you must type the path to an existing folder.

Removing a Drive Path for Mount Point

You cannot modify a drive path. If you need to change a drive path, you must remove it and then create a new drive path with the new information. You can view all drive paths in Disk Management by clicking **View**, and then clicking **All Drive Paths**.

To remove a drive path, click the drive path, and then click **Remove**.

Changing Drive Letters to Other Letters or Mount Points

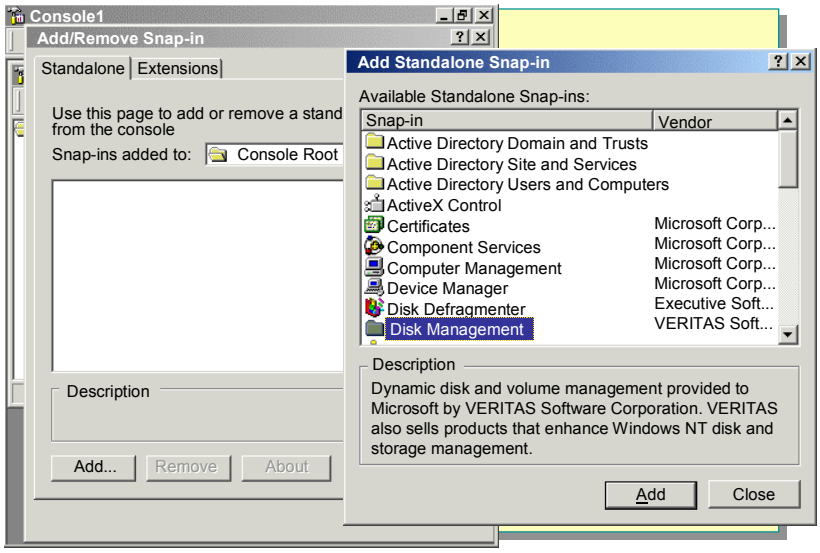
You can change a drive letter to another driver letter if you want to reorganize your drive letters or to a mount point if you want to free up drive letters. You do not lose data. To change a drive letter to a different drive letter or to a mount point, open Disk Management, right-click the appropriate partition or volume, and then click **Change Drive Letter and Path**. In the **Drive Letter and Paths** dialog box, do one of the following:

- If you are changing the drive to another drive letter, click **Edit**, and then select the new drive letter.
- If you change a drive letter to a mount point, you must first remove the drive letter, and then add a new mount point.

Managing Disks Remotely

Topic Objective
To show how to connect to disks remotely.

Lead-in
Remote management is a key feature of Windows 2000.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Ask students to brainstorm possible reasons for managing disks remotely.

Then demonstrate by remotely managing the disk on a student's computer.

In a Windows 2000 network, you can manage the hard disks on one computer remotely from another computer, if for example you want to manage all client computers from your computer. To manage hard disks remotely, both the computer you are connecting from and the computer you are connecting to must be members of the same domain or workgroup, or be within a trusted domain. In addition, the user account you log on with must be a member of the Administrators or Server Operators group on the remote computer.

To manage disks remotely, perform the following steps:

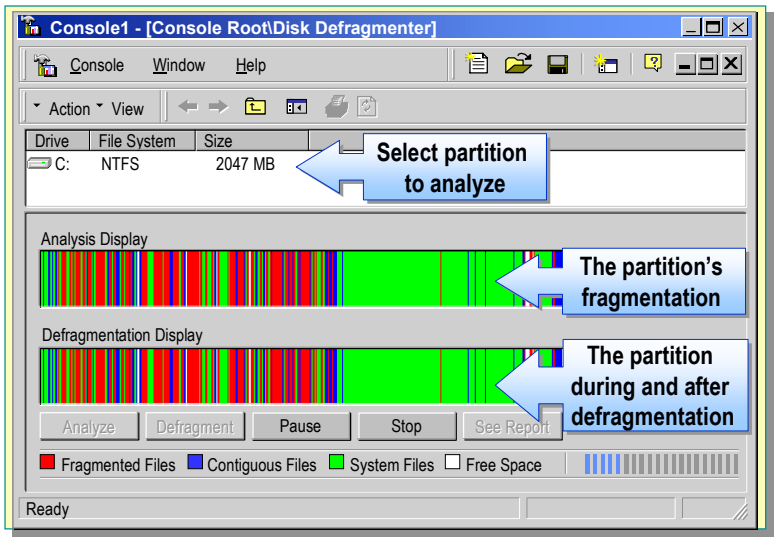
1. On the **Start** menu, click **Run**, type **mmc** and then click **OK**. This sets up an MMC console that you can configure to use for remote management of a hard disk.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the list of snap-ins, click **Disk Management**, and then click **Add**.

   Disk Management on your local computer only allows you to manage local disks. If you want to manage disks on another computer, you must, you must create a new console with snap-ins to manage a hard disk on a remote computer.
4. Click **Another computer**, type the name of the remote computer, and then click **Finish**.

Defragmenting Partitions

Topic Objective
To present the Disk Defragmenter interface.

Lead-in
You use Disk Defragmenter to defragment partitions.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Show students Disk Defragmenter for the hard disk on your computer. You also may want to direct them to look at Disk Defragmenter on their own computers.

Key Point
Fragmentation of files decreases system performance because the computer must read data files from various locations.

Windows 2000 attempts to save files or folders in locations on the hard disk that are large enough to accommodate the entire file or folder. If there is no suitable location, Windows 2000 saves fragments of the file or folder in several locations. This fragmentation of files on the hard disk decreases system performance because the computer must read file data from various locations on the hard disk. You can use the Windows 2000 Disk Defragmenter to locate and rearrange the fragments into a single space on the hard disk.

The Disk Defragmenter window has three panes that provide the following information.

- The upper pane lists the partitions you can select to analyze and defragment.
- The middle pane, called the Analysis Display, provides a graphical representation of how fragmented the selected partition is at a particular point. That point is when you choose to analyze the hard disk.
- The lowest pane, called the Defragmentation Display, provides a graphical representation of the partition during and after defragmentation.

To start Disk Defragmenter, click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Defragmenter**. To analyze and defragment a partition with Disk Defragmenter, select the options that are described in the following table.

Option	Description
Analyze	Click this button to analyze the disk for fragmentation. After the analysis, Analysis Display provides a graphic representation of how fragmented the partition is.
Defragment	Click this button to defragment the disk. After defragmentation, Defragmentation Display provides a graphic representation of the defragmented partition.

By comparing Analysis Display to Defragmentation Display, you can quickly see the improvement in the partition after defragmentation.

Note Although you can use a computer while its hard disk is undergoing defragmentation, it is not recommended as it causes a serious deterioration in disk performance and significantly increases the time it takes to perform the defragmentation.

Lab B: Creating and Mounting a New Volume

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will create and mount a new volume.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a new volume.
- Mount a simple volume.

Prerequisites

Before working on this lab, you must have:

- Knowledge of basic and dynamic disks.
- Knowledge of storage types on basic and dynamic disks.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server.
- A single hard disk partitioned with:
  - Drive C as the primary partition.
  - A minimum of 2 GB of unallocated disk space.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating and Mounting a New Volume

Scenario

You have unused disk space on an existing hard disk and want to be able to use it, but you also want it to be part of the C partition you have already created. To do this, you must format the volume and create a mount point on the C volume.

Goal

In this exercise, you will create a new simple volume. You will then mount the new volume to an existing empty folder on another volume.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and create a new simple volume. • Mount folder: C:\ Mount	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Computer Management from the **Administrative Tools** menu. **c.** In the console tree, under **Storage**, click **Disk Management**. **d.** In the lower-right pane of Computer Management, right-click the unallocated space on Disk 0, and then click **Create Volume**. **e.** On the **Welcome to the Create Volume Wizard** page, click **Next**. **f.** On the **Select Volume Type** page, click **Next**. **g.** On the **Select Disks** page, under **Size**, in the **For selected disks** box, type **25** and then click **Next**. **h.** On the **Assign Drive Letter or Path** page, click **Mount this volume at an empty folder that supports drive paths**, and then click **Browse**. **i.** In the **Browse for Drive Path** dialog box, expand **C:**, click **New Folder**, name the folder Mount, press ENTER, click **OK**, and then click **Next**. **j.** On the **Format Volume** page, select the **Perform a Quick Format** check box, click **Next**, and then click **Finish**. *The new volume is created, formatted, and mounted to the C:\Mount folder.* **k.** Close Computer Management.
2. Examine the new volume.	**a.** Open Windows Explorer. **b.** Under **My Computer**, click **Local Disk (C:)**. *Notice that the icon for the Mount folder is different than the other folders listed.* **c.** Open the **Properties** dialog box for the Mount folder. *The **Mount Properties** dialog box appears.*

Tasks	Detailed Steps
What type of folder is C:\Mount? **Mounted volume.**	
What is the target for the mount point called? **New Volume.**	
2. (*continued*)	**d.** Click **OK** to close the **Mount Properties** dialog box. **e.** Create a new text document in Mount. **f.** Close Windows Explorer. **g.** At a command prompt, change to the root folder of drive C if necessary, type **dir** and then press ENTER. *Notice that Mount appears as <JUNCTION>, which indicates that this is a mount point.*
How much free space does the **dir** command report? **Answers will vary.**	
2. (*continued*)	**h.** At the command prompt, change to C:\Mount, type **dir** and then press ENTER.
How much free space does the **dir** command report? **Answers will vary.**	

Tasks	Detailed Steps
Why is there a difference between the free space reported for drive C and the free space reported for C:\Mount? **The amount of free space reported for C:\Mount is the amount of free space available on the mounted volume.**	
2. (*continued*)	**i.** Close any open windows, and then log off.

Best Practices

Topic Objective
To introduce issues that can occur during disk configuration and management.

Lead-in
At times, you need to resolve issues that you encounter when configuring or managing disks. Proactive management is the best way to address problems before they occur.

**********ILLEGAL FOR NON-TRAINER USE**********

The following table lists the some best practices to consider for disk configuration and disk storage issues.

Best practice	Rationale
Always keep a minimum of 1 MB free on each basic disk.	This will enable you to convert to dynamic storage if you so choose. The 1 MB is used to store disk configuration information.
Use NTFS for the greatest flexibility in disk storage methods.	NTFS allows you the highest security protection and to fully use all aspects of dynamic storage.
Create a mirrored volume for your disk containing the startup files.	With some configuration, this will enable your server to continue functioning in the event of a startup disk failure.
Implement a RAID-5 volume to protect your data from a single disk failure.	This allows your data to be protected and to allow your users continued access to data in the event of a single disk failure.
Keep written records of your disk configuration information.	On larger servers and in environments that use fault tolerance, disk configuration can be complex. Recreating drive configuration information and restoring data in the event of a disk failure will be easier with records of existing configuration information.
Use Disk Defragmenter regularly to maximize data access.	Data access is slowed over time by fragmentation of files. By regularly using Disk Defragmenter, you can maximize user access and help prevent a decrease in performance.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Windows 2000 Disk Types
- Creating Partitions on a Basic Disk
- Creating Volumes on a Dynamic Disk
- Performing Common Disk Management Tasks
- Best Practices

**********ILLEGAL FOR NON-TRAINER USE**********

1. You install a new 10-gigabyte (GB) hard disk that you want to divide into five equal 2-GB sections. What are your options?

   You can leave the disk as a basic disk, and then create a combination of primary partitions (up to three) and logical drives on an extended partition, or you can upgrade the disk to a dynamic disk and create five 2-GB simple volumes.

2. You are trying to create a striped volume on your computer running Windows 2000 to improve performance. You confirm that you have enough unallocated disk space on two disks in your computer, but when you right-click an area of unallocated space on one of the disks, your only option is to create a partition. What is the problem and how would you resolve it?

   You can create striped volumes on dynamic disks only. The option to create a partition rather than a volume indicates that the disk that you are trying to use is a basic disk. You will need to upgrade all of the disks that you want to use in your striped volume to dynamic disks.

3. You add a new disk to your computer and attempt to extend an existing simple volume to include the unallocated space on the new disk, but the option to extend the volume is not available. What is the problem and how would you resolve it?

   The existing volume is not formatted with NTFS. You can extend only volumes that are formatted with NTFS. You should back up any data on the existing volume, convert it to NTFS, and then extend the volume.

4. You want to use a folder on a local partition to mount the inventory database records for staff from an existing partition. How would you implement this?

   Create an empty folder on a local partition named Inventory. Right-click on the existing partition, logical disk, or volume where the inventory database is stored, and then in Disk Management remove the drive letter for the existing partition, and add the mount point for the folder.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 13: Implementing Disaster Protection

Contents

Overview	1
Introduction to Disaster Protection	2
Configuring an Uninterruptible Power Supply	4
Implementing Fault Tolerance by Using RAID	6
Lab A: Implementing Fault-Tolerant Volumes	19
Backing Up and Restoring Data	20
Lab B: Backing Up and Restoring System State Data	30
Using Disaster Recovery Tools	34
Review	41

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
55 Minutes

Labs:
35 Minutes

This module provides students with the knowledge and skills necessary to implement fault tolerance and disaster protection techniques in Microsoft® Windows® 2000 Professional and Server. The module presents information on Windows 2000 fault-tolerant volumes, advanced startup options, the Recovery Console, and the enhanced Backup utility.

At the end of this module, students will be able to:

- Describe the purpose of disaster protection.
- Configure an uninterruptible power supply.
- Provide data redundancy with fault-tolerant volumes.
- Back up and restore data in Windows 2000.
- Recover from a computer disaster.

Materials and Preparation

This section provides you with the required materials and preparation tasks needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2152B_13.ppt.
- Lab A, "Implementing Fault-Tolerant Volumes," under **Lab Simulations** on the Student Materials compact disc.

Preparation Tasks

To prepare for this module, you should:

- Read all the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for a lab.

Lab A: Implementing Fault-Tolerant Volumes

► **To prepare for the lab**

- Lab A is a simulation that can run on any computer running Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.

Lab B: Backing Up and Restoring System State Data.

► **To prepare for the lab**

- Students must have completed module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Module Strategy

Use the following strategy to present this module:

- Introduction to Disaster Protection

  In this topic, provide a conceptual overview of disaster protection and recovery. Define disaster recovery, and then explain fault tolerance and data redundancy.

- Configuring an Uninterruptible Power Supply

  In this topic, describe the process of configuring an uninterruptible power supply (UPS) in Windows 2000. Describe how to display the **UPS Configuration** dialog box, and then explain the configuration options available.

- Implementing Fault Tolerance by Using RAID

  In this topic, describe Windows 2000 support for fault-tolerant volumes. Explain the process for implementing mirrored volumes and RAID-5 (redundant array of independent disks) volumes from unallocated disk space, and then describe how to mirror an existing volume. Complete the topic by describing the three methods for recovering each type of fault-tolerant volume.

- Backing Up and Restoring Data

  In this topic, describe the Backup utility included in Windows 2000. Discuss backing up and restoring files and folders. Explain the five types of backup and discuss the examples of when to use each type of backup. Explain the components of the system state data on various computers. Then, explain how to back up the system state data and how to schedule a backup. Complete the topic by describing how to restore files and folders.

- Using Disaster Recovery Tools

  In this topic, describe strategies for recovering from a computer disaster. Begin by describing how to start a computer by using advanced startup options, and continue by explaining how to recover a computer by using the Recovery Console. Finish the module by discussing how to create an Emergency Repair Disk (ERD), and then explain the emergency repair process.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

To prepare student computers for the labs in this module, complete module 1, "Installing or Upgrading to Microsoft Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration change:

- Lab B creates a backup of the system state data on the root of drive C called Backup.bkf.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about techniques in Windows 2000 for preventing and recovering from computer disasters.

- **Introduction to Disaster Protection**
- **Configuring an Uninterruptible Power Supply**
- **Implementing Fault Tolerance by Using RAID**
- **Backing Up and Restoring Data**
- **Using Disaster Recovery Tools**

**********ILLEGAL FOR NON-TRAINER USE**********

This module will help you identify computer disasters and use the features in Microsoft® Windows® 2000 to prevent disasters and recover from disasters after they occur. Understanding these Windows 2000 features is essential to developing and implementing an effective disaster protection and recovery plan.

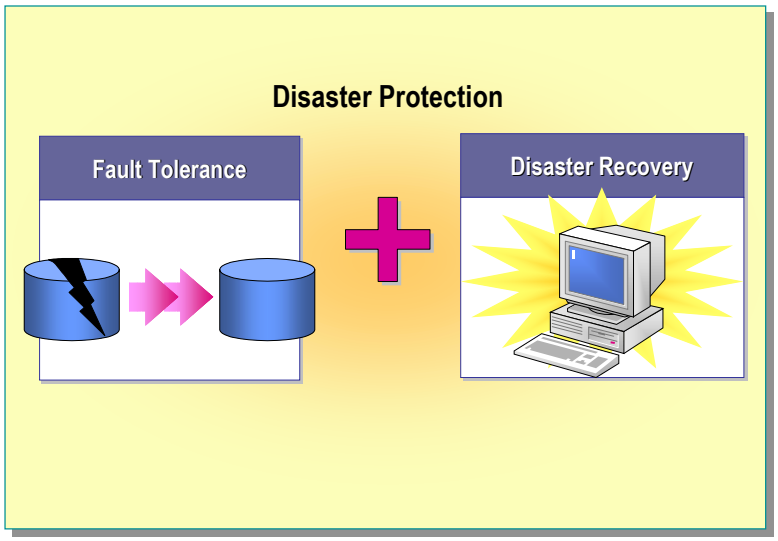
At the end of this module, you will be able to:

- Describe the purpose of disaster protection and recovery.
- Configure an uninterruptible power supply.
- Provide data redundancy with fault-tolerant volumes.
- Backup and restore data in Windows 2000.
- Use disaster recovery tools.

Introduction to Disaster Protection

Topic Objective
To illustrate that disaster protection is achieved though a combination of fault tolerance and disaster recovery.

Lead-in
You achieve disaster protection through a combination of fault tolerance and disaster recovery.



**********ILLEGAL FOR NON-TRAINER USE**********

A *computer disaster* is any event that renders a computer unable to start. Examples of a computer disaster include:

- Corruption of the boot block stored on a computer's system device (the disk containing the files necessary to start the computer).
- The deletion of one or more operating system files.
- Failure of a computer's physical system device, leaving the rest of the computer intact.
- Physical destruction of the computer itself, such as in the case of a fire.

Disaster protection is a term that describes the efforts by support professionals to prevent computer disasters and to minimize downtime in the event of system failure. Implement disaster protection on your computers through a combination of fault tolerance and disaster recovery techniques.

Fault Tolerance

Fault tolerance is the ability of a computer or operating system to respond to a catastrophic event, such as a power outage or hardware failure, so that no data is lost and that work in progress is not corrupted. Fully fault-tolerant systems use redundant disk controllers and power supplies in addition to as fault-tolerant disk subsystems. In addition, fault-tolerant systems often include an uninterruptible power supply (UPS) to safeguard against local power failure.

Caution Although the data is available and current in a fault-tolerant system, you should still make backup copies to protect the information on hard disks from erroneous deletions, fire, theft, or other physical disasters. Disk fault tolerance is not an alternative to a backup strategy with offsite storage, which is the best insurance for recovering lost or damaged data.

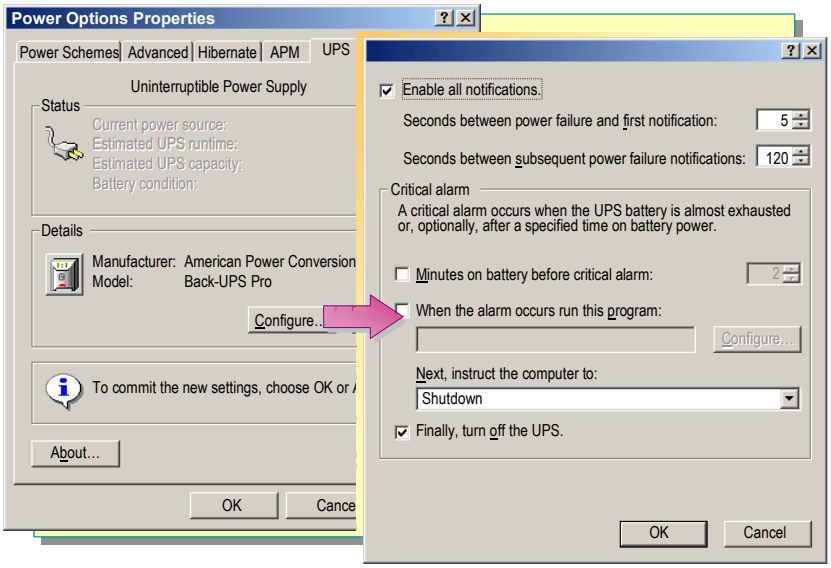
Disaster Recovery

Disaster recovery is the process of restoring a computer after a computer disaster occurs so that users can log on and gain access to system resources. Ideally, disaster recovery techniques restore the damaged computers to the state they were in prior to the disaster.

Configuring an Uninterruptible Power Supply

Topic Objective
To illustrate the interface for configuring a UPS.

Lead-in
You can use a UPS to provide power in the event of a local power outage.



**********ILLEGAL FOR NON-TRAINER USE**********

One common type of computer disaster is the loss of local power. Power loss can result in damaged or lost data on a server or client computer. While companies usually protect servers against this type of disaster, you should also consider providing protection for client computers against power loss, depending on the reliability of your local utility power supply. This provides added security against accidental data loss during a power interruption.

An *uninterruptible power supply* provides electricity during power interruptions caused by problems in the public utility power grid. UPS devices are usually rated to provide a specific amount of power for a specific period of time. In general, a UPS should provide at least enough power for you to shut down a computer in an orderly way by saving work, and then quitting processes and closing sessions.

Note Before purchasing a UPS for use with Windows 2000, determine whether the device is on the Windows 2000 Hardware Compatibility List (HCL).

Selecting and Configuring Options for the UPS Service

After the computer is plugged into the UPS, turned on, and the UPS is connected to the computer with a serial cable (or a cable specified by the manufacturer), you are ready to select and configure the UPS.

To select the UPS support in Windows 2000, perform the following steps:

1. Open **Power Options** in Control Panel. On the **UPS** tab, click **Select**.
2. On the **UPS Selection** screen, under **Select manufacturer**, choose a manufacturer. Select a model and the port on which the computer is connected to the UPS, and then click **Finish**.
3. Open **Power Options** in Control Panel. On the **UPS** tab, click **Configure**.
4. In the **UPS Configuration** dialog box, customize the following settings:
   - Enable all notifications. Select Seconds between power failure and first notification or Seconds between subsequent power failure notifications as appropriate, and configure the desired time.
   - Critical alarm settings. Configure the total minutes on battery before sounding the critical alarm, the program to run when the alarm occurs, and instructions for the computer to either shut down or hibernate upon activation of the critical alarm.
5. In the **UPS Configuration** dialog box, click **OK**, and then click **OK** again to save the new settings.

Note The configuration options for the UPS service can vary depending on the specific UPS device attached to your computer. For details about possible settings, see the documentation included with your UPS device.

Testing a UPS Configuration

After you select and configure the UPS service for your computer, test the configuration to ensure that your computer is protected from power failures. Simulate a power failure by disconnecting the main power supply to the UPS device. During the test, the computer and peripherals connected to the UPS device should remain operational, messages should display at the configured intervals, and events should be logged.

In addition, you should wait until the UPS battery reaches a low level to verify that an orderly shutdown occurs. Then, restore the main power to the UPS device and check the event log to ensure that Windows 2000 logged all actions and that there were no errors.

Note Some UPS manufacturers provide their own UPS software to take advantage of the unique features of their UPS devices. Such features include power event logs, paging/e-mail for power problems, remote management through a Web browser, power quality log, and others.

◆ Implementing Fault Tolerance by Using RAID

Topic Objective
To identify the topics related to implementing fault tolerance by using RAID systems.

Lead-in
The loss of a hard disk because of mechanical or electrical failure is a common form of computer disaster.

- RAID Implementations
- Mirrored Volumes
- RAID-5 Volumes
- Implementing Fault-Tolerant Volumes
- Recovering a Failed Mirrored Volume
- Recovering a Failed RAID-5 Volume

**********ILLEGAL FOR NON-TRAINER USE**********

The loss of a hard disk because of mechanical or electrical failure is a common form of computer disaster. If you experience this problem before implementing fault tolerance, your only option for recovering data on the failed drive is to use disaster recovery methods such as a backup. However, in the interim, lost access to the data can translate into lost time and money for your organization.

To maintain access to data during the loss of a single hard disk, Windows 2000 Server provides a software implementation of a fault tolerance technology known as redundant array of independent disks (RAID). RAID provides fault tolerance by implementing data redundancy. With *data redundancy*, a computer writes data to multiple disks, so that if one disk fails, the information is still available.

Understanding how to implement fault-tolerant volumes in Windows 2000 ensures that you can protect data against a potential disk failure.

Note Fault-tolerant volumes in Windows 2000 Server are only available on dynamic disks. For more information about dynamic disks, see module 12, "Configuring and Managing Disks," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Microsoft Windows 2000 Professional does not provide support for fault-tolerant volumes.

RAID Implementations

Topic Objective
To identify the hardware implementation of RAID and the three software implementations supported by Windows 2000 Server.

Lead-in
You can implement fault tolerance as either a software RAID or a hardware RAID solution.

- **Software Implementation (Supported by Windows 2000 Server)**
  - RAID 0: Striped Volumes
  - RAID 1: Mirrored volumes
  - RAID 5: Striped volumes with parity
- **Hardware Implementation**
  - Disk controller interface handles the creation and regeneration of redundant information
  - RAID level dependent on hardware manufacturer

**********ILLEGAL FOR NON-TRAINER USE**********

You have two options for implementing fault tolerance in Windows 2000: a software implementation of RAID or a hardware implementation of RAID. Windows 2000 provides three implementations of software RAID.

Software Implementation of RAID

In a software implementation of RAID, the operating system provides a mechanism for ensuring data redundancy. Windows 2000 Server supports three types of software RAID, as described in the sections below.

RAID 0

RAID 0 is also known as Disk Striping, where a volume stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly in stripes to these disks. Striped volumes offer the best performance of all the volume types available in Windows 2000, but they do not provide fault tolerance. For more information on stripe volumes see module 12, "Configuring and Managing Disks," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

RAID 1

RAID 1 is also known as Disk Mirroring. Disk Mirroring writes data to two disks simultaneously. If one disk fails, the system uses data from the other disk to continue operation. Windows writes all data to both the primary disk and the secondary or mirror disk, so it can only use only 50 percent of the total available disk space.

RAID 5

RAID 5 volumes share data across all the disks in an array. RAID level 5 is unique because it writes the parity information to all the disks. *Parity information* is the redundant information that is associated with a block of information. In Windows 2000 Server, parity is a calculated value used to reconstruct data after a failure. Windows 2000 achieves data redundancy by arranging a data block and its parity information on different disks in the array.

Important With software implementations of RAID, there is no fault tolerance following a failure until the cause of the failure is repaired. If a second failure occurs before you regenerate the data lost from the first fault, you must restore the data from a backup copy.

Hardware Implementation of RAID

In a hardware implementation, the disk controller interface handles the creation and regeneration of redundant information. Some hardware vendors implement RAID data protection directly into their hardware, as with disk array controller cards. Because these methods are vendor-specific and bypass the fault tolerance software drivers of the operating system, they usually offer performance improvements over software implementations of RAID. In addition, hardware implementations of RAID usually include extra features, such as hot swapping of failed hard disks and dedicated cache memory for improved performance.

Note The level of RAID supported in a hardware implementation is dependent on the hardware manufacturer.

Consider the following points when deciding whether to use a software or a hardware implementation of RAID:

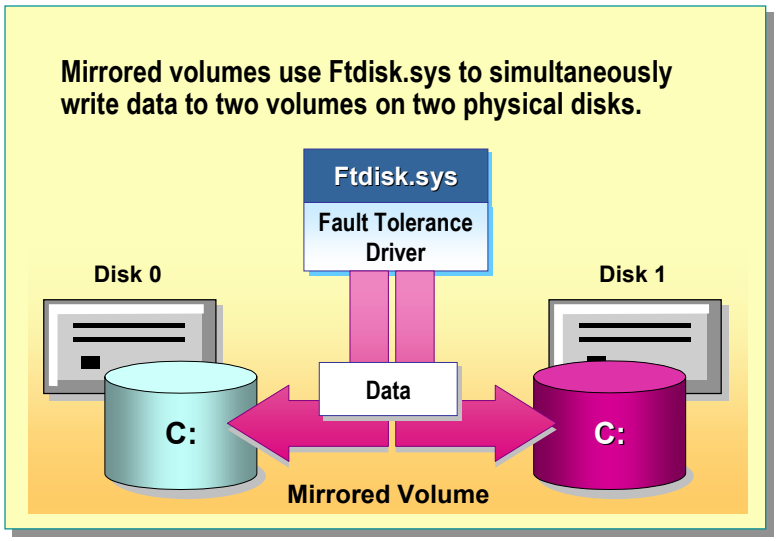
- Hardware fault tolerance is more expensive than software fault tolerance.
- Hardware fault tolerance generally provides faster computer performance than software fault tolerance.
- Hardware fault tolerance solutions may limit equipment options to a single vendor.
- Hardware fault tolerance solutions may implement hot swapping of hard disks to allow for replacement of a failed hard disk without shutting down the computer.

Note When you upgrade Microsoft Windows NT® version 4.0 to Windows 2000, any existing mirror sets or stripe sets with parity are retained. Windows 2000 provides limited support for these fault-tolerant sets, allowing you to manage and delete them.

Mirrored Volumes

Topic Objective
To illustrate the function of a mirrored volume.

Lead-in
Implementing a mirrored volume helps to ensure the survival of data in the event that one member of the mirrored volume fails.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Use the whiteboard in the classroom to diagram the operation of mirrored volumes.

A mirrored volume uses the Windows 2000 Server fault tolerance driver (Ftdisk.sys) to simultaneously write the same data to the volume of each member on each of two physical disks. Each volume is considered a member of the mirrored volume. Implementing a mirrored volume helps to ensure the survival of data in the event that one member of the mirrored volume fails.

Note A mirrored volume can contain any partition, including the boot or system partition. However, both disks in a mirrored volume must be Windows 2000 dynamic disks.

Characteristics of Mirrored Volumes

Emphasize to students that this topic discusses volumes. Clarify to students that mirrored volumes must use two volumes on two separate disks. However, they do not need to use the whole disk. Enforce the point that a volume can be any size.

The following list describes some of the benefits and drawbacks of mirrored volumes:

- Mirrored volumes support file allocation table (FAT) and NTFS file system volumes.
- You can protect system or boot partitions by using mirrored volumes.
- Mirrored volumes require two hard disks.
- Mirrored volumes have relatively high cost per megabyte (MB) because disks are only 50 percent utilized for data storage.
- Mirrored volumes have good read and write performance.
- Mirrored volumes use less system memory compared to RAID-5 volumes.

Performance of Mirrored Volumes

Mirrored volumes can enhance read performance, because the fault tolerance driver reads from both members of the volume at once. Note that you might experience a slight decrease in write performance, because the fault tolerance driver must write to both members. When one member of a mirrored volume fails, performance returns to normal, because the fault tolerance driver works with only one partition.

Because the computer can only use 50 percent of the disk (two members for one set of data), mirrored volumes can be relatively expensive to implement.

Caution Deleting a mirrored volume deletes all of the information stored in that volume. Make sure you save copies of important data before deleting the volume that contains that data.

Disk Duplexing

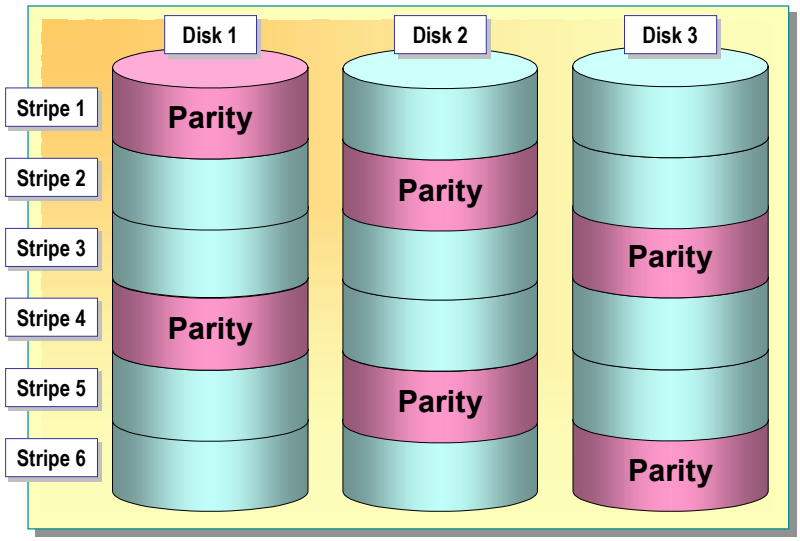
If the same disk controller controls both physical disks in a mirrored volume, and the disk controller fails, neither member of the mirrored volume is accessible. Install a second disk controller in the computer so that each disk in the mirrored volume has its own controller. This arrangement, called *disk duplexing*, can protect the mirrored volume against both controller failure and hard disk failure. Disk duplexing also reduces bus traffic and can potentially improve read performance.

Note Disk duplexing is a hardware enhancement to a Windows 2000 mirrored volume and requires no additional software configuration.

RAID-5 Volumes

Topic Objective
To illustrate the function of a RAID-5 volume.

Lead-in
A RAID-5 volume is currently the most popular approach to fault tolerance design.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
RAID-5 volumes involve a minimum of three drives and a maximum of 32.

Windows 2000 stores parity information on each drive.

Windows 2000 Server also supports fault tolerance through striped volumes with parity, more commonly referred to as RAID-5. *Parity* is a mathematical method of determining the number of odd and even bits in a number or series of numbers, which can be used to reconstruct data if one number in a sequence of numbers is lost.

In a RAID-5 volume, Windows 2000 achieves fault tolerance by adding a parity-information stripe to each disk partition in the volume. If a single disk fails, Windows 2000 can use the data *and* parity information on the remaining disks to reconstruct the data that was on the failed disk.

RAID-5 and Disk Performance

Because of the parity calculation, write operations on a RAID-5 volume are slower than on a mirrored volume. However, RAID-5 volumes provide better read performance than mirrored volumes, especially with multiple controllers, because data is distributed among multiple drives. If a disk fails, however, the read performance on a RAID-5 volume slows while Windows 2000 Server reconstructs the data for the failed disk by using parity information.

Characteristics of RAID-5 Volumes

RAID-5 volumes have a cost advantage over mirrored volumes because disk usage is optimized. The equation to determine the amount of space used in the RAID 5 volume is the total number of space in the RAID 5 volume less one volume. The more disks that you have in the RAID-5 volume, the less the cost of the redundant data stripe.

The following table shows how the amount of space required for the data stripe decreases with the addition of 2-gigabyte (GB) disks to the RAID-5 volume.

Number of disks	Disk space used	Available disk space	Redundancy
3	6 GB	4 GB	33 percent
4	8 GB	6 GB	25 percent
5	10 GB	8 GB	20 percent

The following list describes additional benefits and disadvantages to RAID-5 volumes. RAID-5:

- Volumes support FAT and NTFS.
- Cannot protect system or boot partitions.
- Requires a minimum of three hard disks.
- Has lower cost per MB as compared to mirrored disks.
- Has moderate write performance but excellent read performance.
- Requires more system memory.

Note A software implemented RAID-5 volume cannot contain the boot or system partition.

Implementing Fault-Tolerant Volumes

Topic Objective
To illustrate the options that are available in the Create Volume wizard.

Lead-in
You implement fault-tolerant volumes by using the Create Volume wizard in Computer Management.

Option	Description
Select Disks	The dynamic disks that will participate in the volume (two disks for a mirrored volume; at least three for a RAID-5 volume)
Volume Size	The amount of unallocated space to use on each selected dynamic disk
Assign a Drive Letter or Path	A drive letter or path for the volume
Format Volume	The formatting options for the volume

**********ILLEGAL FOR NON-TRAINER USE**********

With Windows 2000 Server, you can create fault-tolerant volumes from unallocated space by using the Create Volume wizard in Computer Management. To create a mirrored volume in Windows 2000, you must have two dynamic disks available. To create a RAID-5 volume in Windows 2000, you must have at least three dynamic disks available.

Creating a Mirrored Volume

To create a mirrored volume from unallocated space on two dynamic disks, perform the following steps:

1. Open Computer Management from the **Administrative Tools** menu.
2. In the console tree, expand **Storage**, and then click **Disk Management**.
3. Right-click an area of unallocated space, and then click **Create Volume**.
4. Click **Next**, and then, on the **Select Volume Type** page, select **Mirrored volume**, and click **Next**.
5. On the **Select Disks** page, select two dynamic disks, set the size of the mirrored volume, and click **Next**. (Remember that the size of the smaller disk will be the total size of the mirrored volume according to the definition of a mirrored volume.)
6. On the **Assign Drive Letter or Path** page, select either a drive letter, a path, or neither, and then click **Next**.
7. On the **Format Volume** page, you can choose to leave the mirrored volume unformatted or you can choose to format it with FAT, FAT32 or NTFS, and then click **Next**.
8. On the **Completing the Create Volume Wizard** page, review your selections, and then click **Finish**.

Mirroring an Existing Volume

To mirror an existing volume on a dynamic disk, perform the following steps:

1. Right-click the volume that you want to mirror, and then click **Add Mirror**.
2. In the **Add Mirror** dialog box, select the second disk in the mirrored volume, and then click **Add Mirror**.

Note If you are mirroring the existing volume you will receive a message, stating that you mirrored your boot volume. To be able to boot from the mirrored disk, you must add the appropriate entry to your Boot.ini file. To learn more about modifying the Boot.ini file, see the documents, *How to Recover Mirroring Windows NT Using IDE Devices*, and *Creating a Boot Disk for an NTFS or FAT Partition*, under **Additional Reading** on the Student Materials compact disc.

Creating a RAID-5 Volume

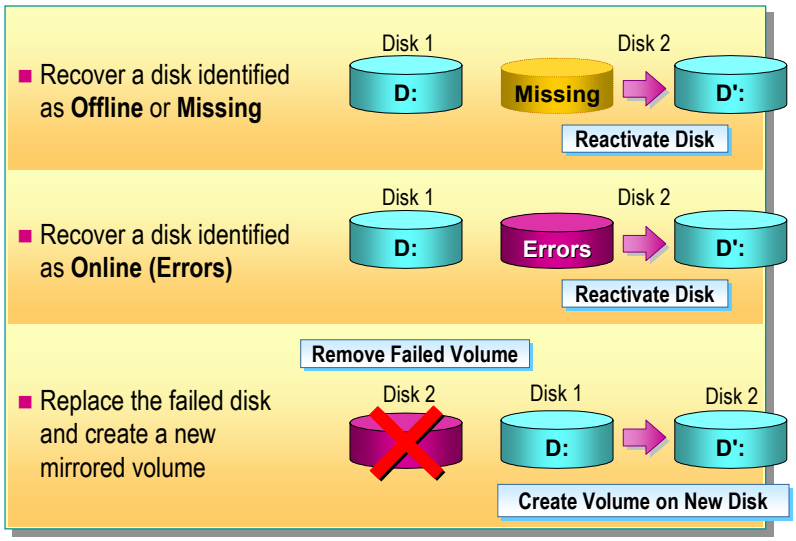
To create a RAID-5 volume from unallocated space on three dynamic disks, perform the following steps:

1. Open Computer Management from the **Administrative Tools** menu.
2. In the console tree, expand **Storage**, and then click **Disk Management**.
3. Right-click an area of unallocated space, and then click **Create Volume**.
4. Click **Next**. On the **Select Volume Type** page, select **RAID-5 volume**, and then click **Next**.
5. On the **Select Disks** page, select three dynamic disks, set the size of the free space to use on each disk for the RAID-5 volume, and then click **Next**.
6. On the **Assign Drive Letter or Path** page, select either a drive letter, a path, or neither, and then click **Next**.
7. On the **Format Volume** page, you can choose to leave the striped set with parity volume unformatted or you can choose to format it with FAT, FAT32 or NTFS, and then click **Next**.
8. On the **Completing the Create Volume Wizard** page, review your selections, and click **Finish**.

Recovering a Failed Mirrored Volume

Topic Objective
To illustrate the procedure for recovering a failed mirrored volume.

Lead-in
When one member of a mirrored volume fails, the other member continues to operate, but it is no longer fault tolerant.



**********ILLEGAL FOR NON-TRAINER USE**********

When one member of a mirrored volume fails, the other member continues to operate, but it is no longer fault tolerant. To prevent potential data loss, you should recover the mirrored volume as soon as possible.

The status of the failed volume appears in Disk Management as **Failed Redundancy**, and one of the disks will appear as **Offline**, **Missing**, or **Online (Errors)**. The method that you use to recover the mirrored volume depends on the status of the disk.

Important If Windows 2000 cannot repair the volume, you may have only the option to delete the volume. This occurs in instances where the disk is severely damaged or not repairable.

Recovering a Failed Mirrored Volume on a Disk Identified as Offline or Missing

To recover a mirrored volume if the disk status is either **Offline** or **Missing**, perform the following steps:

1. Ensure that the disk is attached to the computer and has power.
2. In Disk Management, right-click the disk that is identified as missing or offline, and then click **Reactivate Disk**.

   The status of the disk should return to **Healthy** and the mirrored volume should regenerate automatically.

Recovering a Failed Mirrored Volume on a Disk Identified as Online (Errors)

To recover a mirrored volume if the disk status is **Online (Errors)**, in Disk Management, right-click the disk, and then click **Reactivate Disk**. The status of the volume should return to **Healthy** and the mirrored volume should regenerate automatically.

Warning If a disk continues to appear as **Online (Errors)**, it may be about to fail. You should replace the disk as soon as possible.

Replacing a Disk and Creating a New Mirrored Volume

If the preceding procedures fail to reactivate the disk or if the status of the volume does not return to **Healthy**, you must replace the failed disk and create a new mirrored volume.

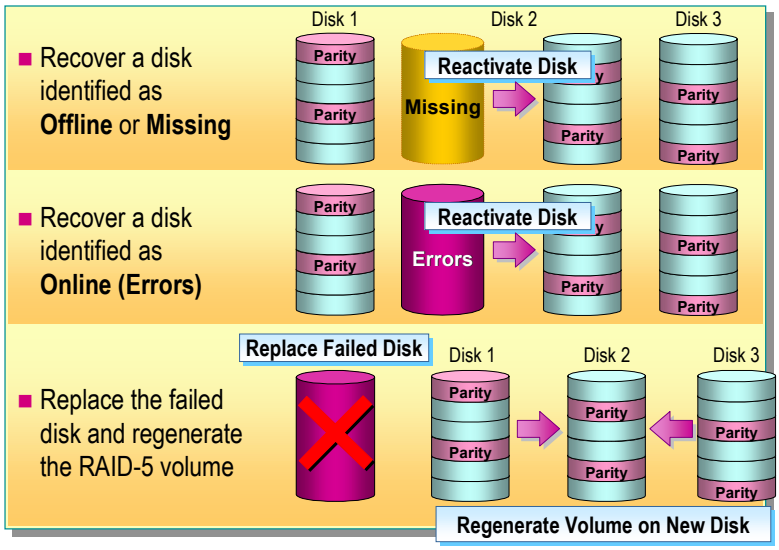
To create a new mirrored volume, perform the following steps:

1. In Disk Management, right-click the mirrored volume on the failed disk, and then click **Remove Mirror**.
2. In the **Remove Mirror** dialog box, click the failed disk, and then click **Remove Mirror**.
3. Click **Yes** when prompted to confirm your choice.
4. Right-click the volume that you want to mirror, and then click **Add Mirror**.
5. Select the second disk in the mirrored volume, and then click **Add Mirror**.

Recovering a Failed RAID-5 Volume

Topic Objective
To illustrate the procedure for recovering a failed RAID-5 volume.

Lead-in
If a member of a RAID-5 volume fails, the computer continues to operate with access to all data.



**********ILLEGAL FOR NON-TRAINER USE**********

When one member of a RAID-5 volume fails, the other members continue to operate even though the volume is no longer fault-tolerant. To prevent potential data loss, you should recover the RAID-5 volume as soon as possible.

The status of the failed volume appears in Disk Management as **Failed Redundancy**, and one of the disks appears as **Offline**, **Missing**, or **Online (Errors)**. The method that you use to recover the RAID-5 volume depends on the status of the disk.

Important If Windows 2000 cannot repair the volume, you may have only the option to delete the volume. This occurs in instances where the disk is severely damaged or not repairable.

Recovering a Failed RAID-5 Volume on a Disk Identified as Offline or Missing

To recover a RAID-5 volume if the disk status is either **Offline** or **Missing**, perform the following steps:

1. Ensure that the disk is attached to the computer and has power.
2. In Disk Management, right-click the disk that is identified as missing or offline, and then click **Reactivate Disk**.

   The status of the disk should return to **Healthy** and the RAID-5 volume should regenerate automatically.

Recovering a Failed RAID-5 Volume on a Disk Identified as Online (Errors)

To recover a RAID-5 volume if the disk status is **Online (Errors)**, in Disk Management, right-click the disk, and then click **Reactivate Disk**. The status of the volume should return to **Healthy** and the RAID-5 volume should regenerate automatically.

Warning If a disk continues to appear as **Online (Errors)**, it may be about to fail. You should replace the disk as soon as possible.

Replacing a Disk and Regenerating a RAID-5 Volume

If the preceding procedures fail to reactivate the disk or if the status of the volume does not return to **Healthy**, you must replace the failed disk and regenerate the RAID-5 volume.

To regenerate a RAID-5 volume using a different disk, perform the following steps:

1. In Disk Management, right-click the RAID-5 volume on the failed disk, and then click **Repair Volume**.
2. In the **Repair RAID-5 Volume** dialog box, select the disk that will replace the failed disk in the RAID-5 volume, and then click **OK**.

Lab A: Implementing Fault-Tolerant Volumes

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will implement fault-tolerant volumes.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Implement RAID-5 volumes.
- Implement mirrored volumes.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors.

► To start the lab

1. Insert the Student Materials compact disc into your CD-ROM drive.
2. At the root of the compact disc, double-click **Default.htm**.
3. On the Student Materials Web page, click **Labs**.
4. Click **Implementing Fault-Tolerant Volumes**.
5. Read the introduction information, and then click the link to start the lab.

Estimated time to complete this lab: 15 minutes

Backing Up and Restoring Data

Topic Objective
To identify the topics related to using Backup.

Lead-in
Windows 2000 includes an enhanced, graphical backup utility, called Backup, that is designed to protect data from accidental loss as a result of hardware or storage media failure.

- Overview of Data Backup and Restoration
- Backup Types
- Example Backup Schedules
- Configuring File and Folder Backup
- Backing Up System State Data
- Scheduling a Backup
- Restoring Files and Folders

**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 includes a backup utility, called Backup, that is designed to protect data from accidental loss resulting from the failure of your hardware or storage media. Using Backup, you can:

- Back up files and folders.
- Back up system state data.
- Schedule a backup.
- Restore files and folders.

Note You can also create an Emergency Repair Disk (ERD) by using Backup. More detailed information about the ERD is provided later in the module.

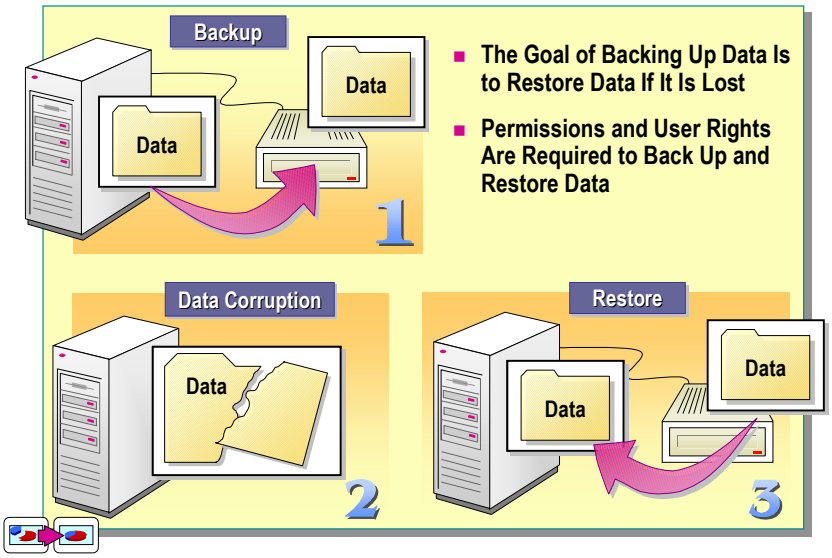
Key Point
Backup supports a variety of storage devices in addition to tape drives.

Backup supports a variety of storage devices and media, including tape drives, logical drives, removable disks, and recordable CD-ROM drives. In addition, Backup includes wizards that are designed to make using the utility easy and efficient. Using Backup helps to ensure a quick system recovery in the event of a failure.

Overview of Data Backup and Restoration

Topic Objective
To introduce backing up and restoring data.

Lead-in
While maintaining a network, it is important to ensure that network data, such as Active Directory, is not lost. For this purpose, you use Backup.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation. Use this slide to explain why data backup is an important task. The animation begins with the process of data backup, then it presents the data becoming corrupt, and finally it depicts the data being restored from the back up copy.

Key Points
The goal of all backup jobs is to successfully restore lost and corrupt data.

A user must have the appropriate user right or permission to back up and restore data.

The goal of all backup jobs is the efficient recovery of lost data, should a failure occur. A *backup job* is a single process of backing up data. Regularly backing up data on server and client computer hard disks prevents data loss because of disk drive failures, power outages, virus infections, and other accidents. If data loss occurs, and you have performed regular backup jobs based on careful planning, you can restore the lost data, regardless of whether a single file or an entire hard disk is involved.

Backup

Backup allows you to quickly and easily back up and restore data to a file or to a tape drive. Use Backup to back up data manually or to schedule unattended backup jobs on a regular basis. You can back up files to hard disks, removable disks, recordable compact discs, and optical drives. You access Backup on the **System Tools** menu.

Permissions and User Rights

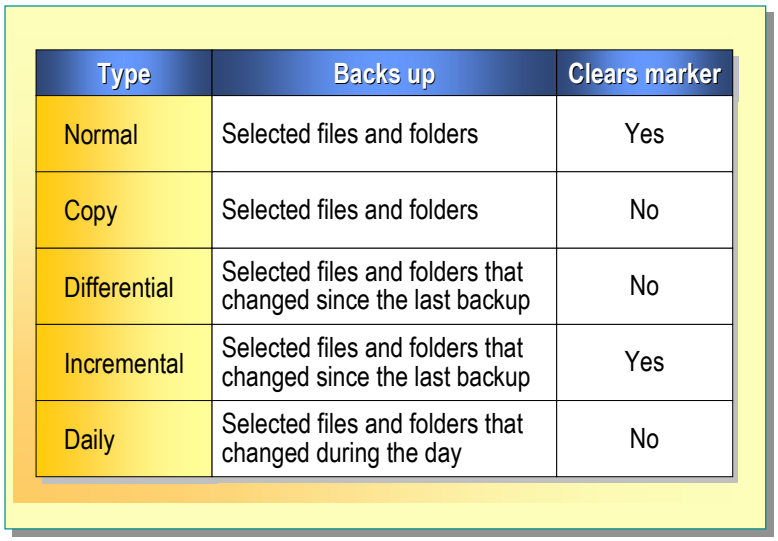
To successfully back up and restore data on a computer running Windows 2000, you must have the appropriate permissions and user rights, as described in the following list:

- All users can back up their own files and folders. They can also back up files for which they have the Read permission.
- All users can restore files and folders for which they have the Write permission.
- Members of the Administrators, Backup Operators, and Server Operators groups can back up and restore all files (regardless of the assigned permissions). By default, members of these groups have the Backup Files and Directories and the Restore Files and Directories user rights.

Backup Types

Topic Objective
To describe the five backup types.

Lead-in
Backup types provide you with methods for backing up data.



Type	Backs up	Clears marker
Normal	Selected files and folders	Yes
Copy	Selected files and folders	No
Differential	Selected files and folders that changed since the last backup	No
Incremental	Selected files and folders that changed since the last backup	Yes
Daily	Selected files and folders that changed during the day	No

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Show students the Archive attribute in the **Properties** dialog box for a document.

Backup provides five backup types: normal, copy, differential, incremental, and daily. Each of these backup types target specific categories of files for backup, such as files that have changed since the last backup or all files in a specific folder.

Key Points
Differential backups *do not* clear backup markers.

Incremental backups *clear* backup markers.

Markers are critical when you combine different backup types, as both incremental and differential backups check for markers.

Some backup types use backup *markers*, also known as archive attributes, which mark a file as having changed. When a file changes, an attribute or marker is set on the file, indicating that the file has changed since the last backup. When you back up the file, the marker is cleared or reset.

The following table presents the backup types, what each type backs up, whether the backup type clears markers, and tips for using the backup type.

Type	Backs up
Normal	All selected files and folders. It clears markers but does not look for markers. Normal backups speed up the restore process because the backup files are the most current and you do not need to restore multiple backup jobs.
Copy	All selected files and folders. It neither looks for nor clears markers. If you do not want to clear markers and affect other backup types, use Copy. For example, use a Copy backup between a Normal and an Incremental backup to create an archival snapshot of network data.
Differential	Only selected files and folders that have a marker. It does not clear markers. Because a Differential backup does not clear markers, if you did two Differential backups in a row on a file, and nothing changed in the file, the entire file would be backed up each time.

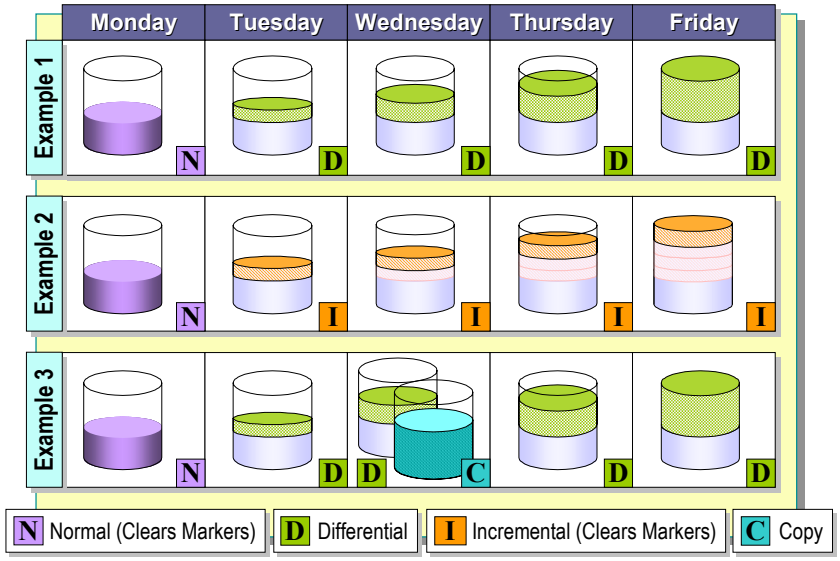
(continued)

Type	Backs up
Incremental	Only selected files and folders that have a marker. It clears markers. Because an Incremental backup clears markers, if you did two Incremental backups in a row on a file and nothing changed in the file, the file would not be backed up the second time.
Daily	All selected files and folders that have changed during the day. It neither looks for nor clears markers. If you want to back up all files and folders that change during the day, use a Daily backup.

Example Backup Schedules

Topic Objective
To present examples of using the different backup types.

Lead-in
To help you understand how backup types work, here are some examples.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Use the slide to show students how combining backup types affects the way that an administrator restores data.

For each example, go through each day of the week, explaining what data is backed up. Then, explain what would be restored if data were restored on Friday.

In Example 3, the copy backup type performed on Wednesday is not part of the Friday restore.

Each cylinder contains the entire amount that you need to restore. The bright color section of the cylinder represents what was backed up on a particular day.

An effective backup strategy typically combines different backup types. Some backup types require more time to back up data than to restore data. Conversely, other backup types require less time to back up data than to restore data. The following examples explain scenarios that combine different backup types, and show how you might use backup types in your own environment.

Example 1: Normal and Differential Backups

On Monday, a normal backup is performed, and on Tuesday through Friday, differential backups are performed. Differential backups do not clear markers, which means that each backup includes all changes since Monday. If data becomes corrupt on Friday, you only need to restore the normal backup from Monday and the differential backup from Thursday. This strategy takes more time to back up data than to restore it.

Example 2: Normal and Incremental Backups

On Monday, a normal backup is performed, and on Tuesday through Friday, incremental backups are performed. Incremental backups clear markers, which means that each backup includes only the files that have changed since the previous backup. If data becomes corrupt on Friday, you need to restore the normal backup from Monday and all incremental backups from Tuesday through Friday. This strategy takes less time to back up data than to restore it.

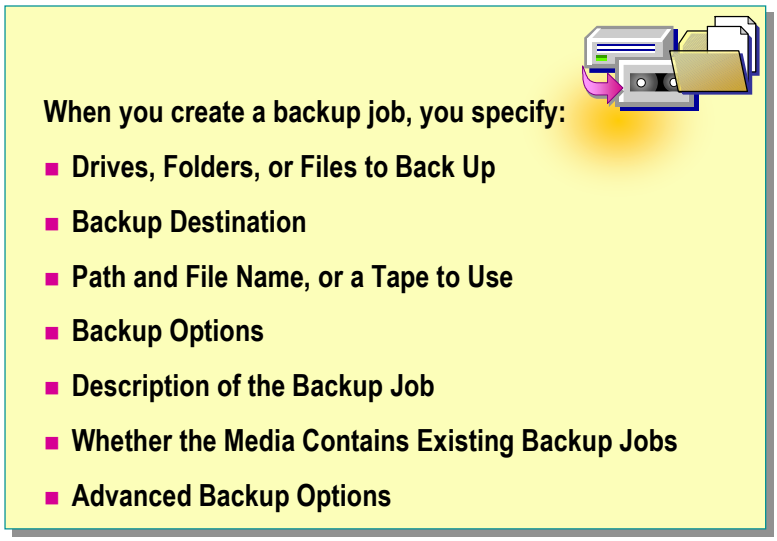
Example 3: Normal, Differential, and Copy Backups

This strategy is the same as that of Example 1 except that on Wednesday, a copy backup is performed. Copy backups include all selected files and do not clear markers or interrupt the usual backup schedule. Therefore, each differential backup includes all changes since Monday. Copy backups are helpful when you need to create a snapshot of your data.

Configuring File and Folder Backup

Topic Objective
To identify the information that is required to back up files and folders.

Lead-in
You use the Backup utility to archive selected files and folders on volumes that are formatted as FAT or NTFS.



**********ILLEGAL FOR NON-TRAINER USE**********

Use Backup to archive files and folders on volumes that are formatted as FAT, FAT32 or NTFS. Backup includes a Backup wizard, which steps you through the entire backup process.

Note You can also use Backup to create a backup job manually, without using the wizard.

When you create a backup job, you specify:

- The drives, folders, or files to back up.
- A backup destination. You can specify to back up files and folders to a file or to a tape, if a tape device is installed on your computer.
- A path and file name for the backup file, or a tape to use.
- Backup options, such as the backup type and the log file type.
- A description of the backup job.
- Whether the backup medium contains existing backup jobs.
- Advanced backup options, such as data verification or hardware compression.

Backing Up System State Data

Topic Objective
To illustrate the components of system state data on client and server computers.

Lead-in
You use Backup to back up the system state data on a local computer.

Component	DC **	Server ***	Professional
Registry	✓	✓	✓
CS* Class Registration Database	✓	✓	✓
System Startup Files	✓	✓	✓
Certificate Services Database	✓	✓	
Active Directory	✓		
Sysvol Folder	✓		

* CS Component Services
** DC A domain controller running Windows 2000 Server
*** Server A computer running Windows 2000 Server that is also a certificate server

**********ILLEGAL FOR NON-TRAINER USE**********

You can use Backup to back up the system state data. If the system state data on a computer has been backed up and that same computer system fails, you can rebuild the computer with the original Windows 2000 compact disc and the system state data.

The system state data contains the information to restore the operating system to its pre-failure state. The system state data includes the following system components:

Mention that the Component Services class registration database was formerly known as the COM+ database.

- Registry
- Component Services class registration database
- System startup files
- Certificate Services database
- Active Directory™ directory service
- Sysvol folder

In Windows 2000 Professional, the system state includes the registry, the Component Services class registration database, and system startup files. In Windows 2000 Server operating systems, the system state data also includes the Certificate Services database (if the computer is a certificate server), Active Directory, and the Sysvol folder (if the computer is a domain controller).

Note You cannot back up individual components of the system state data.

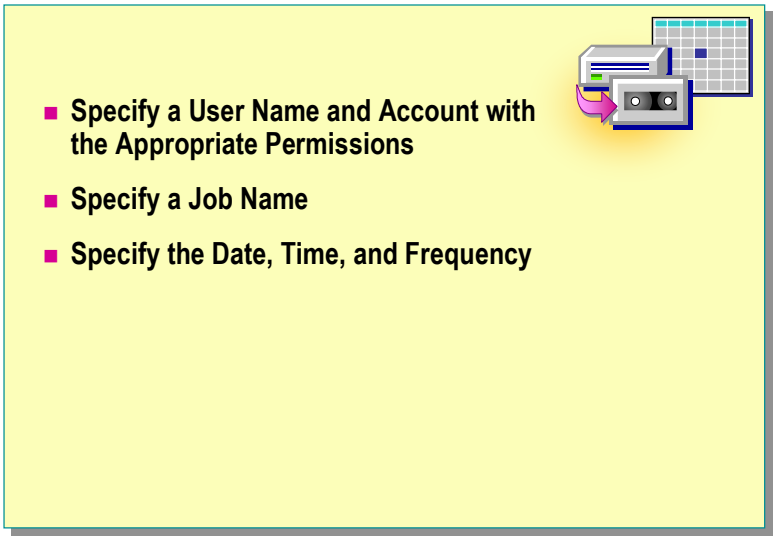
You back up the system state data on a local computer in one of the following three ways:

- In the Backup wizard, on the **What to Back Up** page, click **Only back up the System State data**.
- In the Backup wizard, on the **Items to Back Up** page, expand **My Computer**, and then select the check box to the left of **System State**.
- In the Backup utility, on the **Backup** tab, expand **My Computer**, and then select the check box to the left of **System State**.

Scheduling a Backup

Topic Objective
To identify the information that is required for scheduling a backup.

Lead-in
You can schedule a backup to occur at regular intervals or during periods of relative inactivity on a network.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate how to schedule a backup job.

Schedule the job for only a few minutes later so that you have a job to use when you demonstrate a restore.

Backup is integrated with Task Scheduler. As a result, use Backup to schedule a backup job. You should try and schedule a backup job to occur at regular intervals or during periods of relative inactivity on a network.

You can schedule a backup one of two ways: during the process of creating a backup job or by using the **Scheduled Jobs** tab in Backup.

To create a scheduled backup during the process of creating a backup job, perform the following steps:

1. On the Completing the Backup Wizard page, click **Advanced**.
2. On the **When to Back Up** page, click **Later**, enter a job name, and then click **Set schedule**.
3. In the **Schedule Job** dialog box, configure options (such as frequency and start time), and then click **OK**.

To create a scheduled task using the **Schedule Job** tab in Backup, perform the following steps:

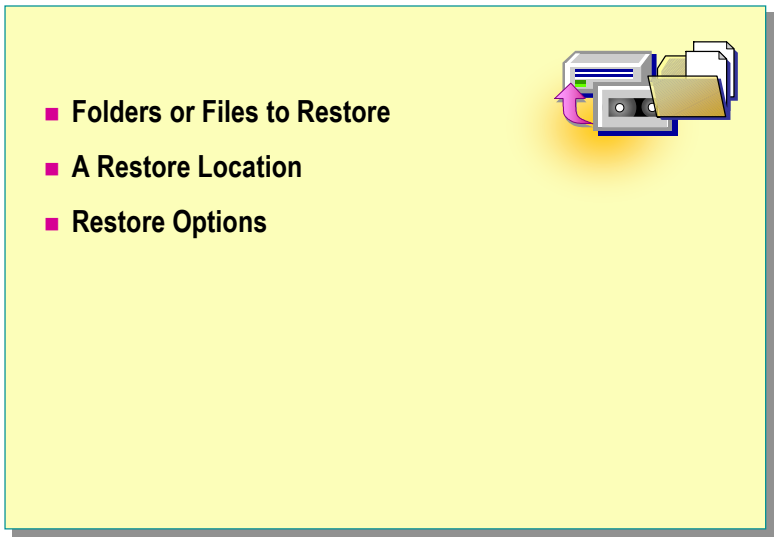
1. On the **Scheduled Jobs** tab in **Backup**, double-click the day you wish to start the scheduled backup.
2. Complete the information in the Backup wizard.

Note To view scheduled jobs, click the **Schedule Jobs** tab in Backup.

Restoring Files and Folders

Topic Objective
To identify the information that is required to restore files and folders.

Lead-in
You use the Backup utility in Windows 2000 to restore files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

You also use Backup to restore files and folders in the event of data loss. Backup includes a Restore wizard that steps you through the entire restore process.

Note You can use Backup to restore files and folders manually, without using the wizard.

When you restore files and folders, you specify:

- The folders or files to restore.
- A restore location. Restore files to the original location, an alternate location, or to a single folder.
- Restore options, such as whether to replace existing files with backup files.

Caution You must restore data that is archived from a Windows 2000 NTFS volume to another Windows 2000 NTFS volume to avoid data loss and preserve access permissions, Encrypting File System settings, disk quota information, mounted drive information, and remote storage information. For example, if you restore an encrypted file on an NTFS volume to a FAT partition, you will lose all of the decryption data, rendering the file unreadable.

Lab B: Backing Up and Restoring System State Data

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will back up and restore system state data.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Back up system state data.
- Restore system state data.

Prerequisites

Before working on this lab, you must have:

- Knowledge of the backup and restore process.
- Knowledge of the system state data.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.
- A local user account named EFSUser with a password of **password**.

Estimated time to complete this lab: 20 minutes

Exercise 1
Backing Up and Restoring System State Data

Scenario

The Package Handling department is concerned about losing information stored in the registry. They have a member server that has just been installed and they have been setting up users and groups. They want to see how Backup might be used to protect the server from administrator error in deleting the wrong user or group. Using Windows 2000 Advanced Server in the Package Handling department, you are going to demonstrate the ability of Backup to back up system state data.

Goal

In this exercise, you will back up the system state data of your computer to a location on the hard drive and then delete a local user account. After deleting the local user account you will restore the system state data and verify that the user account has been restored.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with a password of **domain**. Using Backup, back up the system state data to C:\Backup.bkf.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your student number) Password: **domain** Log on to: **nwtraders** **b.** Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**. **c.** On the **Welcome** tab, click the button to the left of **Backup Wizard**. **d.** On the **Welcome to the Windows 2000 Backup and Recovery Tools** page, click **Next**. **e.** On the **What to Back Up** page, click **Only back up the System State data**, and then click **Next**. **f.** On the **Where to Store the Backup** page, type **C:\Backup.bkf** and then click **Next**. **g.** On the **Completing the Backup Wizard** page, click **Advanced**.

What are the backup types you can select to perform?

Normal

Copy

Incremental

Differential

Daily

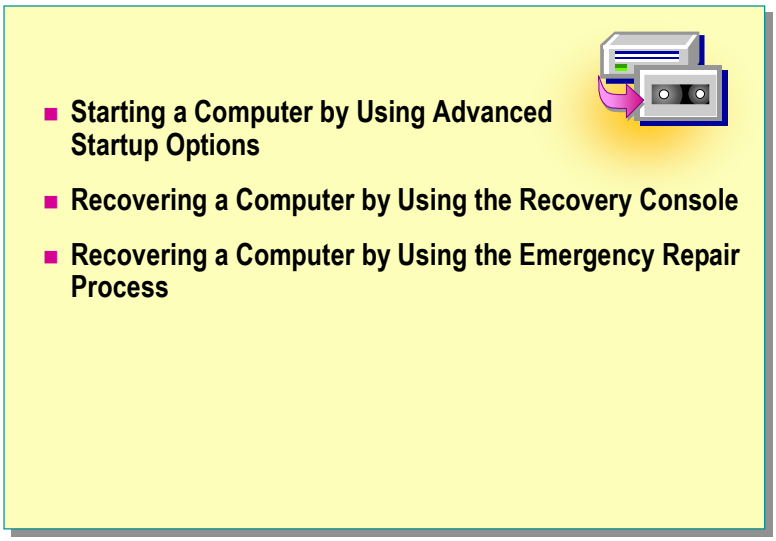
Tasks	Detailed Steps
1. (*continued*)	**h.** On the **Type of Backup** page, verify that **Normal** is selected, and then click **Next**. **i.** On the **How to Backup** page, select the **Verify data after backup** check box, and then click **Next**. **j.** On the **Media Options** page, click **Next** to accept the defaults. **k.** On the **Backup Label** page, click **Next** to accept the defaults. **l.** On the **When to Back Up** page, click **Next** to accept the defaults. **m.** On the **Completing the Backup Wizard** page, click **Finish**. **n.** When the backup is complete, click **Close** to close the **Backup Progress** dialog box, and then close Backup.
2. Delete the EfsUser local account.	**a.** Open Computer Management from the **Administrative Tools** menu. **b.** In the console tree, under **System Tools**, expand **Local Users and Groups**, and then click **Users**. **c.** In the details pane, right-click **EfsUser**, and then click **Delete**. **d.** In the message, click **Yes** to confirm deletion. **e.** Close Computer Management.
3. Using Backup, restore the system state data.	**a.** Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**. **b.** On the **Welcome** tab, click the button to the left of **Restore Wizard**. **c.** On the **Welcome to the Restore Wizard** page, click **Next**. **d.** On the **What to Restore** page, expand **File**, expand **Media created** *xx/xx/xx* (where *xx/xx/xx* is the current date), select the **System State** check box, and then click **Next**. **e.** On the **Completing the Restore Wizard** page, click **Finish**. **f.** In the **Enter Backup File Name** dialog box, in the **Restore from backup file** box, verify that **C:\backup.bkf** appears, and then click **OK**. **g.** When the restore is complete, click **Close** to close the **Restore Progress** dialog box. **h.** In the **Backup** message, click **Yes** to restart the computer.
4. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password **domain** and verify that the user account EfsUser has been restored.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Open Computer Management from the **Administrative Tools** menu. **c.** In the console tree, under **System Tools**, expand **Local Users and Groups**, click **Users**, and then verify that **EfsUser** appears in the details pane.

Tasks	Detailed Steps
What component of the system state data contains the EfsUser user account? **The registry.**	
4. (*continued*)	**d.** Close Computer Management, and then log off.

Using Disaster Recovery Tools

Topic Objective
To identify the topics related to recovering from a computer disaster.

Lead-in
Windows 2000 includes several options you can use in an attempt to recover from a computer disaster.



**********ILLEGAL FOR NON-TRAINER USE**********

If a computer disaster occurs, Windows 2000 provides several options you can use in an attempt to restore the computer. Understanding these options and what they can do will help you to restore a computer to working condition.

Starting a Computer by Using Advanced Startup Options

Topic Objective
To illustrate the advanced startup options in Windows 2000.

Lead-in
Windows 2000 includes advanced startup options for use in troubleshooting and repairing startup problems, maintaining and repairing Active Directory, and debugging the operating system.

Operating System Selection	F8
Safe Mode	Loads basic devices and drivers
Safe Mode with Networking	Loads safe mode options and networking services and drivers
Safe Mode with Command Prompt	Loads safe mode options but starts a command prompt instead of the graphical user interface
Enable Boot Logging	Logs the loading and initialization of drivers and services
Enable VGA Mode	Loads the basic VGA driver
Last Known Good Configuration	Uses the last known good configuration to start the computer
Directory Services Restore Mode	Allows Active Directory restoration on domain controllers
Debugging Mode	Enables debugging

**********ILLEGAL FOR NON-TRAINER USE**********

Windows 2000 includes advanced startup options to use when troubleshooting and repairing startup problems and when connecting the computer to a debugger. These new startup options enhance your ability to diagnose and resolve driver incompatibility and startup problems in Windows 2000.

Note To display the advanced startup options, press F8 during the operating system selection phase of the startup process in Windows 2000.

The following table describes the Windows 2000 advanced startup options.

Option	Description
Safe Mode	Loads only the basic devices and drivers that are required to start the computer, including the mouse, keyboard, mass storage devices, base video, and the standard, default set of system services. This option also creates a log file.
Safe Mode with Networking	Loads only the basic devices and drivers that are required to start the computer and enable networking. This option also creates a log file.
Safe Mode with Command Prompt	Loads safe mode options but starts a command prompt instead of the graphical user interface. This option also creates a log file.
Enable Boot Logging	Creates a log file that references all of the drivers and services that the system loads (or does not load). This log file is called Ntbtlog.txt and is located in the system root folder (the folder that contains the Windows 2000 system files).
Enable VGA Mode	Loads the basic VGA driver. This mode is useful if a video driver is preventing Windows 2000 from starting properly.

(continued)

Option	Description
Last Known Good Configuration	Uses the last known good configuration information in the registry to start the computer.
Directory Services Restore Mode	Allows restoration and maintenance of Active Directory and restoration of the Sysvol folder on domain controllers.
Debugging Mode	Sends debugging information to another computer through a serial cable.

Note A domain controller can utilize the **Safe Mode** and **Safe Mode with Command Prompt** options, but Active Directory services will not be available.

Recovering a Computer by Using the Recovery Console

Topic Objective
To identify the functionality of and means of accessing the Recovery Console.

Lead-in
The Windows 2000 Recovery Console is a command-line interface that you use to perform a variety of administrative tasks.

Use the Recovery Console to:

- Start and stop services.
- Read and write data on a local hard drive.
- Format hard disks and display hidden system files.

**********ILLEGAL FOR NON-TRAINER USE**********

The Recovery Console in Windows 2000 is a command-line console that you can start from the Windows 2000 Setup program. The Recovery Console is particularly useful if you need to repair a system by copying a file from a disk or compact disc to the hard drive, or if you need to reconfigure a service that is preventing a computer from starting properly.

Using the Recovery Console

You can use the Recovery Console to:

- Start and stop services.
- Read and write data on a local drive (including drives that are formatted with the NTFS file system).
- Format hard disks and display hidden system files.

Installing the Recovery Console

To install the Recovery Console, start a command prompt in Windows 2000, change directories to the I386 folder on the Windows 2000 compact disc, and then run the **winnt32** command with the **/cmdcons** switch. After you install the Recovery Console, you can access it from the **Startup** menu.

Note You can also access the Recovery Console by using the Windows 2000 Setup disks or the Windows 2000 compact disc to start your computer, and then selecting the **Recovery Console** option when you are prompted to choose repair options.

When you start the Recovery Console, you must specify the installation of Windows 2000 that you want to log on to (even on a computer with a single-boot configuration). You then must log on as Administrator.

Recovery Console Commands

When you run the Recovery Console, you can get help on the available commands by typing **help** at the command prompt and then pressing ENTER.

The following table describes the commands available in the Recovery Console.

Command	Description
chdir (cd)	Displays the name of the current folder or changes the current folder
chkdsk	Checks a disk and displays a status report
cls	Clears the screen
copy	Copies a single file to another location
delete (del)	Deletes one or more files
dir	Displays a list of files and subfolders in a folder
disable	Disables a system service or a device driver
enable	Starts or enables a system service or a device driver
exit	Exits the Recovery Console and restarts your computer
fdisk	Manages partitions on your hard disks
fixboot	Writes a new partition boot sector onto the system partition
fixmbr	Repairs the master boot record of the partition boot sector
format	Formats a disk
help	Displays a list of the commands that you use in the Recovery Console
logon	Logs on to a Windows 2000 installation
map	Displays the drive letter mappings
mkdir (Md)	Creates a folder
more	Displays a text file
rmdir (rd)	Deletes a folder
rename (ren)	Renames a single file
systemroot	Sets the current folder to the systemroot folder of the system that you are currently logged on to
type	Displays a text file

Recovering a Computer by Using the Emergency Repair Process

Topic Objective
To illustrate the steps for recovering a computer by using the emergency repair process.

Lead-in
You can use the emergency repair process to fix problems that may be preventing a computer from starting.

To Create an Emergency Repair Disk:

- **Start the Computer by Using the Windows 2000 Setup Disks or the Compact Disc**
- **Choose the Repair Options During Setup**
- **Choose the Type of Repair**
- **Start the Recovery Process**
- **Restart Your Computer**

**********ILLEGAL FOR NON-TRAINER USE**********

Use the emergency repair process with your registry, system files, partition boot sector, and startup environment. However, you may not be able to use the emergency repair process to fix your system unless you have created an ERD, which you can create using the Backup utility. If you have not created an ERD, you can still attempt to use the emergency repair process to fix your computer, but the emergency repair process may not be able to fix your problems.

Creating an Emergency Repair Disk

Before you use the emergency repair process to repair a system, you must create an ERD for that system. Create an ERD by using the Backup utility. To create an ERD, perform the following steps:

1. Open Backup.
2. On the **Welcome** tab, click **Emergency Repair Disk**.
3. Insert a blank, 1.44 MB floppy disk into the floppy disk drive, and then click **OK** in the **Emergency Repair Diskette** dialog box.

Note You can also specify to backup the registry to the repair directory to help recover a system if the registry is damaged.

4. When the creation process is complete, click **OK** in the **Emergency Repair Diskette** dialog box, and then remove the disk and label it appropriately.

Note You cannot use this disk to start the computer. You can only use this disk to repair damaged disks.

Using the Emergency Repair Process

The sections below provide a general overview of the emergency repair process. You use this process to perform emergency repairs on a computer.

Note The repair process relies on information that is saved in the *Systemroot*\Repair folder. You must not change or delete this folder.

Start the Computer by Using the Windows 2000 Setup Disks or the Compact Disc

The first step in the emergency repair process is to start the failed computer by using the Windows 2000 Setup disks or the Windows 2000 compact disc.

Choose the Repair Options During Setup

After the computer starts, the Setup program starts. During Setup, you are prompted to choose whether you want to continue installing the Windows 2000 operating system. Press ENTER to start the installation process. During installation, specify whether to install a fresh version of Windows 2000 or to repair an existing installation. To repair a damaged or corrupt system, press R. You are then prompted to choose whether to repair the system by using the Recovery Console or by using the emergency repair process. Press R to repair the system using the emergency repair process.

Choose the Type of Repair

Next, specify the repair option you want to use. The fast repair option does not require any user interaction. This option attempts to repair problems related to the registry, system files, the partition boot sector on your boot volume, and your startup environment (if you have a dual-boot or multiple-boot configuration).

The manual repair option requires user input. This option allows you to choose whether to repair system files, partition boot sector problems, or startup environment problems, but not problems with your registry. For example, you would use the manual repair option to attempt to repair system files if you know your partition boot sector and your startup environment are both intact.

Start the Recovery Process

To start the repair process, make sure you have the 1.44 MB ERD that you created by using the Backup utility. You should also have the original Windows 2000 compact disc available for use. If you do not have an ERD, the emergency repair process attempts to locate your Windows 2000 installation files and to start repairing the system, but it may fail in the process.

Restart Your Computer

If the emergency repair process was successful, your computer will automatically restart and you should have a working system.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to Disaster Protection
- Configuring an Uninterruptible Power Supply
- Implementing Fault Tolerance by Using RAID
- Backing Up and Restoring Data
- Using Disaster Recovery Tools

**********ILLEGAL FOR NON-TRAINER USE**********

1. What requirement applies to disks used to create new fault-tolerant volumes in Windows 2000?

   All disks that will participate in a fault-tolerant volume must be upgraded to dynamic storage.

2. After installing a new hardware device, you restart your computer and log on. Immediately after logging on, your computer fails with a Stop error that indicates that the problem resulted from the new device driver. How would you solve this problem?

   You would restart the computer and select the Safe Mode advanced startup option. When the computer starts in Safe Mode, you would remove the device that was causing the Stop error.

3. Describe two methods for accessing the Recovery Console.

   You can access the Recovery Console by starting the computer from the Windows 2000 compact disc or from the Windows 2000 Startup disks, and then choosing the Repair option in Setup.

   You can also access the Recovery Console by running Winnt32.exe /cmdcons, and starting the Recovery Console from the Operating System Selection menu.

4. An administrator on your network has accidentally deleted Windows 2000 registry files on a computer that is configured to dual boot and was started in another operating system. The administrator had selected the option **Back up everything on my computer** just prior to the accident. What feature of Backup will allow the administrator to restore the computer's operating system to its original state?

   Because the administrator did a backup of all data on the computer, the system state data was also backed up. The administrator must reinstall the operating system and then restore the system state data by using Backup.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 14: Installing and Configuring Terminal Services

Contents

Overview	1
Introduction to Terminal Services	2
Planning the Installation	8
Installing Terminal Services	17
Configuring Terminal Services	19
Establishing a Terminal Session	23
Configuring Session Settings	26
Lab A: Installing Terminal Services	27
Installing Applications on a Terminal Server	33
Lab B: Installing an Application	37
Review	40
Course Evaluation	42

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

Labs:
75 Minutes

This module introduces Terminal Services in Microsoft® Windows® 2000. The module covers planning tasks, installation and configuration of the server and client, and how to establish a Terminal session. The module also covers the installation of applications on a Terminal server.

At the end of this module, students will be able to:

- Describe the purpose and use of Terminal Services.
- Plan a Terminal Services installation.
- Install Terminal Services.
- Configure Terminal Services.
- Establish a Terminal session.
- Configure session settings.
- Install applications on a Terminal server.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_14.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.

Module Strategy

Use the following strategy to present this module:

- Introduction to Terminal Services

  In this topic, introduce Terminal Services for Windows 2000. Explain how Terminal Services works, and then explain the steps for starting a Terminal session. Briefly describe the features and benefits of Terminal Services in the context of business purposes.

- Planning the Installation

  In this topic, describe the planning tasks for installation. Explain each task and discuss the issues that are associated with client applications, client hardware, server configuration, and licensing requirements.

- Installing Terminal Services

  In this topic, describe the two options for installing Terminal Services. Demonstrate the steps for installing Terminal Services after the Windows 2000 Setup process to reinforce the lab exercise.

- Configuring Terminal Services

  In this topic, present procedures for configuring Terminal Services for users. First, explain how to configure the default security setting to enable application access. Next, explain the settings you can configure for user profiles. Finally, explain the options for distributing the Terminal Services client software and the procedures for creating a client installation disk and installing the Terminal Services client.

- Establishing a Terminal Session

  In this topic, present the procedures that users follow during a Terminal session. Explain the procedure and options for connecting to a Terminal server. Then, explain the difference between disconnecting and logging off from a session.

- Configuring Session Settings

  In this topic, present the options for settings to configure for Terminal sessions. Explain the options for limiting sessions.

- Installing Applications on a Terminal Server

  In this topic, presents the procedure for installing applications on a Terminal server and running compatibility scripts. Describe the two options for installing an application on a Terminal server. Then, explain application compatibility scripts and describe the procedure for running the scripts.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

The labs in this module require each pair of student computers to be member server of the nwtraders.msft domain. To prepare the student computers to meet this requirement, complete module 1, "Installing or Upgrading to Microsoft Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- Student computers will have Terminal Services installed.
- Student computers will have Terminal Services 32-bit client software installed.
- Student computers will have created two folders: C:\Tsprofiles and C:\Tshomes.
- Student computers will have the Windows 2000 Support Tools installed.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about installing and configuring Terminal Services in Windows 2000.

- Introduction to Terminal Services
- Planning the Installation
- Installing Terminal Services
- Configuring Terminal Services
- Establishing a Terminal Session
- Configuring Session Settings
- Installing Applications on a Terminal Server

**********ILLEGAL FOR NON-TRAINER USE**********

Terminal Services is an optional component of the Microsoft® Windows® 2000 server family. Terminal Services provides the Windows graphical user interface to remote devices over a network, wide area network (WAN) connection, or Internet connection.

Terminal Services is ideal for making line-of-business applications available to mobile users, branch offices, or workers using Windows-based terminals. Terminal Services is also ideal for providing desktop users with access to limited, nonstandard, or infrequently used applications. Because all application and data processing takes place on the server, clients do not require significant amounts of RAM or processing power. Therefore, Terminal Services can help an organization reduce total cost of ownership (TCO) by using existing client hardware and lower-cost equipment, such as Windows-based terminals or handheld devices, and by providing centralized management and control of applications.

At the end of this module, you will be able to:

- Describe the purpose and use of Terminal Services.
- Plan a Terminal Services installation.
- Install Terminal Services.
- Configure Terminal Services.
- Establish a Terminal session.
- Configure session settings.
- Install applications on a Terminal server.

Introduction to Terminal Services

Topic Objective
To introduce Terminal Services for Windows 2000.

Lead-in
The fundamentals of Terminal Services provide an understanding of the many purposes and uses of Terminal Services in an organization.

- How Terminal Services Works
- User Environments
- Features and Benefits

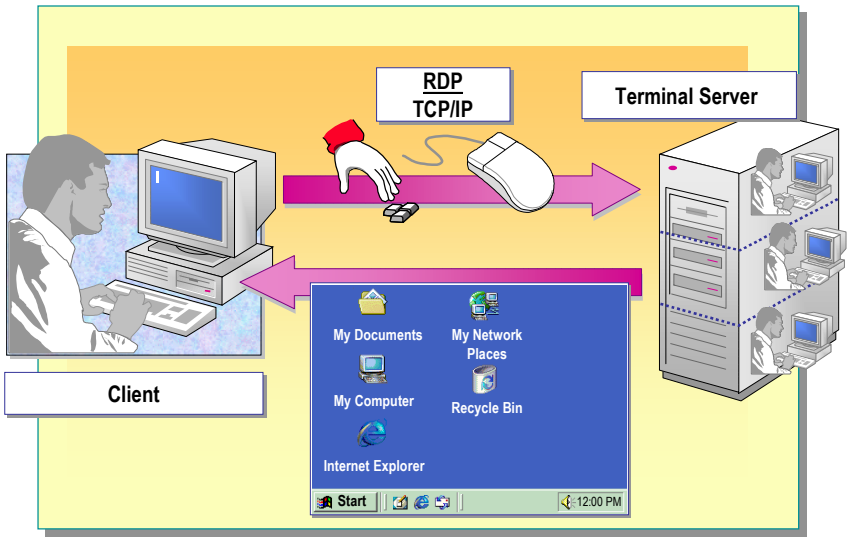
**********ILLEGAL FOR NON-TRAINER USE**********

Terminal Services enables multiuser access to Windows 2000, allowing several people to run sessions from a single computer simultaneously. Administrators can install Windows-based applications on a Terminal server and make these applications available to all clients who connect to the server. Although users may have different hardware and operating systems, the Terminal session that opens on the client desktop looks and runs the same on each device.

How Terminal Services Works

Topic Objective
To illustrate the three parts of Terminal Services.

Lead-in
Terminal Services adds multiuser system capability to a server running Windows 2000.



**********ILLEGAL FOR NON-TRAINER USE**********

Terminal Services consists of three parts:

- *Terminal server*. The server manages the computing resources for each client session and provides all users who are logged on with their own unique environment. The server receives and processes all keystrokes and mouse actions that the remote client performs, and directs all display output for both the operating system and applications to the appropriate client.

Key Point
Terminal Services requires the network protocol TCP/IP.

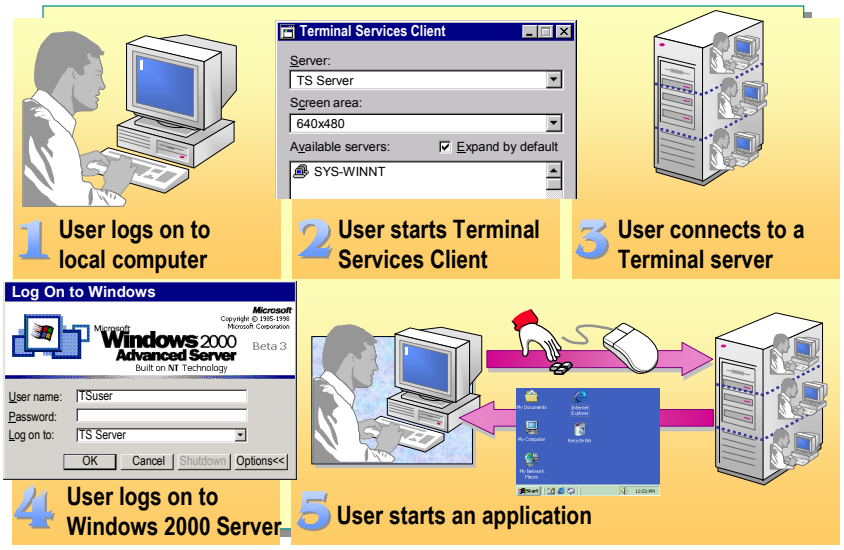
- *Client*. The Terminal session opens as a window within the local desktop environment. The remote desktop of the server runs within that window. The client computer or device requires only enough processing power to establish a connection to the server and display the user interface, which is why client computers that connect to a Terminal server are often called *thin clients*.
- *Remote Desktop Protocol (RDP)*. RDP supports communication between the client and server. RDP is optimized to display graphic interface elements to the client. RDP is an application-layer protocol that relies on Transmission Control Protocol/Internet Protocol (TCP/IP) to carry it across the network. RDP is based on the International Telecommunication Union (ITU) T.120 standard, which is a standard for international, multi-channel conferencing.

Note Many network-based applications, such as Microsoft NetMeeting®, employ the ITU T.120 standard. For more information about the T.120 standard, see the International Multimedia Teleconferencing Consortium Web site at http://www.imtc.org/

User Environments

Topic Objective
To provide an overview of the user environment.

Lead-in
The Terminal Services client environment is the same as the Windows 2000 desktop.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain that the illustration in the slide shows how Terminal Services appears to a user in a remote access scenario.

After installing the client software, users gain access to the Terminal server by opening Terminal Services Client from the **Programs** menu. When a user connects and logs on to the Terminal server, the Windows 2000 desktop appears on the client desktop. When a user starts an application, the fact that the application is not running locally is totally transparent.

To start a Terminal session, perform the following steps:

1. Log on to the client.
2. Start Terminal Services Client.
3. Select an available Terminal server, and then click **Connect**.
4. Log on to the server.

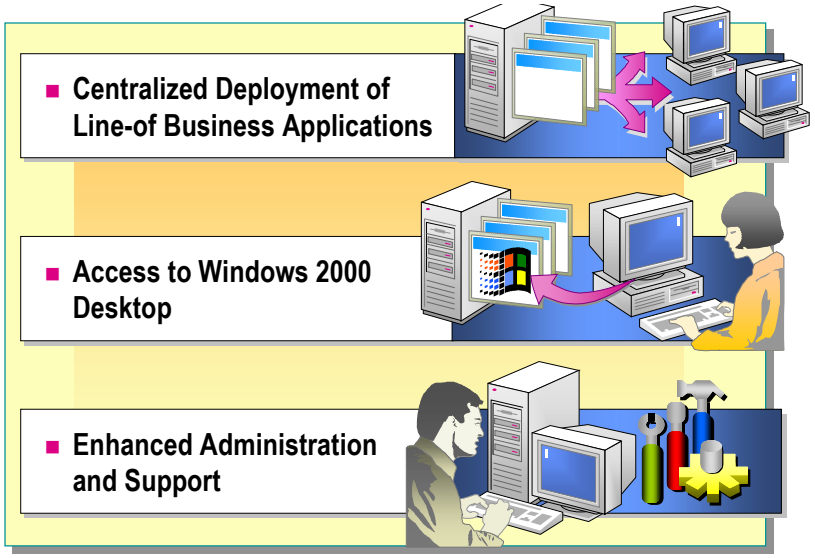
   The Windows 2000 desktop appears in a window on the client desktop.
5. In the Terminal Services window, click **Start**, point to **Programs**, and then click an application.

   The application opens in the Terminal Services window on the client desktop. All application processing takes place on the Terminal server and the server sends the display information to the client.

Features and Benefits

Topic Objective
To describe the features and benefits of Terminal Services.

Lead-in
Terminal Services provides several features and benefits to meet a broad range of business needs.



**********ILLEGAL FOR NON-TRAINER USE**********

The features of Terminal Services provide several benefits that an organization can use to deploy, access, and manage business applications.

Centralized Deployment of Line-of-Business Applications

Organizations can deploy line-of-business applications where applications run entirely on the server. Terminal Services has the lowest TCO for a single application device running a line of business application, such as a reservation system or a call center. Terminal Services provides the following benefits:

- Less expensive hardware. Employees who perform jobs that only require access to one line-of-business application can be equipped with less-expensive terminals or computers.
- Easy access to new or upgraded software. When Terminal Services is enabled on Windows 2000 Server, administrators do not have to install applications on each desktop computer. Instead, the application is installed once on the server and the clients automatically have access to the new or upgraded software package.

Access to Windows 2000 Desktop

Running productivity applications in a Terminal Services environment may affect system performance.

Terminal Services can extend Windows 2000 and Windows-based applications to a variety of clients. Terminal Services allows you to:

- Run Windows applications. Terminal Services can make Windows-based applications available to a wide range of clients. Windows-based applications can run on different operating systems and hardware with little or no modification.

Explain to students that although Terminal Services includes some features of the Citrix MetaFrame product, MetaFrame contains additional features and provides non-Windows client support.

> **Note** With the Citrix MetaFrame add-on installed, non-Windows clients can also connect to Terminal Services.

- Extend the use of older equipment. An organization can implement Terminal Services as a transitional technology to bridge older operating systems and desktop environments to Windows 2000 and 32-bit Windows-based applications.
- Replace text-based terminals. Because many Windows-based terminals can support mainframe connectivity and terminal emulation on the same device, organizations can replace text-based terminals with Windows-based terminals. Windows-based terminals enable users who work with data from mainframe systems to have access to newer Windows-based applications, such as Microsoft Outlook.
- Increased security and reliability. Because no application or user data ever resides on the client, Terminal Services can provide a more secure computing environment for sensitive data. Terminal Services also provides multilevel encryption support, which you can enable whenever there is a risk of unauthorized transmission interception on the connection between the server and the client. There are three levels of encryption available: low, medium, and high. All levels of encryption use the standard Rivest-Shamir-Adleman (RSA) RC4 encryption, which is a standard encryption for data that is sent over public networks, such as the Internet.

Enhanced Administration and Support

Key Points
Using Terminal Services for remote administration requires you to configure the server for remote administration access during installation. You will not be able to use a server configured for remote administration as an application server.

Terminal Services has several features that are useful for administration and support tasks, which can also help reduce administration and support costs:

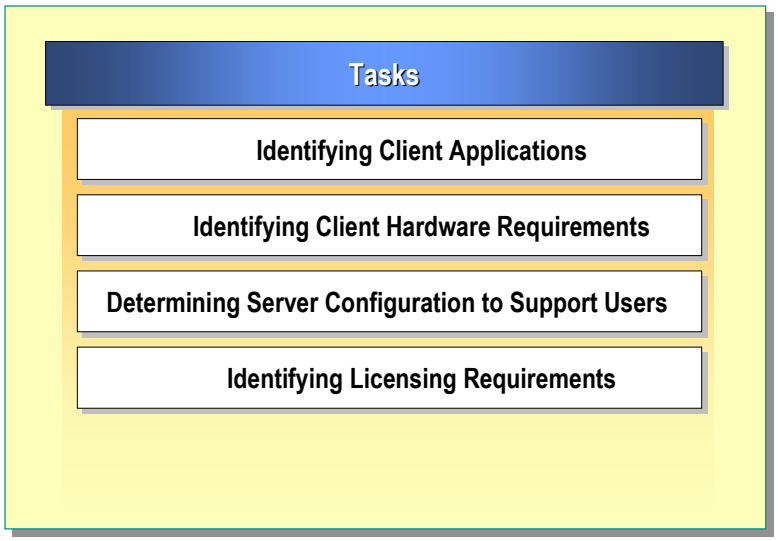
- *Remote administration.* Remote administration mode is a new feature in Terminal Services for Windows 2000. It is designed to provide operators and administrators with remote access to typical Microsoft BackOffice® servers and domain controllers. The administrator has access to the graphical user interface-based tools that are available in the Windows environment, even if he or she is not using a Windows-based computer to administer the server.
- *Remote support.* Administrators can perform remote support for a user who is logged on to a Terminal server by following the client session from another client session. Administrators or support personnel can also input keyboard and mouse actions on behalf of a user by enabling remote control. Remote control can be useful for training or supporting users on new systems or applications.

Important Using Terminal Services for remote administration requires you to configure the server for remote administration access during installation. You will not be able to use a server configured for remote administration as an application server.

◆ Planning the Installation

Topic Objective
To identify the tasks that you must perform before installing Terminal Services.

Lead-in
When planning a Terminal Services installation, you must consider the client requirements for applications and hardware, the server resources that are required to support clients, and the required licenses.



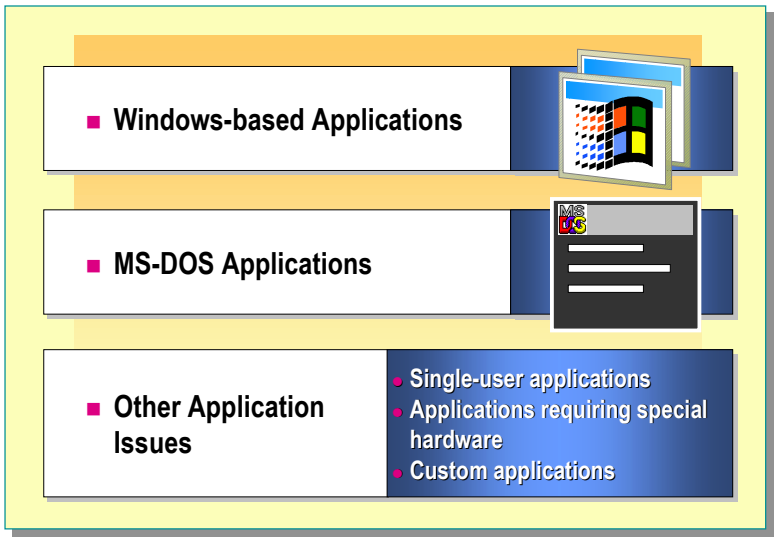
**********ILLEGAL FOR NON-TRAINER USE**********

Before you set up Terminal Services, you need to develop a plan based on the needs of your organization. Then, you can be certain that when users or administrators use Terminal Services, they will be successfully performing their tasks, be it using an application or managing user accounts.

Identifying Client Applications

Topic Objective
To identify the types of client applications that you can run in a Terminal Services environment.

Lead-in
There are issues related to client applications that should be considered when planning a Terminal Services installation.



**********ILLEGAL FOR NON-TRAINER USE**********

Explain to students that compatibility scripts are covered later in the module.

Before you install Terminal Services, identify the applications that you intend to deploy to client desktops. Most applications that run properly on Windows 2000 will also run on a Terminal server. Some applications may require minor modification, which can be performed with compatibility scripts, to run successfully in a Terminal Services environment. You should install applications on a test server before you deploy these applications in your production environment to ensure compatibility with your existing applications.

Key Points
Windows-based applications must be compatible with Windows 2000 or they will not run in a Terminal server environment.

32-bit application operate more efficiently on a Terminal server.

Windows-based Applications

Applications that you install on a Terminal server must be compatible with Windows 2000. If an application does not run on Windows 2000, it will not run in the multiuser environment of a Terminal server.

32-bit applications operate more efficiently than 16-bit applications by taking full advantage of 32-bit hardware and operating systems. Running 16-bit applications on a Terminal server can reduce the number of users that a processor can support by as much as 40 percent and increase the memory that is required per user by 50 percent.

Note Microsoft has set up a testing program with independent testing companies to assist organizations in deploying applications with Terminal Services. For more information, see http://microsoft.com/Ntserver/Terminalserver/Exec/Vendors/Resources.asp

MS-DOS Applications

Because Microsoft MS-DOS®-based applications were never designed for a multitasking environment, running MS-DOS applications on a Terminal server can slow the performance of the system with idle processes. If server performance slows significantly when users run MS-DOS applications, you may need to adjust system settings.

Caution Microsoft does not test or support any MS-DOS-based applications for use with Terminal Services. It is recommended that you replace MS-DOS-based applications with 32-bit, Windows-based applications.

Other Application Issues

Some applications have features that may prevent them from working with Terminal Services or cause them to perform poorly. The following types of applications need careful consideration before you choose to use them:

- Single-user applications

  Some applications, such as older text-based applications, were designed to run in a single-user or single-desktop environment and may not install or function properly in a Terminal Services environment.

- Applications that require special hardware

  Devices such as bar code scanners or smart card readers can be used with a Terminal Services client only if:

  - Devices are connected to the computer or terminal in such a way that the peripheral device is recognized as a keyboard-type device.
  - Connecting software and hardware supports the connection to the client.
  - A custom Virtual Channel extension can be written to support specialized hardware on the client.

- Custom applications

  Custom applications may need to be modified to run in the Terminal Services environment, which may require access to the source code. For example, you may need to modify applications that reference path names for user data files.

Identifying Client Hardware Requirements

Topic Objective
To present the system requirements for Terminal Services Client.

Lead-in
These are the system requirements to run Terminal Services Client.

Operating System	RAM	Processor	Video Card
Windows 2000	32 MB	Pentium	VGA
Windows NT versions 3.51 and 4.0	16 MB	486	VGA
Windows 98	16 MB	486	VGA
Windows 95	16 MB	386	VGA
Windows for Workgroups 3.11	16 MB	386	VGA
Windows CE, Handheld PC/PRO	Vendor	Vendor	Vendor

**********ILLEGAL FOR NON-TRAINER USE**********

Client computers that connect to a Terminal server are not required to have much processing power. Therefore, it is very easy to integrate Terminal Services into a network that has older computers and equipment.

Terminal Services Platform Support

Terminal Services supports the following platforms:

- Microsoft Windows 2000
- Microsoft Windows NT® versions 3.51 and 4.0
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows for Workgroups 3.11
- Microsoft Windows CE, Handheld PC Edition 3.0
- Windows CE, Handheld PC Professional Edition 3.0
- Windows-based Terminals

Note If you need client support for non-Windows platforms, including MS-DOS, UNIX, Macintosh, Java, and OS/2 Warp, you can use the Citrix MetaFrame add-on product. For more information, see the Citrix Web site at http://www.citrix.com/

Terminal Services Client Software

There are two versions of the Terminal Services client software:

- 16-bit Windows-based computers running Windows for Workgroups with the 32-bit TCP/IP stack installed
- 32-bit Windows-based computers running Windows 95, Windows 98, Windows NT version 3.51, Windows NT version 4.0, or Windows 2000 Professional

Manufacturers of Windows-based Terminals usually embed Terminal Services Client into the operating system.

In addition, there is Terminal Services Client support for the following devices:

- Windows CE, Handheld PC Edition 3.0 and Windows CE, Handheld PC Professional Edition 3.0
- Windows-based Terminals, Standard and Professional (based on Windows NT Embedded 4.0)

Note Download the Windows CE client for Terminal Services on the Web at http://www.microsoft.com/Windowsce/Products/Download/Term-serv.asp

The requirements for the 32-bit and 16-bit versions of Terminal Services Client are the same as the system and hardware specifications for the operating system. A network adapter and TCP/IP must also be installed on the client computer. The minimum hardware configuration for Windows CE, Handheld PC and PC Professional supports the Terminal Services Client.

Hardware Requirements

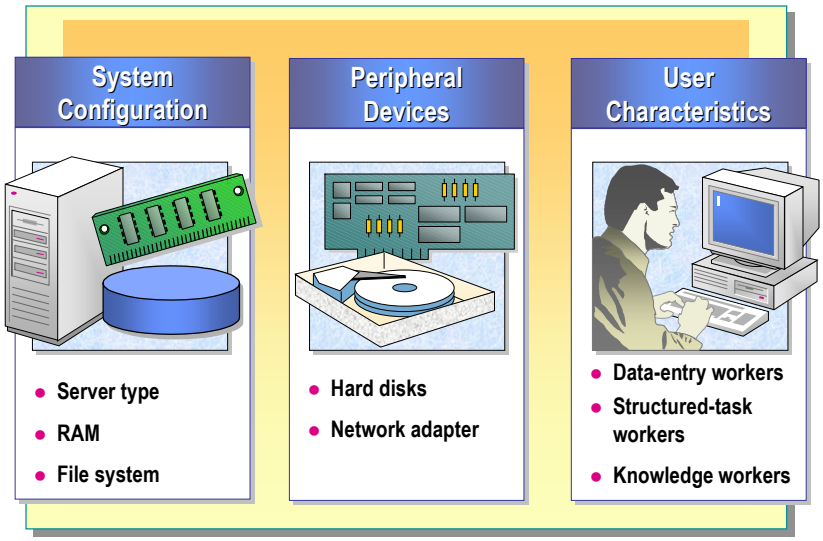
The following table describes the specific client hardware requirements for Terminal Services.

Operating System	RAM	Processor	Video Card
Windows 2000	32 megabytes (MB)	Pentium	VGA
Windows NT versions 3.51 and 4.0	16 MB	486	VGA
Windows 98	16 MB	486	VGA
Windows 95	16 MB	386	VGA
Workgroups for Windows 3.11	16 MB	386	VGA
Windows CE, Handheld PC/PRO	Vendor	Vendor	Vendor

Determining Server Configuration to Support Users

Topic Objective
To identify factors that affect server capacity in a Terminal Services environment.

Lead-in
There are three major factors that impact the performance of a Terminal server.



**********ILLEGAL FOR NON-TRAINER USE**********

Because all application processing takes place on the server, a Terminal server normally requires more server resources per user than a computer running Windows 2000 Server. Ensuring that your server can accommodate your user base is crucial. To determine how powerful a server running Terminal Services must be to support users, consider the following factors: system configuration, peripheral devices, and user characteristics.

System Configuration

Before you install Terminal Services, consider the following system recommendations:

- *Server type*. It is recommended that you install Terminal Services on a member server and not on a domain controller. Installing Terminal Services on a domain controller can hamper the performance of the server because of the additional memory, network traffic, and processor time that it requires to perform the tasks of a domain controller in a domain.

Explain that the amount of RAM is dependent upon the applications you run.

- *RAM*. Generally, a Terminal server requires an additional 4 to 10 MB of RAM for each terminal session.
- *File system*. It is recommended that you install Terminal Services on a partition that is formatted with the NTFS file system. NTFS provides security for users in a multiple session environment who access the same data structures.

Tip Terminal Services can take advantage of multiple processors. Purchasing a system that supports multiple processors, even if you initially purchase only one processor, allows you to increase the number of processors easily as your requirements grow.

Peripheral Devices

Peripheral devices can also affect the performance of a Terminal server:

- *Hard disks.* Disk speed is critical for the performance of a Terminal server. Small computer system interface (SCSI) disk drives, especially devices compatible with Fast SCSI and SCSI-2, have significantly better throughput than other types of drives. This is less important on systems that do not store user profiles and data on the Terminal server, but will still affect initial program load time. For highest disk performance, consider using a SCSI redundant array of independent disks (RAID) controller. RAID controllers automatically place data on multiple disks to increase disk performance and improve data reliability.
- *Network adapter*. A high-performance network adapter is recommended, especially if users require access to data that is stored on network servers or run client/server applications. Using multiple adapters can significantly increase network throughput, and can increase system security by separating the client access from back-end services.

Key Point
To ensure reliability, all hardware for Terminal Services must be on the HCL for Windows 2000.

Note To ensure reliability, all hardware on the server must be on the Hardware Compatibility List (HCL) for Windows 2000. A copy of the HCL is included on the Student Materials compact disc.

User Characteristics

Usage patterns of computer users can have a significant impact on the performance of Terminal Services. Microsoft performance testing simulates users in the following three categories:

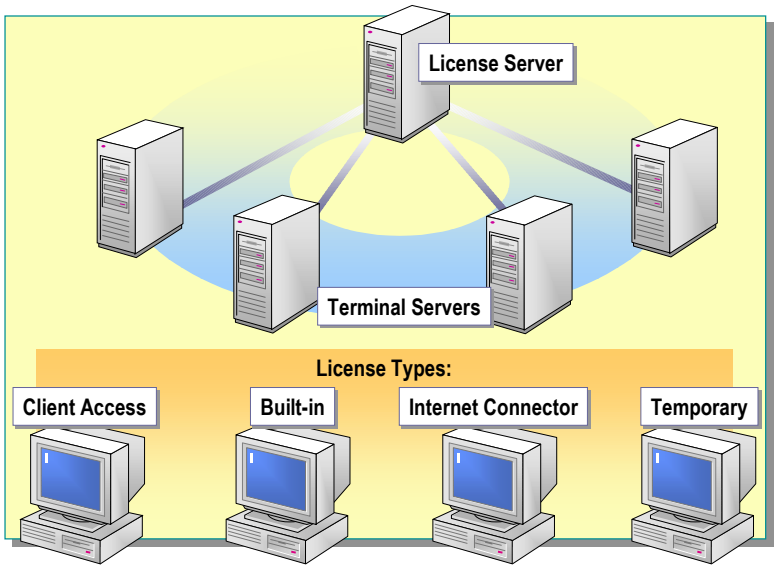
- *Data-entry worker.* These workers typically run a single application that they use for data entry (for example, business applications written in Microsoft Visual Basic®).
- *Structured-Task worker.* These workers run one or two applications at a time. Typical users run applications whose data processing demands on the system are not heavy (for example, a word processor and a browser), applications are opened and closed frequently, and typing rate is relatively high.
- *Knowledge worker*. Knowledge workers run three or more applications simultaneously, and generally leave the applications open. Knowledge workers also may run applications whose data processing demands on the system are heavy (for example, detailed queries on large databases), and typing rate is moderate.

These guidelines allow Microsoft to produce benchmarks for a variety of worker and system configurations. These are for reference only. The only way to accurately assess the performance and scaling requirements of your system is to perform accurate simulations using your work conditions and system configuration.

Identifying Licensing Requirements

Topic Objective
To illustrate Terminal Services licensing requirements.

Lead-in
There are four types of licenses required for Terminal Services clients.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Windows 2000 clients do not require CALs. Also, no CALs is required for remote administration mode.

Terminal Services requires each device that initiates a Terminal session to be licensed, either with a Windows 2000 license, or a Terminal Services Client Access License (CAL). It also requires a license server, which is a computer on which the Terminal Services Licensing service is enabled.

Guidelines for a License Server

A license server stores all Terminal Services licenses that have been installed for a group of Terminal servers and tracks the licenses that have been issued. Terminal Services Licensing allows Terminal Services to obtain and manage its CALs, thus simplifying the task of license management for the system administrator.

The Terminal Services Licensing service is a component service of Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server, and is a separate entity from Terminal Services. Terminal Services Licensing is used only with Terminal Services in Application Server mode. One license server can support several Terminal servers.

A domain, site, or workgroup hosting Terminal servers must also host a license server. In a Windows 2000 domain, the license server must be a domain controller. For a workgroup or a Windows NT 4.0 domain, the license server may be deployed on any peer server; however, Terminal Services Licensing does not manage or communicate with Terminal servers running Windows NT Server 4.0, Terminal Server Edition.

There are no hardware requirements for a license server other than those required to install Windows 2000 Server. Terminal Services Licensing requires approximately 5 MB of hard disk space per 6000 client licenses issued. Memory usage is under 10 MB of RAM, whether idle or active.

Note For more information on Terminal Services Licensing, see the white paper "Microsoft Windows 2000 Terminal Services Licensing" under **Additional Reading** on the Student Materials compact disc.

Client License Types

Briefly describe the different types of licenses.

The license server manages the following license types:

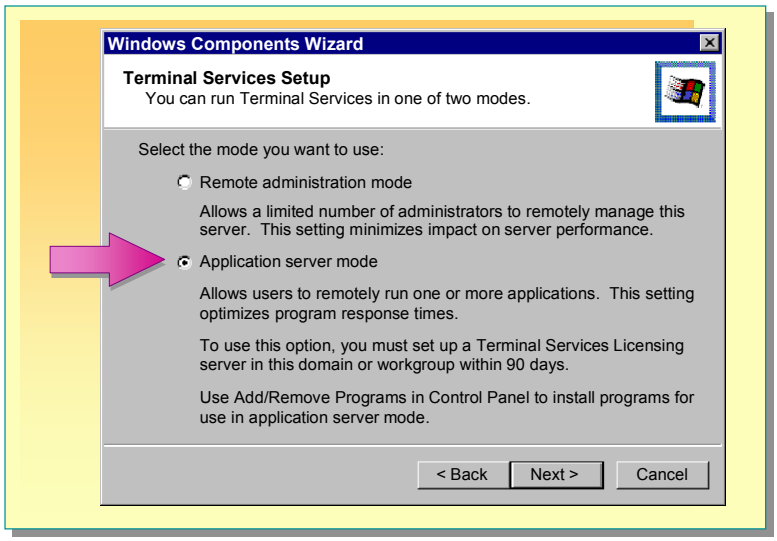
- *Terminal Services CALs.* These licenses are purchased for known, non-Windows 2000 devices connecting to a Terminal server.
- *Terminal Services Internet Connector licenses.* This license is used to allow anonymous use of a Terminal server by users across the Internet on a concurrent basis.
- *Built-in licenses.* Clients that are running Windows 2000 are automatically licensed as Terminal Services Clients.
- *Temporary licenses.* When a Terminal server requests a license and the License server has none to give, it will issue a temporary license. The license server will track the issuance and expiration of these temporary licenses.

Each client requires one of these licenses to gain access to the Terminal server. Note that this is in addition to other licenses that might be needed, such as application licenses, operating system licenses, and any Windows 2000 Server or BackOffice® CALs.

Installing Terminal Services

Topic Objective
To illustrate the Terminal Services option in the Windows Components wizard.

Lead-in
There are two options for installing Terminal Services: during Windows 2000 Setup or after Setup through **Add/Remove Programs** in Control Panel.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Demonstrate the steps for installing Terminal Services after Windows 2000 Setup.

Key Point
On installation, the Terminal server will seek a license server. Terminal Services operates for 90 days without a license server. After 90 days, the Terminal server does not allow unlicensed clients to connect unless a license server is available.

To deploy Terminal Services, you enable the Terminal Services component either during installation of Windows 2000, or afterward by using the Windows Components wizard. You may enable Terminal Services in one of two modes: Application Server or Remote Administration. Remote Administration does not require licensing and only allows two connections.

You can install Terminal Services Licensing with Terminal Services or you can install it by itself on a different computer. When you install Terminal Services licensing, you specify whether the license server will serve the domain or workgroup, or the site. Choosing enterprise licensing allows any Terminal server in the same physical site to use the license server, even across domain boundaries.

Important On installation, the Terminal server will seek a license server. Terminal Services will operate for 90 days without a license server. After 90 days, the Terminal server will not allow unlicensed clients to connect unless a license server is available to supply the client with a CAL.

Explain that if you install a license server, **Terminal Services Licensing** will be added to the **Administrative Tools** menu also.

Terminal Services adds several items to the **Administrative Tools** menu. The following table describes these additions.

Item	Description
Terminal Services Client Creator	Create floppy disks for installing Terminal Services client software.
Terminal Services Configuration	Manage Terminal Services protocol configuration and server settings.
Terminal Services Manager	Manage and monitor sessions and processes on the Terminal server.

Note By default, the Terminal Services client software installs in the *Systemroot*\System32\Clients\Tsclient folder. To prevent the client software from installing when you are deploying several Terminal servers, select **Terminal Services**, click **Details**, clear the **Client Creator Files** check box, and then click **OK**.

Configuring Terminal Services

Topic Objective
To identify the tasks required to configure Terminal Services for use in a multiuser environment.

Lead-in
There are several settings that you need to configure in Terminal Services before you install applications.

- Configuring User Access
- Installing Terminal Services Client

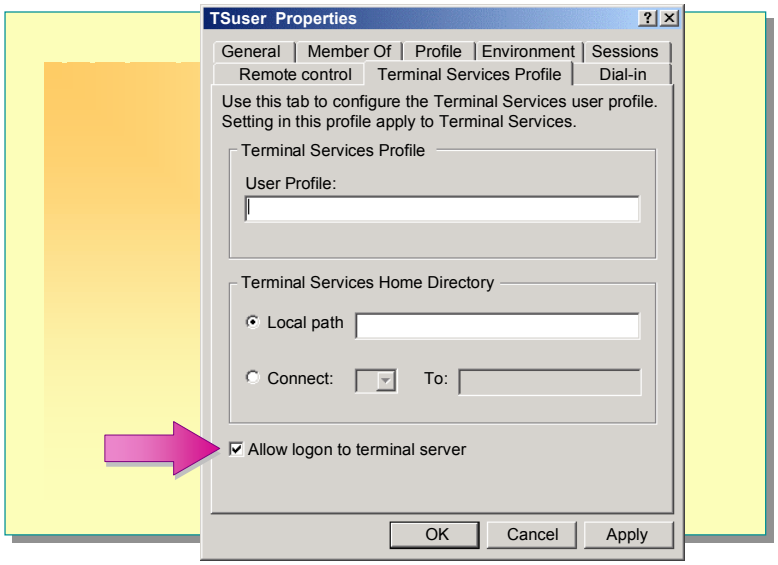
**********ILLEGAL FOR NON-TRAINER USE**********

Before you install applications on a Terminal server, you need to configure the server to allow the use of applications in a multiuser environment. You can also create user profiles and home directories for users that apply only to Terminal sessions. After configuring the server and user access, create client installation disks or download the client software across the network to install Terminal Services Client.

Configuring User Access

Topic Objective
To identify the settings for configuring user access in Terminal Services.

Lead-in
To enable user access to Terminal Services, the user account must allow the user to log on to the Terminal server.



**********ILLEGAL FOR NON-TRAINER USE**********

Users who have user accounts on the Terminal server are allowed to log on to the server by default.

To disable the logon process for a user, clear the **Allow logon to terminal server** check box on the **Terminal Services Profile** tab in the **Properties** dialog box for the user account, and then click **Apply**.

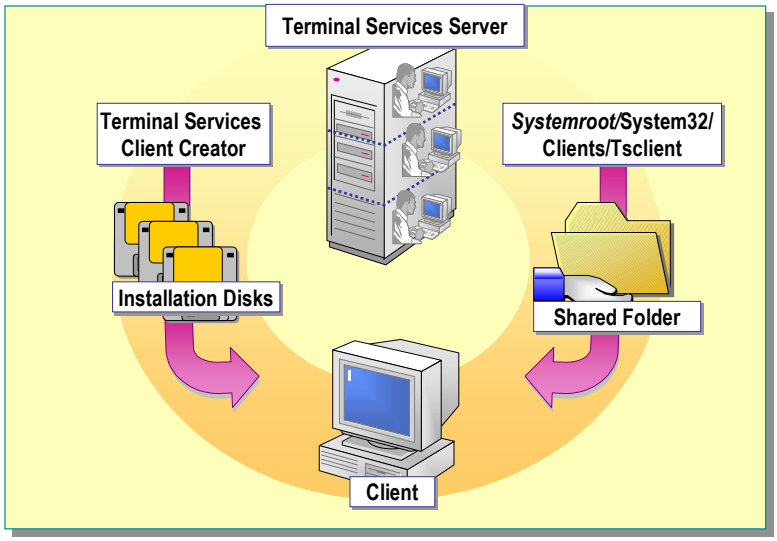
Key Points
You can specify a profile and home directory for a user account in Terminal Services that is different from the user profile in Windows 2000.

On this tab, you can also specify home directories and user profiles for users. You can assign a profile for a user that applies to Terminal sessions. This enables you to create user profiles for the Terminal Services environment. For example, you can disable screen savers and animated menu effects, which can slow performance during a Terminal session.

Installing Terminal Services Client

Topic Objective
To illustrate the two methods of installing Terminal Services Client.

Lead-in
There are two ways to install Terminal Services Client.



**********ILLEGAL FOR NON-TRAINER USE**********

There are two installation methods for the Windows-based Terminal Services Client:

- Install the client software from installation disks.
- Use a shared folder to install the client software over the network.

Creating Client Installation Disks

Windows 2000 includes Terminal Services Client Creator for creating installation disks for the client software. After you install the software on the client, the client will be able to connect to a Terminal server.

To create client installation disks, perform the following steps:

1. Open Terminal Services Client Creator.
2. Select the type of Terminal Services client software that you want to create. There are two options:
   - **Terminal Services for 16-bit windows** (requires 4 disks)
   - **Terminal Services for 32-bit *x*86 windows** (requires 2 disks)
3. Insert a disk into the destination drive.
4. After copying the files to the disks, close the **Create Installation Disk** dialog box, or click **OK** to create more disks.

Downloading Client Software over a Network

You can find the source files for Terminal Services Client in the *Systemroot*\System32\Clients\Tsclient folder on the Terminal server. The Tsclient folder contains the Net, Win16, and Win32 subfolders. To enable users to gain access to Terminal Services Client over the network and install it on their computers, share the folders for the appropriate platforms. Users can then run Setup.exe from one of the shared folders.

Installing the Terminal Services Client

Before installing Terminal Services Client, ensure that the client is properly configured and connected to the network. To install Terminal Services Client, perform the following steps:

1. Run the **Setup.exe** command.
2. Specify and confirm the user name and the organization.
3. Read and accept the license agreement.
4. Accept the default folder or specify another destination folder.
5. Specify whether to install client software for all users of the computer or for only the current user.

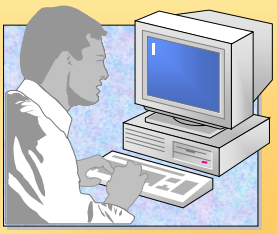
   Setup copies the appropriate files from the disk or shared folder to the specified folder on the client.

Establishing a Terminal Session

Topic Objective
To identify the procedures for establishing and ending a Terminal session.

Lead-in
After the server and client configuration is complete, a user can establish a Terminal session.

- **Connecting to a Terminal Server**
- **Using Keyboard Shortcuts in a Session**
- **Ending a Terminal Session**
  - Disconnecting from a session
  - Logging off from a session



**********ILLEGAL FOR NON-TRAINER USE**********

After the server and client configuration is complete, a user can establish a Terminal session. The user can access the network and local resources, including the hard disks and printers, from the client. When ending a session, the user can either disconnect to rejoin the session later or log off to close the session completely.

Connecting to a Terminal Server

Explain that the Client Connection Manager allows you to store configurations, and that these can be distributed as fully configured clients.

When users connect to a Terminal server, they can select options to accommodate slow networks and improve the performance of the session. To connect to a server, performs the following steps:

1. Start Terminal Services Client.

   The **Terminal Services Client** dialog box appears, which contains the options described in the following table.

For this option	Do this
Server	Enter the name of a Terminal server or a TCP/IP address.
Screen area	Select a screen resolution. This setting is not dependent on the screen resolution of the server, but is limited by the resolution of the client.
Available servers	Select a server from a list of available servers.
Low-speed connection	Click **Low-speed connection** if using a modem or for a slow network.
Cache bitmaps to disk	Click **Cache bitmaps to disk** to save desktop display elements to the local cache. This option will cause the screen to refresh from the local cache and will improve performance.

2. Click **Connect**.
3. Log on to the Terminal server.

Using Keyboard Shortcuts in a Session

The shortcut keys described in the following table are available from a Terminal Services Client for navigating through the interface.

Key combination	Description
CTRL+ALT+END	Opens the **Windows Security** dialog box.
ALT+PAGE UP	Switches between programs from left to right.
ALT+PAGE DOWN	Switches between programs from right to left.
ALT+INSERT	Cycles through the programs in the order they were started.
ALT+HOME	Displays the **Start** menu.
CTRL+ALT+BREAK	Switches the client between a window (if applicable) and a full screen.
ALT+DELETE	Displays the window's pop-up menu.
CTRL+ALT+MINUS SIGN (-)	Places a snapshot of the active window, within the client, on the Terminal server clipboard (provides the same functionality as pressing PRINT SCREEN on a local computer).
CTRL+ALT+PLUS SIGN (+)	Places a snapshot of the entire client window area on the Terminal server clipboard (provides the same functionality as pressing ALT+PRINT SCREEN on a local computer).

Ending a Terminal Session

Key Points
Disconnected sessions continue to consume resources on the server. The server can be configured for if and how long disconnected sessions are allowed, and to log off or disconnect idle clients after a period

Terminal Services provides two options for a user to end a Terminal session:

- Disconnecting from a session

  Disconnecting from a session leaves the session running on the server. The user can reconnect to the server and resume the session. For example, if a remote access dial-up connection terminates, the session stays running on the server. This allows the user to dial-in again and resume the session. Disconnected sessions continue to consume resources on the server.

  To disconnect from a session, click **Start**, click **Shut Down,** and then click **Disconnect** in the **Shut Down Windows** dialog box.

- Logging off from a session

  Logging off from a session ends the session running on the server. Any applications running within the session will be closed and unsaved data is lost.

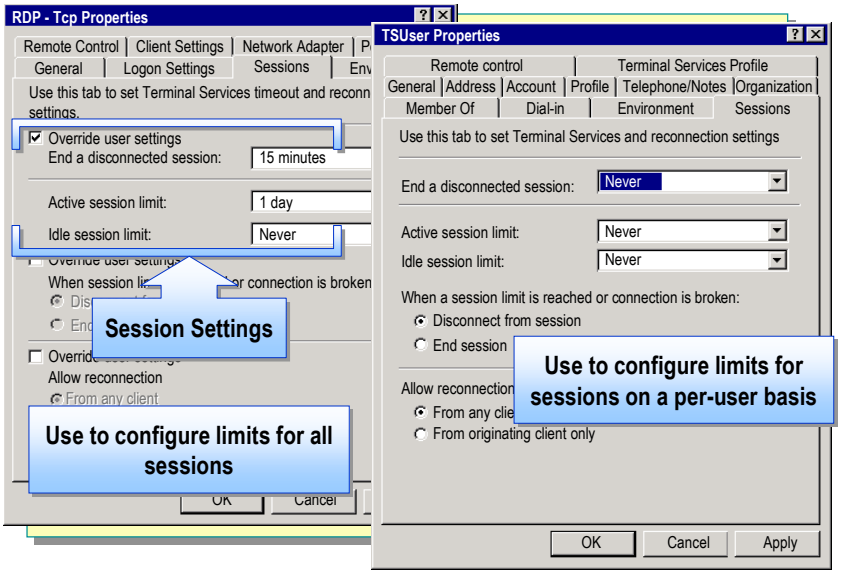
  To log off from a session, click **Start**, click **Shut Down,** and then click **Log off** in the **Shut Down Windows** dialog box.

Note It is recommended that users log off from sessions to make server memory and server resources available for other sessions.

Configuring Session Settings

Topic Objective
To identify settings to apply to Terminal sessions.

Lead-in
Setting session limits helps make system resources available for active sessions.



**********ILLEGAL FOR NON-TRAINER USE**********

To ensure that system resources are available for active Terminal sessions, you can set time limits for disconnected and idle sessions. You can configure session limits to apply to all sessions on the server or you can configure session limits on a per-user basis.

To configure limits for all sessions, use the **Sessions** tab in the **RDP-Tcp Properties** dialog box in Terminal Services Configuration.

To configure limits for individual users, use the **Sessions** tab in the **Properties** dialog box for the user.

You can specify **Never** or select increments of minutes, hours, or days for each session setting. The following table describes the settings for limiting the length of a session.

Setting	Description
End a disconnected session	Specifies the maximum duration to retain a disconnected session. When the time limit expires, the session is logged off and can no longer be resumed.
Active session limit	Specifies the maximum connection duration to retain an active session. When the time limit expires, the session is either reset or disconnected.
Idle session limit	Specifies the maximum idle time (time without connection activity) allowed before the session is disconnected or reset.

Lab A: Installing Terminal Services

Topic Objective
To introduce the lab.

Lead-in
In this lab, students will install, configure, and test Terminal Services.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install Terminal Services.
- Install Terminal Services Client software.

Prerequisites

Before working on this lab, you must have knowledge of Terminal Services concepts and operations.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.

Estimated time to complete this lab: 30 minutes

Exercise 1
Installing and Configuring Terminal Services

Scenario

You are in the process of upgrading all of your desktop computers. In the interim, you want to allow users to gain experience with the Windows 2000 user interface and take advantage of the new features in Windows 2000.

Goal

In this exercise, you will install Terminal Services and configure a local user account's properties to be allowed to use Terminal Services.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your assigned student number) with the password of **domain** and install Terminal Services and Terminal Services Licensing. Configure Terminal Services to provide application server support. Be sure to make Terminal Services available only for your domain.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** In Control Panel, double-click **Add/Remove Programs**, and then click **Add/Remove Windows Components**. **c.** In the Windows Components wizard, under **Components**, select the **Terminal Services** check box, and then click **Next**. **d.** On the **Terminal Services Setup** page, under **Select the mode you want to use**, click **Application server mode**, and then click **Next**. **e.** Verify that the Windows 2000 Advanced Server compact disc is in the CD-ROM drive. **f.** On the **Terminal Services Setup** page, click **Permissions compatible with Windows 2000 Users**, and then click **Next**. **g.** If the **Terminal Services Setup** page reappears, click **Next**. **h.** When the file copy process is complete, click **Finish**, and then close all windows. **i.** In the **System Settings Change** dialog box, click **Yes** to restart the computer.

Tasks	Detailed Steps
2. Log on to nwtraders as Admin*x* (*where x* is your assigned student number) with the password of **domain** and configure the local TSUser*x* (where *x* is your assigned student number) user account Terminal Services profile and home directory paths to use the following folders: • Profile folder: C:\Tsprofiles • Home folder: C:\Tshomes You must create the folders manually before configuring the Terminal Services profile.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** Create two folders at the root of C: Tsprofiles Tshomes **c.** Open Computer Management from the **Administrative Tools** menu. **d.** In the console tree, expand **Local Users and Groups** if necessary, click **Users**, and then in the details pane, double-click **TSUser***x* (where *x* is your assigned student number). **e.** In the **TSUser***x* **Properties** dialog box, on the **Terminal Services Profile** tab, under **Terminal Services Profile**, in the **User Profile** box, type **c:\tsprofiles** **f.** Under **Terminal Services Home Directory**, in the **Local path** box, type **c:\tshomes** **g.** Verify that the **Allow logon to terminal server** check box is selected, and then click **OK**. **h.** Close Computer Management.

Exercise 2
Installing and Testing Terminal Services Client Software

Scenario

You and a co-worker have just completed the installation of Terminal Services on your servers and have enabled a local user account on each to be able to use that service. Before announcing that Terminal Services is available, you must install the client software on the servers and ensure that the service is working properly.

Goal

In this exercise, you will install the Terminal Services Client software on your server. After your partner has completed this task, you will establish a Terminal session with your partner's computer by using the user account configured in Exercise 1.

Tasks	Detailed Steps
1. Install the Terminal Services Client software by using **Add/Remove Programs**. Use the 32-bit version available on your hard disk at: *C:\Winnt*\System32\Clients\Tsclient\Net\Win32 • Name and organization information: Student*x* (where *x* is your assigned student number)	**a.** In Control Panel, double-click **Add/Remove Programs**, and then click **Add New Programs**. **b.** Click **CD or Floppy**, and then click **Next**. **c.** In the Run Installation Program wizard, click **Browse**, navigate to the C:\Winnt\System32\Clients\Tsclient\Net\Win32 folder, double-click **Setup.exe**, and then click **Next**. **d.** In the **Terminal Services Client Setup** dialog box, click **Continue**. **e.** In the **Name and Organization Information** dialog box, in the **Name** box, type **Student***x* (where *x* is your assigned student number), and then click **OK**. **f.** In the **Confirm Name and Organization Information** dialog box, click **OK**. **g.** In the **License Agreement** message, read the agreement, and then click **I Agree**. **h.** In the **Terminal Services Client Setup** dialog box, click the large button to start installation. **i.** Click **Yes** to install the client software for all users of this computer. **j.** Click **OK**, click **Next**, and then click **Finish** to complete the setup procedure. **k.** Close all open windows.
Note: Wait for your partner to complete the previous procedure before starting this procedure.	

Tasks	Detailed Steps
2. Run the Terminal Services Client software and select your partner's computer from the list of available servers. Attempt to log on to *Server* (where *Server* is your partner's computer name) as TSUser*x* (where *x* is your student number) with the password of **domain**. Select the **Cache bitmaps to disk** check box, and use the following information to start the session: • User name: **TSUser***x* (where *x* is your partner's student number) Password: **password**	**a.** Click **Start**, point to **Programs**, point to **Terminal Services Client**, and then click **Terminal Services Client**. **b.** In the **Terminal Services Client** dialog box, under **Available servers**, click *PartnerServer* (where *PartnerServer* is your partner's assigned computer name). **c.** Select the **Cache bitmaps to disk** check box, and then click **Connect**. **d.** In the **Log On to Windows** dialog box, attempt to log on using the following information: User name: **TSUser***x* (where *x* is your student number) Password: **password** Log on to: *Server* (where *Server* is your partner's computer name) **e.** Click **OK**.

Where you successful? Why?

No. The local user account used to log on did not exist on the Terminal server you were attempting to log on to.

2. (*continued*)	**f.** In the **Log On to Windows** dialog box, attempt to log on specifying the following information: User name: **TSUser***x* (where *x* is your partner's student number) Password: **password** Log on to: *Server* (where *Server* is your partner's computer name)

Where you successful? Why?

Yes. The local user account used to log on existed on the Terminal server you were attempting to log on to.

Tasks	Detailed Steps
If your domain user account was configured to use Terminal Services, would you have been able to log on to both your Terminal server and your partner's Terminal server? Why? **Yes. You could log on to both Terminal servers because the account would be valid on any member server in the domain.**	
2. (*continued*)	**g.** Log off as the Terminal session, and then close the **Terminal Services Client** dialog box. **h.** Close any open windows, and then log off.

Installing Applications on a Terminal Server

Topic Objective
To identify the topics related to installing applications on a Terminal server.

Lead-in
There are many considerations with installing applications on a server.

- Examining Installation Options
- Running Application Compatibility Scripts

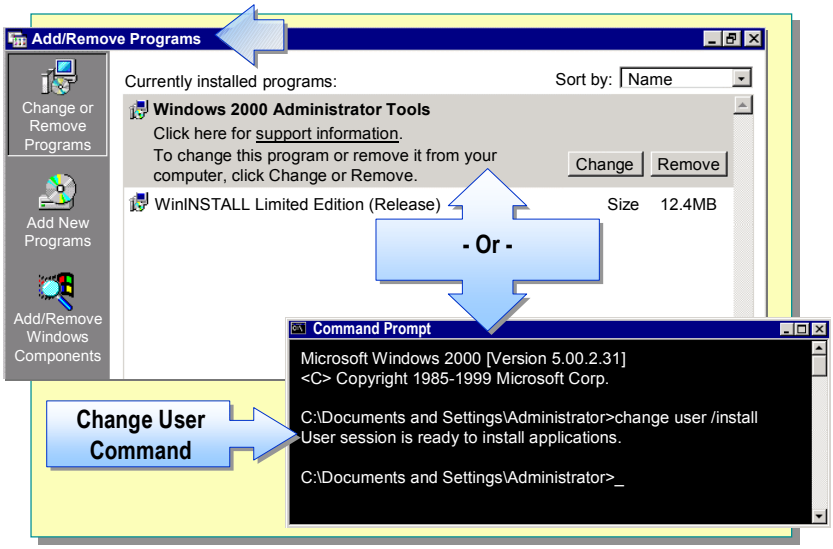
**********ILLEGAL FOR NON-TRAINER USE**********

After you have set up Terminal servers and clients, you can install applications on a Terminal server. Terminal Services clients are then able to gain access to the applications. To install an application, you must log on to the Terminal server by using an administrator account. After installation, you can run a compatibility script to modify the application to run on a Terminal server.

Examining Installation Options

Topic Objective
To identify the two methods for installing applications on a Terminal server.

Lead-in
Application files must be centrally located on the server for multiuser access.



**********ILLEGAL FOR NON-TRAINER USE**********

To make an application available for multiple users, an application setup program must copy application files to a central location on the server instead of a user's home directory.

Note For security purposes, it is recommended that you install applications on an NTFS partition.

There are two methods for installing applications on a Terminal server: **Add/Remove Programs** in Control Panel or the **change user** command at the command prompt.

Delivery Tip
Demonstrate to students how to use **Add/Remove Programs** to add applications to a Terminal server.

Using Add/Remove Programs

Add/Remove Programs, which automatically runs the **change user** command, is the preferred method for installing applications on a Terminal server.

To install an application by using **Add/Remove Programs**, perform the following steps:

1. Log on to the Terminal server as an administrator and close all applications.
2. Click **Start**, point to **Settings**, and then click **Control Panel**.
3. In Control Panel, double-click **Add/Remove Programs**.
4. Click **Add New Programs**, and then click **CD or Floppy**.
5. Browse to the setup file for the application, double-click the executable, and then click **Next**.

6. On the Change User Option page, verify that **All users begin with common application settings** is selected.
7. Install the application on a local drive as directed by the installation program.
8. Follow the instructions in the wizard to finish the installation.

Using the Change User Command

Use the **change user** command only when you are unable to install an application by using **Add/Remove Programs**.

To install an application by using the **change user** command, perform the following steps:

1. Log on to the Terminal server as an administrator and close all applications.
2. At the command prompt, type **change user /install** and then press ENTER.
3. Install the application on a local drive as directed by the installation program.
4. At the command prompt, type **change user /execute** when installation is complete.

The **change user** command performs the following actions:

Before installation, **change user /install** places the system in install mode and turns off .ini file mapping. The system then records how the Setup application programming interfaces (APIs) initially install the application.

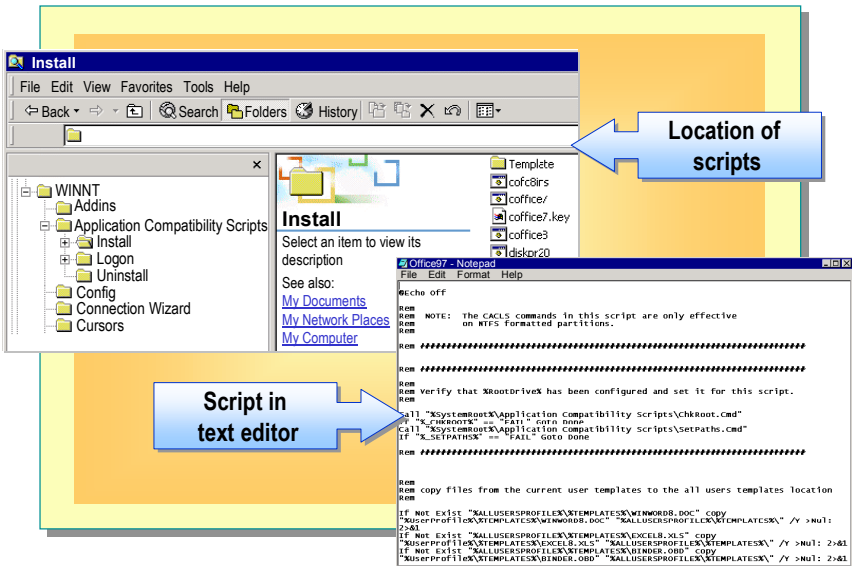
After installation, **change user /execute** returns the system to execute mode, restores .ini file mapping, and redirects user-specific data to the user's home directory. When the user opens the application, user-specific registry settings are automatically propagated as needed to the user's home directory.

Note To install Microsoft Office 2000 on a Terminal server, you must install the Terminal Services components in the Office 2000 Resource Kit. For more information, see the Microsoft Office 2000 Resource Kit Web site at http://www.microsoft.com/Office/Ork/2000/

Running Application Compatibility Scripts

Topic Objective
To illustrate the Install folder and a sample script.

Lead-in
Terminal Services includes application compatibility scripts to modify applications for use in Terminal Services.



**********ILLEGAL FOR NON-TRAINER USE**********

Terminal Services includes compatibility scripts for applications that need modification to run in a multiuser environment. For example, the Microsoft Office 97 compatibility script disables the FindFast utility and sets a number of file attributes to read-only to ensure that multiple users can open files simultaneously.

You must run compatibility scripts for applications that require modification after you install the application on the Terminal server. Scripts are located in the *Systemroot*\Application_Compatibility_Scripts\Install folder. Additional scripts may be found through the Windows Update Corporate Catalog.

To run application compatibility scripts, perform the following steps:

1. In the *Systemroot*\Application_Compatibility_Scripts\Install folder, find the script for the application that you are installing.
2. Open the file in a text editor, such as Notepad.
3. Review the script. If path names and drive letters in the files differ from those you used during application installation, edit the files to correct the path information.
4. At a command prompt, run the script for the application.

Some applications may also require logon scripts. Logon scripts set custom environmental variables for users. For example, the logon script for Microsoft Internet Explorer establishes additional support files so users can have access to personal bookmarks and address books. Logon scripts are located in the *Systemroot*\Application_Compatibility_Scripts\Install folder. Additional scripts may be found through the Windows Update Corporate Catalog.

Lab B: Installing an Application

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will install an application.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objective.

Objective

After completing this lab, you will be able to install an application that will be accessible by all Terminal Services clients.

Prerequisite

Before working on this lab, you must have familiarity with the concept of Terminal Services in Windows 2000.

Lab Setup

To complete this lab, you need the following a computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.

Estimated time to complete this lab: 45 minutes

Exercise 1
Installing an Application

Scenario

You need to have access to various Windows 2000 Support Tools utilities when troubleshooting problems at the client's desktop. To provide access to these utilities, it is necessary to install Windows 2000 Support Tools on your Terminal server and make it available for use by Terminal Services clients.

Goal

In this exercise, you will use **Add/Remove Programs** in Control Panel to install the Windows 2000 Support Tools and make it available to all Terminal Services clients. To test the installation, verify that the **Windows 2000 Support Tools** command is added to the **Start** menu.

Tasks	Detailed Steps
1. Start a Terminal session on your partner's server and use **Add/Remove Programs** to install the Windows 2000 Support Tools on your server from the \Support\Tools folder on the Windows2000 compact disc. • Installation Type: Typical	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders** **b.** On the Terminal Services Client menu, click **Terminal Services Client**. **c.** In the Terminal Services Client window, under **Available servers**, click *PartnerServer* (where *PartnerServer* is your partner's assigned server name). **d.** Select the **Cache bitmaps to disk** check box if necessary, and then click **Connect**. **e.** In the **Log On to Windows** dialog box, log on to *PartnerServer* (where *PartnerServer* is your partner's assigned server name) as Administrator with a password of **password**.
Note: Perform the following steps within the Terminal Services Client window.	

Tasks	Detailed Steps
1. (*continued*)	**f.** In Control Panel, double-click **Add/Remove Programs**. **g.** In the **Add/Remove Programs** dialog box, click **Add New Programs**, and then click **CD or Floppy**. **h.** Verify the Windows 2000 Advanced Server compact disc is in your partner's CD-ROM drive. **i.** In the **Install Program From Floppy Disk or CD-ROM** wizard, click **Next**. **j.** On the **Run Installation Program** page, click **Browse**. **k.** In the **Browse** dialog box, double-click **Support**, double-click **Tools**, double-click **Setup.exe**, and then click **Next**. **l.** On the **Welcome to the Windows 2000 Support Tools Setup Wizard** page, click **Next**. **m.** On the **User Information** page, in the **Name** box, verify that **Student***x* appears (where *x* is your assigned student number), and then click **Next**. **n.** On the **Select An Installation Type** page, verify that **Typical** is selected, and then click **Next**. **o.** On the **Begin Installation** page, click **Next**. *You will see the progress of the installation process.* **p.** On the **Completing the Windows 2000 Support Tools Setup Wizard** page, click **Finish**. **q.** On the **After Installation** page, click **Next**. **r.** On the **Finish Admin Install** page, click **Finish**. **s.** Close Add/Remove Programs, and then close Control Panel.
2. Verify that the Windows 2000 Support Tools are available.	**a.** On the **Programs** menu, verify that **Windows 2000 Support Tools** appears, and then log off the Terminal session. **b.** Close the **Terminal Services Client** dialog box, and then log off.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Introduction to Terminal Services
- Planning the Installation
- Installing Terminal Services
- Configuring Terminal Services
- Establishing a Terminal Session
- Configuring Session Settings
- Installing Applications on a Terminal Server

**********ILLEGAL FOR NON-TRAINER USE**********

1. Your management team wants to install new equipment over the next two years instead of immediately upgrading everyone's desktop computers to new, Pentium class computers. Management wants users to become familiar with a standard interface and be able to use the same suite of applications. Management also wants to reduce the need for the onsite technical support staff, but wants staff to show users how to perform tasks in the new interface. What can you tell the management team about Terminal Services that would address these issues?

   Terminal Services allows you to provide the Windows 2000 interface to users with a variety of hardware, such as Windows-based Terminals, and older operating systems, such as Windows for Workgroups. Clients running Terminal Services client software can access many Windows-based applications, and the technical support staff can use the shadowing capabilities of Terminal Services to view the Terminal sessions and guide users through performing tasks with the new Windows 2000 user interface.

2. You support a network of 100 users with computers with 386 processors, 486 processors, and Pentium processors. The management team decided to upgrade all of the computers to Pentium class computers running Windows 2000. Your management team wants to provide access to the Windows 2000 user interface now so that users are familiar with the Windows 2000 desktop environment when Windows 2000 is installed on their computers. If you decide to implement Terminal Services, what issues would be involved in planning the Terminal Services deployment?

   You want to ensure that each client meets the minimum hardware requirements, that you purchase the necessary number of Client Access Licenses, and that you identify the applications that Terminal Services supports. You would also need to ensure that the Terminal server has sufficient hardware to support the amount of users that you expect to access the server.

3. You have been asked to install Windows 2000 Terminal Services on a test computer and create the Terminal Services client software for the Information Technology (IT) staff to install on their network computers for testing purposes. How would you install Terminal Services, and what is the easiest way to provide the IT staff with the client software?

   You install Windows 2000 Terminal Services by using the Windows Components wizard. You can share the appropriate folders in *Systemroot*\System32\Clients\Tsclient on the Terminal server and allow the IT staff to connect to the shared folders to install the Terminal Services client software.

4. You have five users who are connecting to a Terminal server. All of them say that each time they connect to the server, the wallpaper and screensaver settings have changed and sometimes their data files have been deleted. How can you resolve these problems?

   You can configure the user account properties for each user to point to a different Terminal Services profile and home directory.

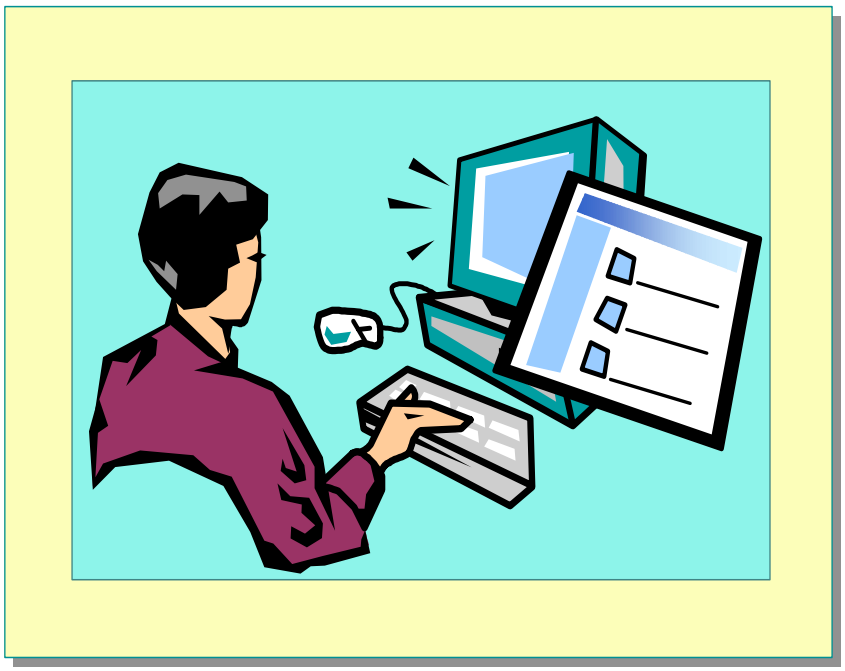
5. Your organization wants to make Office 2000 available for Terminal Service users. What do you need to do to ensure Office 2000 is installed properly?

   First, install the Terminal Services components in the Office 2000 Resource Kit, and then install Office 2000 using the transform.

Course Evaluation

Topic Objective
To direct students to a Web site to complete a course evaluation.

Lead-in
Go to the Web site listed on this page to complete a course evaluation.



**********ILLEGAL FOR NON-TRAINER USE**********

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time between now and the end of the course, please complete a course evaluation, which is available at http://www.metricsthatmatter.com/survey.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.

Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Module 15: Implementing Windows 2000 Clients

Contents

Overview	1
Deploying Windows 2000	2
Performing a Manual Network Installation	3
Customizing Installations and Upgrades by Using Switches	5
Installing Windows 2000 Using the Setup Manager Wizard	10
Using Disk Duplication	15
Lab A: Creating an Answer File for an Unattended Installation	18
Installing Windows 2000 Using RIS	23
Troubleshooting Windows 2000 Setup	28
Lab B: Running the System Preparation Tool	30
Review	34

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

Labs:
75 Minutes

This module provides students with an opportunity to learn how to perform network installations of Microsoft® Windows® 2000 and how to automate installations through the use of the Setup Manager wizard and disk duplication. They will also learn how to perform remote and customized installations of Windows 2000 and how to troubleshoot installation problems.

At the end of this module, students will be able to:

- Describe the primary deployment methods for Windows 2000.
- Perform a manual network installation of Windows 2000.
- Customize installations and upgrades using switches.
- Use the Setup Manager wizard.
- Describe the process of disk duplication.
- Perform remote installations of Windows 2000.
- Troubleshoot Windows 2000 Setup.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_15.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for the labs.

Lab A: Creating an Answer File for an Unattended Installation

► **To prepare for the lab, you must**

1. Be familiar with the Sysprep.exe.
2. Be familiar with unattended installation files (or answer files).
3. Be familiar with modifying the Windows 2000 Setup program by using switches.

Lab B: Running the System Preparation Tool

► **To prepare for the lab, you must**

1. Be familiar with the Sysprep.exe.
2. Be familiar with unattended installation files (or answer files).
3. Be familiar with disk imaging software.
4. Be familiar with modifying the Windows 2000 Setup program by using switches.

Module Strategy

Use the following strategy to present this module:

- Deploying Windows 2000

  In this topic, review the primary implementation methods for Windows 2000. Explain the advantages and disadvantages of each of these implementation methods.

- Performing a Manual Network Installation

  In this topic, discuss the basic requirements for performing a network installation of Windows 2000. Review the installation procedure with the students.

- Customizing Installations and Upgrades by Using Switches

  In this topic, discuss network installations and the switches that control the Setup program for Windows 2000 (Winnt.exe) and the upgrade program for Windows 2000 (Winnt32.exe). Explain to students that these switches are most often used in conjunction with a network installation to customize the installation based on specific networking requirements or to optimize resources.

- Installing Windows 2000 Using the Setup Manager Wizard

  In this topic, introduce the Setup Manager wizard in the Windows 2000 Resource Kit. Make sure students understand that the Setup Manager wizard is used to create and edit answer files for several different kinds of automated installations. Before class, install the Resource Kit so that you can demonstrate the Setup Manager wizard.

- Using Disk Duplication

  In this topic, describe the process of disk duplication. Explain how the Sysprep.exe file that starts the Windows 2000 System Preparation Tool fits into this process, and how you can modify the Sysprep.exe operation by using switches.

- Installing Windows 2000 Using RIS

  In this topic, describe the benefits of using Remote Installation Services (RIS). Explain how RIS is the basis of Windows 2000 Remote OS Installation, to deploy Windows 2000 Professional to client computers. Next, cover the requirements of RIS and the requirements of the client computers on which you will be installing Windows 2000. Explain that the information in this module is only an overview of the benefits and requirements of RIS. Detailed information on planning and implementing an RIS server is found in module 7, “Deploying Windows 2000 Professional by Using Remote Installation Services,” in course 1560B, *Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000*.

- Troubleshooting Windows 2000 Setup

  In this topic, list some troubleshooting suggestions for Windows 2000 setup. Describe the most common problems encountered during installation and the recommended solutions.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Lab Setup

The labs in this module require a copy of Windows 2000 Professional and Advanced Server, and enough free disk space to create a source file and install Windows 2000 Professional. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.
- Install Windows 2000 Advanced Server on a 3-gigabyte (GB) partition as a member server of the nwtraders.msft domain.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- An answer file will be created at the root of the C: partition.
- A Windows 2000 Professional source file used for installation will be created at the root of the C: partition.
- Windows 2000 Professional will be installed on the C: partition.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about automating and customizing the installation of Windows 2000 on servers and clients.

- **Deploying Windows 2000**
- **Performing a Manual Network Installation**
- **Customizing Installations and Upgrades by Using Switches**
- **Installing Windows 2000 Using the Setup Manager Wizard**
- **Using Disk Duplication**
- **Installing Windows 2000 Using RIS**
- **Troubleshooting Windows 2000 Setup**

**********ILLEGAL FOR NON-TRAINER USE**********

This module covers the primary deployment methods of Microsoft® Windows® 2000. To deploy Windows 2000, perform network installations of Windows 2000 and automate installations through the use of the Setup Manager wizard and the process of disk duplication using The System Preparation Tool (Sysprep.exe). You will also perform remote and customized installations of Windows 2000 and learn how to troubleshoot installation problems. These procedures will help you to effectively deploy both Windows 2000 Professional-based clients and Windows 2000 Server-based servers.

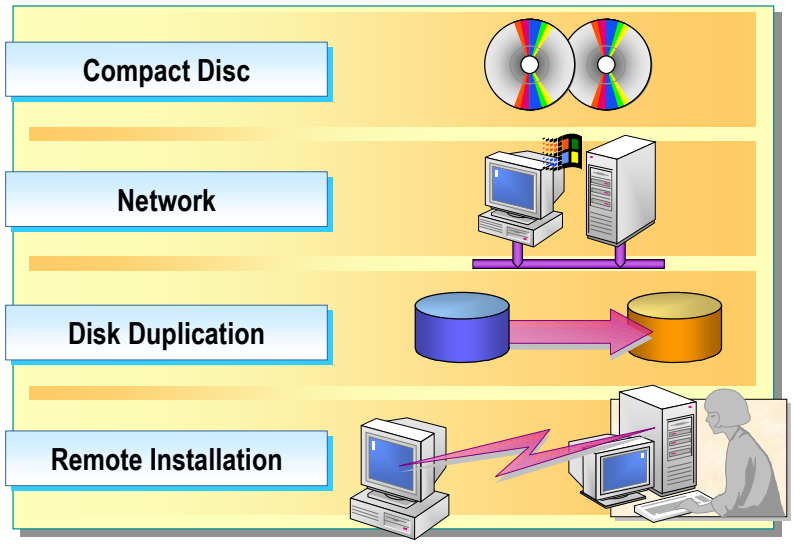
At the end of this module, you will be able to:

- Describe the primary deployment methods for Windows 2000.
- Perform a manual network installation of Windows 2000.
- Customize installations and upgrades using switches.
- Use the Setup Manager wizard.
- Describe the process of disk duplication.
- Perform a remote installation of Windows 2000.
- Troubleshoot Windows 2000 Setup.

Deploying Windows 2000

Topic Objective
To illustrate the deployment methods for Windows 2000.

Lead-in
There are different methods of deployment for Windows 2000. Choosing the appropriate method depends on your environment and the resources you have available to spend on developing deployment methods.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Point
Provide an example of when each different type of installation might be used.

One of your first tasks as a Windows 2000 support professional may be to install and configure the operating system. You can install Windows 2000 in several different ways. There are multiple options and system requirements for each method of installation. Familiarity with the available options and setup procedures will help you to deploy Windows 2000 efficiently. The following table summarizes the various methods of deployment.

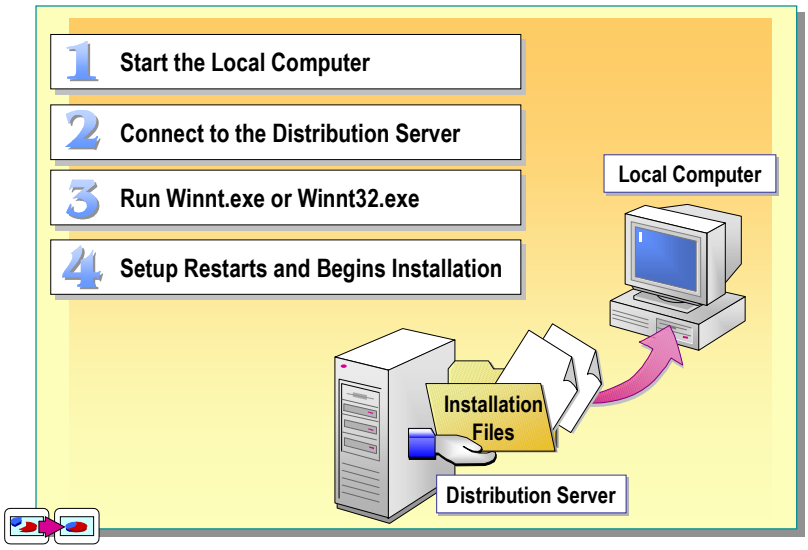
Installation method	Advantage	Disadvantage
Compact disc	Simple and quick.	Must be deployed locally from each client computer. Must have access to the compact disc.
Network	Accessible from anywhere on the network with appropriate access privileges.	Uses storage space on a server; potentially slow installation over slower wide area network (WAN) links; requires setup of network shared folder; deployed locally from each client computer.
Disk duplication	Most efficient and quickest; accessible anywhere across the network.	Uses storage space on a server; requires setup of network shared folder; uses third party software; requires advanced preparation; deployed locally from each client computer.
Remote installation	Can be deployed remotely from a server.	Requires special hardware; uses storage space on a server; requires setup of network shared folder; requires advanced preparation.

Note This module focuses on customizing Windows 2000 using alternative implementation methods. Installation of Windows 2000 using compact disc is the default deployment method. Installation by compact disc is covered in detail in module 1, "Installing or Upgrading to Windows 2000," in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Performing a Manual Network Installation

Topic Objective
To illustrate the steps for performing a manual network installation of Windows 2000.

Lead-in
Performing a manual network installation of Windows 2000 requires three components.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

Installing Windows 2000 over a network connection is relatively simple, but there are a few requirements you must meet in order for it to be successful. These additional requirements are:

- A *distribution server* that contains the installation files from the I386 folder on the Windows 2000 compact disc. A distribution server is a previously existing server on your network. You can create a shared folder on this server and copy the installation files to it from the Windows 2000 compact disc.
- Network client software that allows the local computer to connect to the distribution server.
- A minimum 685-megabyte (MB) partition (1-gigabyte [GB] partition or larger recommended) on the local computer.

Key Points
Tell the students that this method is essentially the same as installing from a compact disc, but that they need a network card configured for MS-DOS clients instead of a CD-ROM drive. Ask the students how the distribution server would be configured and how the client would connect to the distribution server.

Note You must meet the normal requirements for an installation from a compact disc in addition to the requirements listed above. For more information on compact disc installation requirements, see module 1, "Installing or Upgrading to Microsoft Windows 2000" in course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

After you meet these requirements and those for installing from a compact disc, you can perform the network installation. To initiate a network installation, perform the following tasks:

1. Start the local computer by using network client software.
2. Connect to the I386 share on the distribution server across the network.
3. Run Winnt.exe to start the Setup program. Run Winnt32.exe if you are upgrading a previous installation.

   Winnt.exe (or Winnt32.exe) creates the Win_nt.~ls temporary folder and then it copies the Windows 2000 installation files to the temporary folder.
4. Setup restarts the local computer and begins installing Windows 2000.

You can further customize the basic network installation or upgrade by using switches with the Winnt.exe or Winnt32.exe to modify the procedure.

Important Winnt.exe starts the Setup program from a command prompt. Use Winnt32.exe if you are upgrading a previous installation.

Customizing Installations and Upgrades by Using Switches

Topic Objective
To list the topics relevant to modifying installations and upgrades of Windows 2000.

Lead-in
To install Windows 2000, use the 16-bit (Winnt.exe) Setup program, for a complete installation, or use the 32-bit (Winnt32.exe) Setup program if you are performing an upgrade from within a version of Windows NT or Windows 2000.

- **Modifying the Winnt.exe Setup Program Using Switches**
- **Modifying the Winnt32.exe 32-Bit Setup Program Using Switches**

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Make sure students understand that switches are used to modify the default behavior of the Setup program, but are not necessary unless you need to modify the default installation behavior.

Use the Setup program (Winnt.exe) to install Windows 2000 from any 16-bit operating system, such as Microsoft MS-DOS®.

Use the upgrade program for Windows 2000 (Winnt32.exe) to upgrade existing installations of Microsoft Windows NT® to Windows 2000 from *within* a 32-bit operating system. You can also upgrade existing installations of Windows 2000.

Modify the Setup program (Winnt.exe or Winnt32.exe) to customize your installation through the use of *switches*. Switches are customization options you add to a command to alter the command's performance.

Modifying the Winnt.exe Setup Program Using Switches

Topic Objective
To identify the switches that you use with Winnt.exe to control the Setup process.

Lead-in
You can change the server-based installation process by using the Winnt.exe switches.

Use This Switch	To
/a	Enable accessibility options
/e[*:command]*	Execute a command before the final phase of Setup
/udf:id *[,UDB_file]*	Modify the answer file
/r[*:folder]*	Specify an optional folder to be installed
/rx[*:folder]*	Specify an optional folder to be copied
/s[*:source_path]*	Specify the location of Windows 2000 installation files
/t[*:temp_drive]*	Specify a drive for installation
/u[*:answer_file]*	Perform unattended installation with an answer file

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Provide a scenario and give an example of the switches that would be used to support that scenario. Quiz the students with simple scenarios and ask them what switches would be used to accomplish the task.

To use a switch, type the **winnt.exe** command, followed by a space, followed by the switch. Some switches require additional information after the command. For example, to force Windows 2000 to install on drive D instead of drive C, type the **winnt /t:d** command at a command prompt. In this example, **/t** is a switch which specifies the location of the temp folder. **:d** indicates that you want the default temp folder located on drive D rather than on drive C, which is the default location.

To see a list of possible switches and their syntax, at the command prompt, type the following command:

```
Winnt.exe /?
```

Automating Installation with Switches

Switches are also useful for automating an installation, allowing you to start an installation and then leave it to focus on a different task. For example, you can use the **/u:answerfile /s** switch to automatically provide answers to questions that occur during installation. The **/s** switch points to the location of the source files contained in the I386 folder, as shown in the following example.

```
c:\winnt.exe /u:answer file /s
```

- winnt.exe = command that starts the Setup program.
- /**u** = switch that specifies an answer file.
- :answerfile = name and location of the answer file.
- **/s** = switch that points to the source files in the I386 folder.

The following table describes all of the switches that you can use with Winnt.exe to modify Setup.

Switch	Description
/a	Enables accessibility options.
/e[:*command*]	Executes a command at the end of GUI mode Setup.
/udf:*id* [,*UDB_file*]	Indicates an identifier (*id*) that Setup uses to specify how a Uniqueness Database (UDB) file modifies an answer file (see **/u**). The **/udf** parameter overrides values in the answer file, and the identifier determines which values in the UDB file are used. If no *UDB_file* is specified, Setup prompts you to insert a disk that contains the $Unique$.udb file.
/r[:*folder*]	Specifies an optional folder to be installed. The folder remains after Setup finishes.
/rx[:*folder*]	Specifies an optional folder to be copied. The folder is deleted after Setup finishes.
/s[:*source_path*]	Specifies the location of the Windows 2000 installation files. The source path must be a full path in one of the following formats: *x:\[path]* -Or- *\\server\shared_folder[\path]*. The default is the current folder.
/t[:*temp_drive*]	Directs Setup to place temporary files on the specified drive and to install Windows 2000 on that drive. If you do not specify a drive, Setup uses the partition with the most available space.
/u[:*answer_file*]	Performs an unattended installation by using an optional script file. Unattended installations also require use of the **/s** switch. Unattended installations are discussed later in this module.

Initiating a Customized Network Installation

To initiate a customized network installation, perform the following tasks:

1. Start the local computer by using network client software.
2. Connect to the I368 share on the distribution server across the network.
3. At a command prompt, type the following command followed by the particular set of switches you wish to use to customize the installation.

   ```
   x:\winnt.exe /switch /switch
   ```

4. Setup begins the installation process with the parameters defined by the switches used.

Modifying the Winnt32.exe 32-Bit Setup Program Using Switches

Topic Objective
To describe the some of the switches that you use with Winnt32.exe to control the setup process.

Lead-in
You can change the server-based upgrade process by using Winnt32.exe switches.

Use This Switch	To
/copydir:[*foldername*]	Create an additional folder (or use **/copysource**)
/cmd:[*command_line*]	Execute a command before the final phase of Setup
/cmdcons	Install files for the repair and recovery console
/debug [*level*] [:*file*]	Create a debug log at a given level
/s:[*source_path*]	Specify the location of Windows 2000 installation files
/syspart:[*drive*]	Copy Setup files to a drive that you can move
/tempdrive:[*drive*]	Specify a drive for installation
/unattend [*num:file*]	Perform unattended installation with optional answer file
/udf:*id* [,*udf_file*]	Install by using a Uniqueness Database File

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Explain that this command is used when upgrading an existing installation. Explain to the students that Winnt32.exe is more efficient than Winnt.exe because it is a 32-bit, multi-threaded application. Explain the significance of how it performs during the installation.

Using switches, you can modify an upgrade by changing how Winnt32.exe runs the Setup program. The following table describes the switches that you can use with Winnt32.exe to modify the upgrade installation process.

Switch	Description
/copydir: [*folder_name*]	Creates an additional folder within the systemroot folder (the folder that contains the Windows 2000 system files). For example, if your source folder contains a folder called My_drivers, type **/copydir:My_drivers** to copy the My_drivers folder to your systemroot folder. In this example, Windows 2000 would create the C:\Winnt\My_drivers folder. Use the **/copydir** switch to create as many additional folders as you like.
/cmd: [*command_line*]	Executes a command before the final phase of Setup.
/cmdcons	Copies additional files to the hard disk that are necessary to load a command-line interface for repair and recovery purposes.
/debug[*level*] [:*file_name*]	Creates a debug log at the specified level. By default, it creates C:\Winnt32.log at level 2 (the warning level).
/s:[*source_path*]	Specifies the location of the Windows 2000 installation files. To simultaneously copy files from multiple paths, use a separate **/s** switch for each source path.
/syspart: [*drive_letter*]	Copies Setup startup files to a hard disk and marks the drive as active. You can then install the drive in another computer. When you start that computer, Setup starts at the next phase. Use of **/syspart** requires use of the **/tempdrive** switch.

(continued)

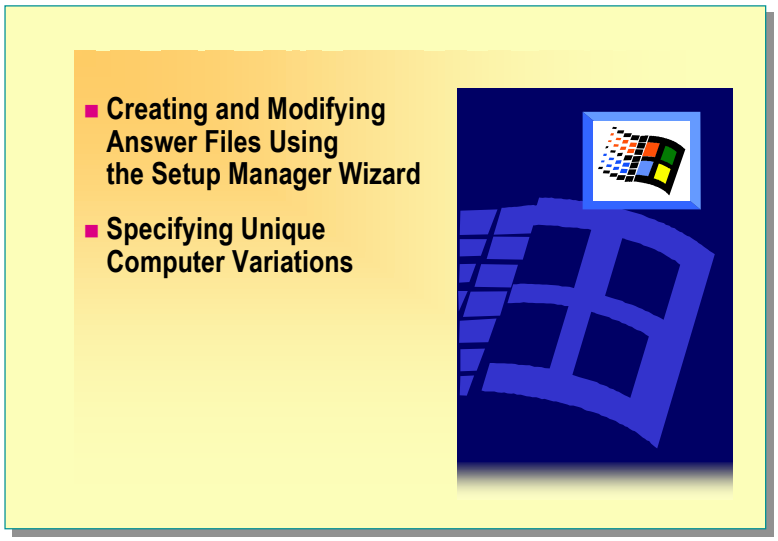
Switch	Description
/tempdrive: [*drive_letter*]	Places temporary files on the specified drive and installs Windows 2000 on that drive.
/unattend [*number*] [:*answer_file*]	Performs an unattended installation. The answer file provides your custom specifications to Setup. If you do not specify an answer file, all user settings are taken from the previous installation. You can specify the number of seconds between the time that Setup finishes copying the files and when it restarts. You can specify the number of seconds only on a computer running Windows 2000 that is upgrading to a newer version of Windows 2000.
/udf:*id* [,*udf_file*]	Indicates an identifier (*id*) that Setup uses to specify how a Uniqueness Database File (UDF) modifies an answer file. The .udf file overrides values in the answer file, and the identifier determines which values in the .udf file are used. For example, **/udf:Remote_user,Our_company.udf** overrides settings that are specified for the Remote_user identifier in the Our_company.udf file. If you do not specify a .udf file, Setup prompts the user to insert a disk that contains the $Unique$.udf file. UDFs are discussed later in this module.

For a complete listing of all switches for the Winnt32.exe utility, refer to Windows 2000 Help. Search for winnt32.

Installing Windows 2000 Using the Setup Manager Wizard

Topic Objective
To list topics relevant to creating answer files with the Setup Manager wizard.

Lead-in
When you need to install Windows 2000 on computers with varying configurations, the Setup Manager wizard provides automation with increased flexibility.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Emphasize the advantages of using the Setup Manager wizard to create installation scripts for automated installations.

Key Point
Explain that using the Setup Manager wizard doesn't necessarily speed up the process of creating script files, but it does simplify the process.

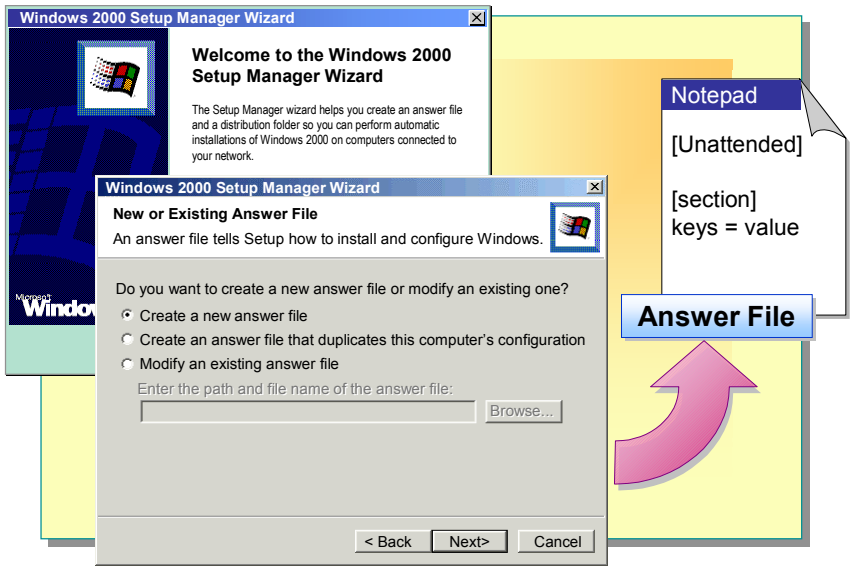
The Setup Manager wizard automates installations of Windows 2000 and provides flexibility when you need to install Windows 2000 on network computers with varying configurations. The Setup Manager wizard allows you to quickly customize an installation of Windows 2000. It also simplifies the process of specifying unique variations in the installation process.

Knowing how to use the Setup Manager wizard enables you to perform customized installations that meet the specific hardware and network requirements of your organization's workstations and servers.

Creating and Modifying Answer Files Using the Setup Manager Wizard

Topic Objective
To illustrate the interface of the Setup Manager wizard.

Lead-in
The Setup Manager wizard makes it easy to create the answer files that are necessary for scripted installations.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Start the Setup Manager wizard and show students the **New or Existing Answer File** and **Product to Install** pages in order to illustrate the available options.

Answer files are text files that automatically provide answers to some or all of the prompts users normally receive during Setup. Use answer files to specify the variations in the hardware configurations of the computers that you are installing.

Using Answer Files and UDF Files

You can use two types of files together to help automate the remote or unattended installation process: answer files and .udf files. The answer file specifies general information that is consistent to all of the computers you are installing. As such, the answer file provides the answers a user would answer during the Installation wizard. The .udf file contains information that is unique to a specific computer on the network, such as the network settings and computer name. Both files together allow a successful remote or unattended installation.

Delivery Tip
Suggest to the students that they create several different answer files and use all of the options they can to create the most complex answer file possible. Then, review the answer file to better understand how it works.

Starting the Setup Manager Wizard

The Setup Manager wizard, Setupmgr.exe is one of the files found in the Deploy.cab file located in the \Support\Tools folder on the Windows 2000 compact disc. Access the Setupmgr.exe file directly from the Windows 2000 compact disc, or extract it to your hard drive.

To extract the Setupmgr.exe file and additional deployment files from the Deploy.cab file, perform the following steps:

1. Create a folder at the root of C.
2. Select all files in the Deploy.cab file, right-click any selected file, and then click **Extract**. The Setup Manager wizard extracts all the selected files.
3. In the **Browse for Folder** dialog box, select the folder you created, and then click **OK**.

Creating Or Modifying Answer Files

To start the Setup Manager wizard, double-click **Setupmgr.exe** in the folder where you extracted the Deploy.cab files. When you start the Setup Manager wizard, it presents you with three options:

- Create a new answer file.
- Create an answer file that duplicates the current computer's configuration.
- Modify an existing answer file.

If you create a new answer file, you need to choose the type of answer file to create. The Setup Manager wizard can create an answer file for:

- A Windows 2000 unattended installation.
- A Sysprep install.
- Remote Installation Services.

Key Points
The Setup Manager wizard can be used to create answer files for all of the following: Windows 2000 Professional-based clients and the Windows 2000 Server-based servers, remote installations, disk duplication (using the System Preparation Tool), and installations over a network or from a compact disc.

If you choose to create an answer file for a Windows 2000 Unattended Installation and you select either **Windows 2000 Professional** or **Windows 2000 Server**, the Setup Manager wizard asks you to specify a level of user interaction. You can set the level of user interaction to one of five levels: Provide defaults, Fully automated, Hide pages, Read only, and GUI attend.

If you are installing Windows 2000 from a compact disc, you can create an answer file that is designed to automatically provide answers for the installation. In the Setup Manager wizard, specify the installation folder, select **No, this answer file will be used to install from a CD** on the **Distribution Folder** page, and then save the file to disk as Winnt.sif. The Setup program will search for this file on the disk when you start the computer from the CD-ROM drive.

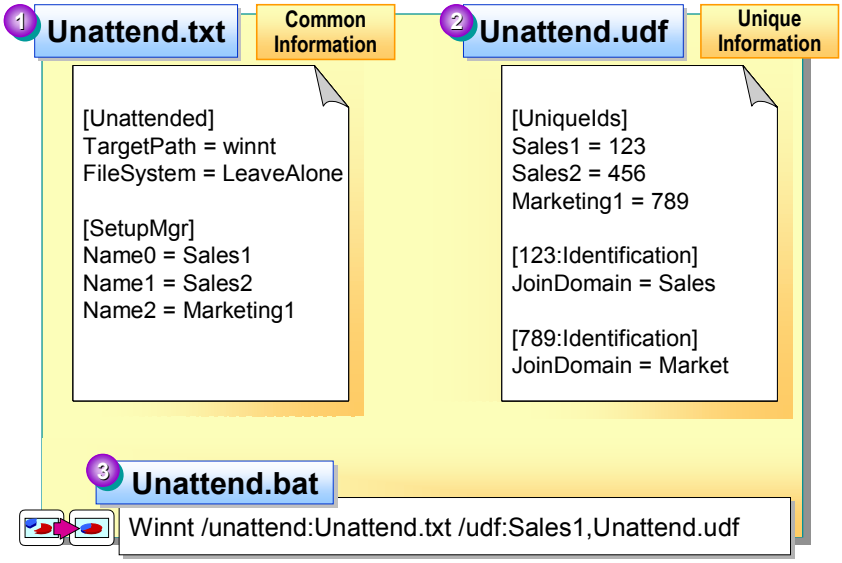
Note You can also automate installation of a domain controller. For more information on automating installations of domain controllers, see module 3, "Creating a Windows 2000 Domain," in course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services,* and the white paper, *Automating the Windows 2000 Upgrade*, located under **Additional Reading** on the Student Materials compact disc.

In addition, you can find more information on the syntax of answer files in the Unattend.doc file under **Additional Reading** on the Web page on the Student Materials compact disc. Although it is possible to create answer files by using a simple text editor, such as Notepad, it is recommended that you use the Setup Manager wizard to reduce errors in syntax.

Specifying Unique Computer Variations

Topic Objective
To illustrate the use of a UDF.

Lead-in
You use the UDFs that the Setup Manager wizard creates to specify configuration variables that must be unique to each computer in the network.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

Key Points
Explain how a single unattended answer file can be used to install the operating system on several computers if a .udf file is also created. Provide a scenario to explain the purpose of the unique database files.

As an administrator, you create unattended files to install a computer. If you need to install more than a few computers, you can specify unique information for each computer on the network. Some configuration variables, such as the computer name, must be unique to each computer on the network. To completely automate installation, you can either create a different answer file for each computer, or you can use .udf files.

One .udf file can have several computer names, and each computer name can specify a slightly different configuration. In the **winnt.exe** or **winnt32.exe** command, a computer name is specified, and any values specified in the section of the .udf file that is associated with that name overrides the values in the Unattend.txt file.

If you specify multiple computer names in the Setup Manager wizard, it creates the files described in the following table.

Default file name	Purpose
Unattend.txt	Specifies setup information that is common to all computers and the computer names of the individual computers.
Unattend.udf	Matches the computer names that are specified in Unattend.txt to security identifiers (SIDs). You specify the UDF that Setup will use for an installation by using the **/udf** switch for Winnt.exe or Winnt32.exe.
Unattend.bat	Provides an example batch file that illustrates the use of the **/u** and **/unattend** switches for Winnt.exe and Winnt32.exe. This batch file may need to be modified to work in your network.

Important SIDs are unique numbers that identify user, group, and computer accounts. Every account on your network is issued a unique SID when it is first created. Internal processes in Windows 2000 refer to an account's SID rather than the user or group name. If you create an account, delete it, and then create another account with the same user name, the new one will not have the rights or permissions previously granted to the old account because they have different SID numbers.

Using Disk Duplication

Topic Objective
To list topics that are relevant to automating Windows 2000 installations by using disk duplication.

Lead-in
When you must install Windows 2000 on several identical computers, using a disk duplication tool will save you time and effort.

- Examining the Disk Duplication Process
- Using the System Preparation Tool

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Describe the situations in which disk duplication is the most efficient method of installing Windows 2000. Explain that Windows 2000 does not provide a disk duplication utility, but several third party products are available. Cite examples.

As your network environment grows, you will be faced with a growing need to automate as many processes and tasks as possible. As administration becomes more complex, you need to increase your efficiency and maximize your resources. One way to maximize your resources and time is to use disk duplication to deploy operating systems and applications quickly and accurately to client computers.

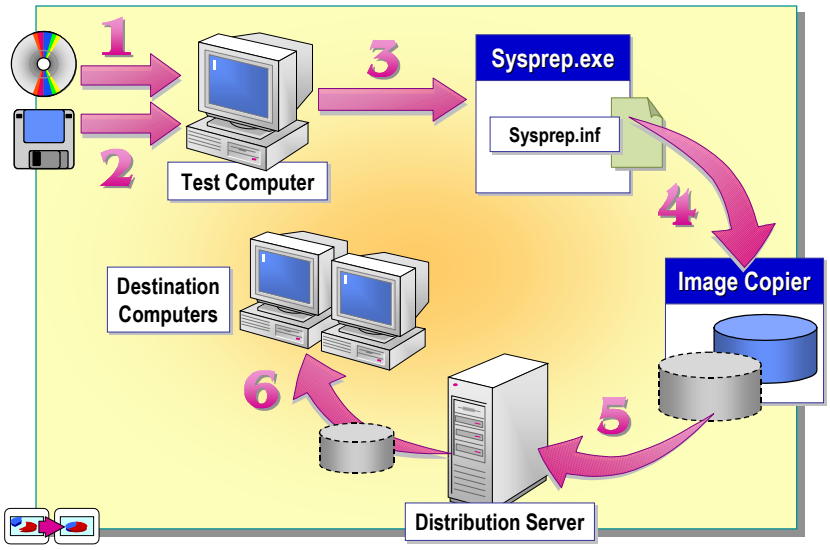
Disk duplication is the most efficient installation method to use when you need to install Windows 2000 on large numbers of computers. By creating a disk image of a Windows 2000 installation, and then copying that image onto multiple destination computers, you save time in the deployment of Windows 2000. This method also creates a convenient baseline installation that you can use to fix a computer that is experiencing problems.

One of the tools that you use for disk duplication is the System Preparation Tool (Sysprep.exe) that is included on the in Windows 2000 compact disc. Knowing how to use the System Preparation Tool can help technical support professionals to prepare master disk images for efficient mass installations.

Examining the Disk Duplication Process

Topic Objective
To illustrate the disk duplication process.

Lead-in
To install Windows 2000 by using disk duplication, configure a test computer and duplicate an image of the disk through a server.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

Key Point
Explain that the purpose of Sysprep.exe is to remove unique information (for example, SIDs) from the computer to prepare it for imagining. This new feature reduces the amount of work necessary when using a third party utility to re-image the computer.

To properly manage a large disk duplication effort, it is important to understand the sequence of steps involved in disk duplication or disk imaging. The disk duplication process consists of the following tasks:

1. Install and configure Windows 2000 on a test computer.
2. Install and configure applications on the test computer.
3. Run Sysprep.exe on the test computer.

   Optionally, run the Setup Manager wizard to create another type of answer file called Sysprep.inf. Sysprep.inf provides answers to a minimal Setup program that runs on the destination computers. You can also use this file to specify customized drivers. The Setup Manager wizard creates a Sysprep folder at the root of the drive image and places Sysprep.inf in this folder. This is where the Mini-Setup program checks for Sysprep.inf when Windows 2000 is being installed.
4. Restart the test computer, and then run a third party disk image copying tool to create a master disk image.
5. Save the new disk image on a shared folder or compact disc.
6. Copy this image to the multiple destination computers.
7. Start the destination computers and complete the installation process.

When users start the destination computers, the Mini-Setup program prompts the user for computer-specific variables, such as the administrator password for the computer and the computer name. If you provided a Sysprep.inf file, the Mini-Setup program is bypassed and the computer loads Windows 2000 without user intervention.

Using the System Preparation Tool

Topic Objective
To explain the use of the various switches that are available with Sysprep.exe.

Lead-in
Familiarity with the features of the System Preparation Tool, the program for preparing a disk for duplication, will help you use this tool effectively.

Use This Switch	To
-quiet	Run with no user interaction
-pnp	Force Setup to detect Plug and Play devices on the destination computers
-reboot	Restart the test computer
-nosidgen	Forbid SID generation on the destination computers

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
While explaining these switches to the students, ask them to give a scenario of when each might be useful.

The System Preparation Tool in Windows 2000 prepares the master computer's hard disk for duplication. One of the primary functions of the System Preparation Tool is to delete SIDs and all other user-specific or computer-specific information. Windows 2000 generates new SIDs when the destination computers are restarted after loading the disk image.

The following table describes the switches that you can use to customize the operation of Sysprep.exe.

Switch	Description
-quiet	Runs with no user interaction
-pnp	Forces Setup to detect Plug and Play devices on destination computers
-reboot	Restarts the test computer instead of shutting down the computer
-nosidgen	Does not regenerate SIDs on destination computers

Lab A: Creating an Answer File for an Unattended Installation

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will use the Setup Manager wizard to create an unattended installation script.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objective.

Objective

After completing this lab, you will be able to create a Unattended.txt file to install Microsoft Windows 2000 Advanced Server.

Prerequisites

Before working on this lab, you must have:

- An understanding of the Windows 2000 installation process.
- An understanding of modifying the installation process using switches.
- An understanding of the System Preparation Tool (Sysprep.exe).

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a member server of the nwtraders.msft domain.
- The Windows 2000 Advanced Server compact disc.
- A floppy disk.

Estimated time to complete this lab: 30 minutes

Exercise 1
Creating an Answer File

Scenario

Your accounting manager purchased a new computer for home use. The manager wants you to install Windows 2000 Professional on the computer and she wants to use her personal copy of the Microsoft Windows 2000 Professional compact disc that she has at home. You have verified that the computer can be started from the CD-ROM drive. You want to automate the installation of Windows 2000 Professional so that the accounting manager can do the installation herself at home. Since she will be installing from compact disc, you decide to create an unattended installation file for her. She can then use her Microsoft Windows 2000 Professional compact disc and the unattended installation file that you created to install Windows 2000 Professional.

Goal

In this exercise, you will copy the files from the Microsoft Windows 2000 Professional compact disc \\Support\Tools\Deploy folder to a folder you create named C:\Deploy. From the C:\Deploy folder, you will run Setupmgr.exe and create an unattended installation file for a Windows 2000 Professional installation.

Tasks	Detailed Steps
1. Log on to nwtraders.msft as Admin*x* (where *x* is your student number) with a password of **password**. Create a folder named C:\Deploy and then copy the files from the Microsoft Windows 2000 Professional compact disc \Support\Tools\Deploy folder to the C:\Deploy folder.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your student number) Password: **domain** Log on to: **nwtraders** **b.** In Windows Explorer, at the root of drive C create a folder named Deploy. **c.** Insert the Microsoft Windows 2000 Professional compact disc into the CD-ROM drive and then close the Microsoft Windows 2000 CD window. **d.** In Windows Explorer, in the console tree, expand the CD-ROM drive. **e.** Expand **Support**, and then click **Tools**. **f.** In the details pane, double-click **Deploy**. **g.** On the menu bar, click **Edit**, and then click **Select All**. **h.** On the menu bar, click **File**, and then click **Extract**. **i.** In the **Browse for Folder** dialog box, expand **Local Disk (C:)**, click **Deploy**, and then click **OK**.
2. From the Deploy folder, run Setupmgr.exe and begin creating an Unattended Installation file completing the portion of the file for the text-based portion of the installation.	**a.** In the console tree, expand **Local Disk (C:)**, and then click **Deploy**. **b.** In the details pane, double-click **Setupmgr**. **c.** On the **Welcome to the Windows 2000 Setup Manager Wizard** page, click **Next**. **d.** On the **New or Existing Answer File** page, verify that **Create a new answer file** is selected, and then click **Next**.

Tasks	Detailed Steps
2. (*continued*)	**e.** On the **Product to Install** page, verify that **Windows 2000 Unattended Installation** is selected, and then click **Next**. **f.** On the **Platform** page, verify that **Windows 2000 Professional** is selected, and then click **Next**.

What are the user interaction levels that you can choose from?

Provide Defaults

Fully Automated

Hide Pages

Read Only

GUI attended

2. (*continued*)	**g.** On the **User Interaction Level** page, click **Fully automated**, and then click **Next**. **h.** On the **License Agreement** page, select the **I accept the terms of the License Agreement** check box, and then click **Next**. **i.** On the **Customize the Software** page, enter the following information, and then click **Next**: Name: **Accounting Manager** Organization: **Northwind Traders**
3. Finish creating an Unattended Installation file completing the portion of the file for the GUI-based portion of the installation and save it to disk.	**a.** On the **Computer Names** page, type **Computer***x* (where *x* is your assigned student number), click **Add**, and then click **Next**. **b.** On the **Administrator Password** page, verify that **Use the following Administrator password (127 characters maximum)** is selected, enter the following information, and then click **Next**: Password: **password** Confirm password: **password** **c.** On the **Display Settings** page, select the following information, and then click **Next**: Colors: **256 Colors** Screen Area: **800 by 600** Refresh frequency: **Use Windows default** **d.** Insert detailed step description here. Use ENTER to add additional steps. Do not use the TAB key.

Important: In a production environment, the information on the **Display Settings** page should reflect capabilities of the target computer's hardware.

Tasks	Detailed Steps
3. (*continued*)	**e.** On the **Network Settings** page, verify that **Typical settings** is selected, and then click **Next**. **f.** On the **Workgroup or Domain** page, verify that **Workgroup** is selected, and then click **Next**. **g.** On the **Time Zone** page, select the time zone for your location, and then click **Next**. **h.** On the **Additional Settings** page, click **No, do not edit the additional settings**, and then click **Next**. **i.** On the **Distribution Folder** page, click **No, this answer file will be used to install from a CD**, and then click **Next**. **j.** Insert a blank, formatted disk into the floppy disk drive. **k.** On the **Answer File Name** page, in the **Location and file name** box, type **A:\Winnt.sif** and then click **Next**. **l.** On the **Completing the Setup Manager Wizard** page, click **Finish**.

In addition to the disk that you just created, what else is needed to install Windows 2000 Professional on the target computer in this scenario?

A Microsoft Windows 2000 Professional compact disc.

4. Verify that the files you just created contain the information needed to perform an unattended installation.	**a.** In Windows Explorer, in the console tree, click **3 ½ Floppy (A:)**. **b.** In the details pane, right-click **winnt.bat**, and then click **Edit**. *A Notepad window opens displaying the contents of the winnt.bat file.*

What answer file will be used to perform the unattended installation? Where will the installation process go to retrieve the source files?

Winnt.sif. The source files will be retrieved from d:\i386.

4. (*continued*)	**c.** Close the Notepad window. **d.** In Windows Explorer, in the details pane, right-click **winnt.sif**, and then click **Open With**.

Tasks	Detailed Steps
4. (*continued*)	**e.** In the Open With dialog box, click **Notepad**, clear the **Always use this program to open these files** check box, and then click **OK**. *A Notepad window opens displaying the contents of the winnt.sif file.* **f.** **Maximize** the Notepad window.

Do the software customization, administrative password, and display settings you configured using the Setup Manager wizard appear to be correct? How can you tell?

Yes. Under [UserData] Accounting Manager and Northwind Traders appears, under [GuiUnattended] the Administrator account is set to password, and under [Display] the settings indicate a screen resolution of 800 by 600 with 256 colors.

4. (*continued*)	**g.** Close any open windows, remove the floppy, and then log off.

Installing Windows 2000 Using RIS

Topic Objective
To list the topics that relate to deploying Windows 2000 by using Remote OS Installation.

Lead-in
The most efficient method of deploying Windows 2000 is to use remote installation.

- **Installing and Configuring Remote Installation Services**
- **Configuring Clients for Remote Installation**

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tips
Discuss the advantages and disadvantages of remote installation over other methods of installation.

Emphasize that detailed information regarding deployments with Remote OS Installation is outside the scope of this course.

The Remote OS Installation feature in Windows 2000 uses the Remote Installation Service (RIS) to perform an automated installation of Windows 2000 Professional on a local computer. RIS reduces the time that administrators must spend personally visiting each computer on a network, thereby reducing the cost of deploying Windows 2000 Professional-based clients. RIS allows both technical staff and users to install the operating system on a computer.

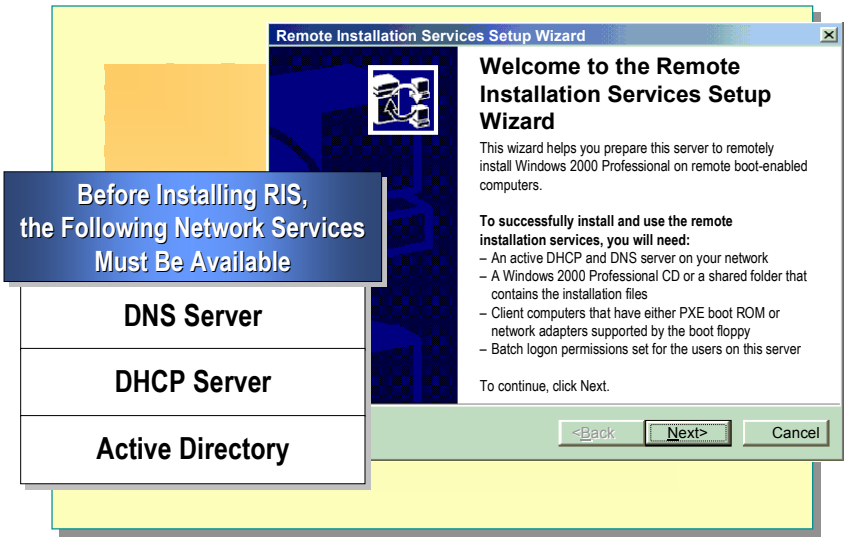
Note Perform remote installations of Windows 2000 Professional if you have a Windows 2000-based server infrastructure in place and the computers in your network support remote startup.

Important This module only provides an overview of Remote OS Installation. For more detailed information on Remote OS Installation, see module 13, "Deploying Windows 2000 Professional by Using RIS," in course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*, and the white paper, *Remote OS Installation*, located under **Additional Reading** on the Student Materials compact disc.

Installing and Configuring Remote Installation Services

Topic Objective
To illustrate the Remote Installation Services Setup wizard.

Lead-in
The first step in a remote installation deployment is to install and configure the required services.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Inform students that this is meant to be an overview of the technology and that more information is available in course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Install RIS through **Add/Remove Programs**, and then configure RIS by using the Remote Installation Services Setup wizard.

RIS Requirements

Use either a member server or domain controller for the RIS server. The following network services do not need to be installed on the same computer as RIS, but they must be available somewhere on the network.

Network service	RIS function
Domain Name System (DNS) Server service	RIS relies on the DNS Server service for locating both the directory service and client computer accounts.
Dynamic Host Configuration Protocol (DHCP) Server service	Client computers that can start from the network receive an Internet Protocol (IP) address from the DHCP Server service.
Active Directory™ directory service	RIS relies on Active Directory in Windows 2000 for locating existing client computers and existing RIS servers.

Delivery Tip
Emphasize the requirements for installation of an RIS server. Discuss the minimum requirements of the entire network, including services available, number of server computers, and client computer configurations.

You must install RIS (included on the Windows 2000 Server compact disc) on a volume that is shared over the network. This shared volume must meet the following criteria:

- It cannot be the same disk that is running Windows 2000 Server.
- It must have enough free space on the disk to hold the RIS software and the various Windows 2000 Professional-based client disk images.
- It must be formatted with the NTFS file system.

Using the Remote Installation Services Setup Wizard

When your network meets the prerequisites for RIS, you can run the Remote Installation Services Setup wizard, which does the following:

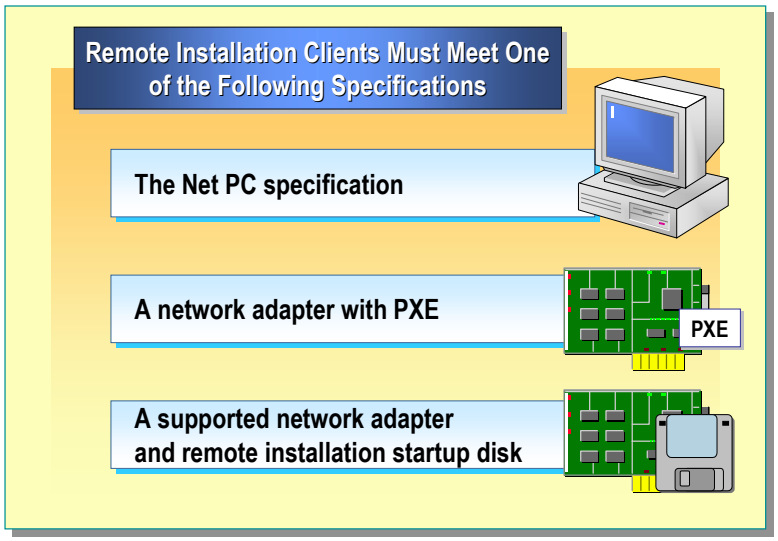
- Installs the RIS software
- Copies the Windows 2000 Professional installation files to the server
- Adds .sif files (a variation of an Unattend.txt file)
- Configures the Client Installation wizard pages that appears during a remote installation

To run the Remote Installation Services Setup wizard, add RIS by using the Windows Components Setup wizard in **Add/Remove Programs**. After you add the components, click **Start**, click **Run**, type **risetup** in the **Open** box, and then click **OK**.

Configuring Clients for Remote Installation

Topic Objective
To illustrate the three client configurations that RIS supports.

Lead-in
Client computers that support remote installation will support the Net PC specifications, have a network adapter capable of starting remotely, or use a remote installation Startup disk.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Students might have trouble understanding what a Network PC is and what the specifications are. Have information available to answer any questions the students might have about Network PCs.

Client computers that support remote installation must have one of the following configurations:

- A configuration meeting the Network PC (Net PC) specification.
- A network adapter with a Pre-Boot Execution Environment (PXE) boot ROM or basic input/output system (BIOS) support for starting from the PXE boot ROM. A PXE boot ROM network adapter is a network card with a specialized chip that allows you to remotely start the computer with the network card. The PXE is an industry standard network card that can request an IP address. If no operating system exists, the card starts up a minimal operating system that contacts a RIS server and then brings up a menu so that the user can select the operating system that they want.
- A supported network adapter and a remote installation Startup disk.

Configuring a Net PC

A Net PC has the ability to perform a network startup, manage upgrades, and prevent users from changing the hardware or operating system configuration. There is a specification that defines the requirements for a Net PC. Additional requirements for the Net PC specification include:

- A network adapter set as the primary startup device within the system BIOS.

Note For more information on Group Policy, see module 4, "Implementing Group Policy," in course 2154A, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

- Users must have permission to create computer accounts in the domain that they are joining. The domain is specified on the **Advanced Settings** tab of the **Properties** dialog box for the RIS server.

Note For more information on the Net PC specification, see http://www.microsoft.com/hwdev/netpc.htm or see the white paper, *Remote OS Installation*, located under **Additional Reading** on the Student Materials compact disc.

Configuring Other Computers

Computers that do not directly meet the Net PC specification can still interact with the RIS server. To enable remote installation on a computer that does not meet the Net PC specification, perform the following tasks:

1. Install a network adapter with a PXE boot ROM.
2. Set the BIOS to start from the PXE boot ROM.
3. Set the user rights and permissions as previously listed for Net PC.

The remote installation Startup disk can be used with computers that do not contain a remote boot-enabled ROM on the network card. The Startup disk is designed to simulate the PXE boot process for computers that lack a supported PXE-compliant network interface card.

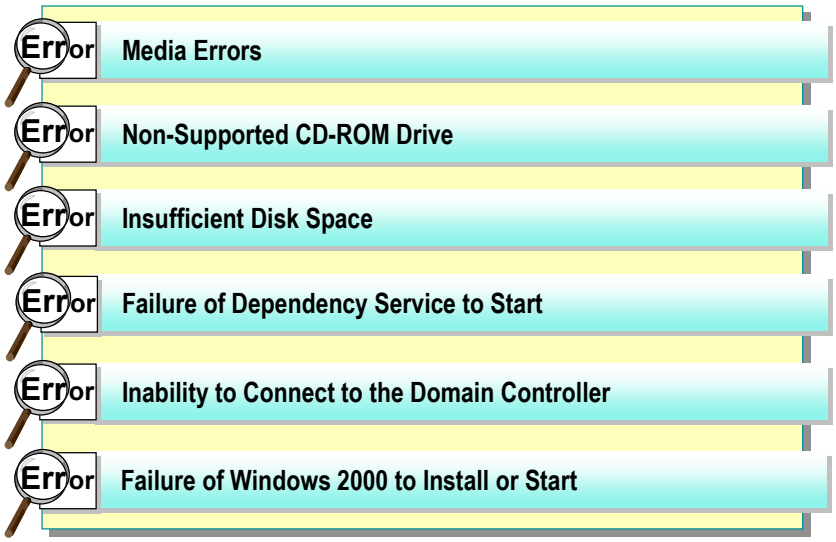
If the network adapter is not equipped with a PXE boot ROM, or the BIOS does not permit the computer to start from the network adapter, create a remote installation Startup disk by running the Windows 2000 Remote Boot Disk Generator or Rbfg.exe. The Rbfg.exe file is found in the \RemoteInstall\Admin folder on the RIS server. You also need to set the user rights and permissions as previously listed for Net PC.

Note RIS does not currently support portable computers.

Troubleshooting Windows 2000 Setup

Topic Objective
To list common installation problems and their solutions.

Lead-in
Sometimes a problem may arise during installation. Knowing the solutions to the most common problems will help you solve the majority of installation issues.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
If time allows, provide a troubleshooting scenario and have students explain how they would troubleshoot the problem.

The following table lists common setup errors that occur during Windows 2000 Setup, and it provides solutions.

Problem	Solution
Media errors	Use a different compact disc. To request a replacement compact disc, contact Microsoft or a local Microsoft vendor.
Non-supported CD-ROM drive	Use Startup disks. Replace the CD-ROM drive with one that is supported. Try another method of installing Windows 2000, such as installing over the network, and then add the CD-ROM driver.
Insufficient disk space	Use the Setup program to create a partition that uses existing free space on the hard disk. You can also delete and create partitions as necessary to create a partition that is large enough for installation.
Failure of dependency service to start	In the Windows 2000 Setup wizard, return to the **Network Settings** page and verify that you installed the correct protocol and network adapter. Verify that the network adapter has the proper configuration settings, such as transceiver type, and that the local computer name is unique on the network.

(*continued*)

Problem	Solution
Inability to connect to the domain controller	Verify that the domain name is correct. Verify that the domain controller and the server running the DNS Server service are both online. If you cannot locate a domain controller, join a workgroup, and then join the domain after installation. Verify that the network adapter and protocol settings are set correctly. If you are reinstalling Windows 2000 and are using the same computer name, delete and then recreate the computer account.
Failure of Windows 2000 to install or start	Verify that Windows 2000 is detecting all of the hardware and that all of the hardware is on the Hardware Compatibility List (HCL).

Lab B: Running the System Preparation Tool

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will configure a reference computer for imaging, use Sysprep.exe, and complete the installation of the System Preparation Tool.

**********ILLEGAL FOR NON-TRAINER USE**********

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure a reference computer for imaging.
- Remove all configuration settings that are unique to a computer by using Sysprep.exe.
- Complete the installation of the System Preparation Tool.

Prerequisites

Before working on this lab, you must have:

- Knowledge of the Setup Manager wizard.
- Knowledge of the steps involved in preparing a computer for imaging.

Lab Setup

To complete this lab you need:

- A computer running Microsoft Windows 2000 Advanced Server.
- A Microsoft Windows 2000 Advanced Server compact disc.

Estimated time to complete this lab: 45 minutes

Exercise 1
Preparing a Computer to be Imaged

Scenario

You are the network administrator for your company. The company has just received a shipment of ten identical computers that will be used as servers. You need to install Windows 2000 Advanced Server on all ten computers and configure each computer with the same set of applications. You have decided the process will be as follows:

1. Use Windows 2000 Setup Manager wizard to create a Sysprep install file.
2. Run Sysprep on the test computer to remove any personal settings.
3. Image the computer.
4. Copy the image to all ten computers.
5. Complete the installation on each computer.

You do not have imaging software at this time, so you will test all steps in the above process, except steps 3 and 4. You will simply restart the test computer after step 2 and complete the installation process in step 5.

Goal

In this exercise you will configure a computer to be imaged using the Windows 2000 Setup Manager wizard. After preparing the computer to be imaged you will restart the computer and finish the installation process.

Tasks	Detailed Steps
1. Log on to nwtraders as Admin*x* (where *x* is your student number) with a password of **domain**.	**a.** Log on using the following information: User name: **Admin***x* (where *x* is your assigned student number) Password: **domain** Log on to: **nwtraders**
2. Begin the creation of a Sysprep.inf file using Setupmgr.exe. Specify the following: • create a new answer file • fully automate the installation • customize the software using the name IT Department and organization Northwind Traders	**a.** Click **Start**, and then click **Run**. **b.** In the **Open** box, type **C:\deploy\setupmgr.exe** and then click **OK**. **c.** On the **Welcome to the Windows 2000 Setup Manager Wizard** page, click **Next**. **d.** On the **New or Existing Answer File** page, verify that **Create a new answer file** is selected, and then click **Next**. **e.** On the **Product to Install** page, click **Sysprep Install**, and then click **Next**. **f.** On the **Platform** page, click **Windows 2000 Server**, and then click **Next**. **g.** On the **License Agreement** page, click **Yes, fully automate the installation**, and then click **Next**. **h.** On the **Customize the Software** page, enter the following information, and then click **Next**: Name: **IT Department** Organization: **Northwind Traders**

(*continued*)

Tasks	Detailed Steps
3. Continue the creation of the Sysprep.inf file using the following information: • licensing is per seat • computer name is ITComputer*x* (where *x* is your assigned student number) • password is **password** • system automatically logs you on as Administrator • display set to 800 by 600 pixels, and 256 colors • use the typical network settings • join the nwtraders domain using the admin*x* (where *x* is your assigned student number) user account with a password of **domain**.	**a.** On the **Licensing Mode** page, click **Per seat**, and then click **Next**. **b.** On the **Computer Name** page, type **ITComputer***x* (where *x* is your assigned student number), and then click **Next**. **c.** On the **Administrator Password** page, verify that **Use the following Administrator password (127 characters maximum)** is selected, and then enter the following information: Password: **password** Confirm password: **password** **d.** On the **Administrator Password** page, select the **When the computer starts, automatically log on as Administrator** check box, and then click **Next**. **e.** On the **Display Settings** page, select the following information, and then click **Next**: Colors: **256 Colors** Screen Area: **800 by 600** Refresh frequency: **Use Windows default** **f.** On the **Network Settings** page, verify that **Typical settings** is selected, and then click **Next**. **g.** On the **Workgroup or Domain** page, select **Windows Server domain**, and then in the **Windows Server domain** box, type **nwtraders.msft** **h.** Select the **Create a computer account in the domain** check box, enter the following information, and then click **Next**: User name: **Admin***x* (where *x* is your student number) Password: **domain** Confirm password: **domain** **i.** On the **Time Zone** page, select the time zone for you location, and then click **Next**. **j.** On the **Additional Settings** page, click **No, do not edit the additional settings**, and then click **Next**. **k.** On the **Sysprep Folder** page, verify that **Yes, create or modify the Sysprep folder** is selected, and then click **Next**. **l.** On the **Additional Commands** page, click **Next** to accept the default settings. **m.** On the **OEM Branding** page, click **Next** to accept the default settings. **n.** On the **Additional Files or Folders** page, click **Next** to accept the default settings. *The **Please specify the location of the file 'sysprep.exe'** message appears, prompting you to point the Windows 2000 Setup Manager Wizard to the Sysprep.exe file found in the C:\Deploy folder.* **o.** In the **Windows 2000 Setup Manager Wizard** message box click **OK**.

Tasks	Detailed Steps
3. (*continued*)	**p.** In the **Open** dialog box, in the **File name** box, verify that **sysprep** appears, and then click **Open**. **q.** **On** the **OEM Duplicator String** page, click **Next** to accept the defaults. **r.** On the **Answer File Name** page, in the **Location and file name** box, type **C:\sysprep\sysprep.inf** and then click **Next**. **s.** On the **Completing the Windows 2000 Setup Manager Wizard** page, verify the following paths and files, and then click **Finish**: C:\Sysprep\Sysprep.inf C:\\Sysprep\Sysprep.bat
4. Identify any applications that are already installed, and then run Sysprep.exe.	**a.** In Control Panel, double-click **Add/Remove Programs**. **b.** In Add/Remove Programs, note any installed software, and then click **Close**.
Note: After Sysprep.exe has been run and the computer has been rebuilt, you will again note any installed software.	
4. (*continued*)	**c.** Close Control Panel. **d.** Click **Start**, and then click **Run**. **e.** In the **Open** box, type **C:\sysprep\sysprep.exe** and then click **OK**. **f.** In the **Windows 2000 System Preparation Tool** dialog box, click **OK**. **g.** Turn off the computer when Windows 2000 indicates that it is safe to do so.
Note: If you were going to image this computer, you would start the computer using an imaging software startup disk, and then image the computer. The image could be copied to a network-shared folder if the startup disk provides for network connectivity. Depending on the computer being imaged, the image file can be quite large.	
5. Restart the computer and complete the Windows 2000 Setup Manager wizard.	**a.** Start the computer. **b.** When the **Your Product Key** page appears, enter the product key supplied by the instructor, and then click **Next**. *The **Licensing Modes** page displays momentarily; it will disappear after a few moments. The **Workgroup or Computer Domain** page also appears momentarily; it will disappear after a few moments.* **c.** When the **Completing the Windows 2000 Setup Wizard** page appears, click **Finish**.
Note: The computer will restart and log the Administrator account on to the local computer.	
5. (*continued*)	**d.** In Control Panel, double-click **Add/Remove Programs**. **e.** In Add/Remove Programs, note that the installed software matches the software installed before you ran Sysprep, and then click **Close**. **f.** Close Control Panel, and then log off.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Deploying Windows 2000
- Performing a Manual Network Installation
- Customizing Installations and Upgrades by Using Switches
- Installing Windows 2000 Using the Setup Manager Wizard
- Using Disk Duplication
- Installing Windows 2000 Using RIS
- Troubleshooting Windows 2000 Setup

**********ILLEGAL FOR NON-TRAINER USE**********

1. You need to upgrade 34 workstations on your network running Windows NT 4.0 to Windows 2000. You want to create a distribution server, and then run the upgrade from the workstations. What steps would you take to accomplish this?

   Copy the I386 folder to the distribution server, share it, and then have users connect to the shared folder and run Winnt32.exe.

2. Your company is upgrading the hardware in 15 servers running Windows NT 4.0, but is keeping the same hard drives. Without waiting for the new hardware, how can you begin the upgrade?

   Run the upgrade program, Winnt32.exe, with the /syspart:*drive letter* /tempdrive:*drive letter* switches.

3. You want to create an automated installation of Windows 2000 Professional using the Setup Manager wizard for 14 computers. You want to configure the installation to run without user intervention. What three files must the Setup Manager wizard create for this scenario?

   Unattend.txt, Unattend.udf, and Unattend.bat.

4. You have just installed Windows 2000 Server and you want to use the Disk Duplication process to build more Windows 2000-based servers from this one Windows 2000-based server. What are the steps involved to complete this process?

   Install and configure the computer, install applications on the test computer, and then run Sysprep.exe on the test computer. Then, restart the computer and image it with a third party utility. Next, save the image to a shared folder or compact disc, copy the image to the target computers, start the computer, and finish the install.

5. You want to run the System Preparation Tool on a host computer, and then follow the steps to image it to another computer. However, the target computer has different hardware than the host computer. How can you run Sysprep.exe so that it accurately detects the new hardware?

   Run Sysprep.exe with the –pnp switch.

6. What services must be available on the network prior to running Remote Install Services?

   The DNS Server service, the DHCP Server service, and Active Directory.

7. You have a computer that you want to use as a client for remote installation but you are not sure whether the computer meets the requirements for a Net PC or a PXE boot ROM. What other method can you use for remote installation?

   You can also use a supported network adapter and a remote installation Startup disk.

Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 16: Implementing Windows 2000-based Servers

Contents

Overview	1
Common Implementation Features	2
Implementing a File Server	11
Implementing a Print Server	20
Implementing an Application Server	26
Implementing a Web Server	29
Routine Administration Tasks	33
Review	37
Course Evaluation	39

Microsoft®

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Rick Selby
Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP), H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor), Barbara Pelletier (S&T Onsite)
Lead Program Manager: Andy Ruth (Infotec Commercial Systems)
Program Manager: Chris Gehrig (Infotec Commercial Systems), Joern Wettern (Wettern Network Solutions)
Graphic Artist: Kimberly Jackson (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Kelly Baker (The Write Stuff)
Copy Editor: Kathy Toney (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: David Myka (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)
Testing Developer: Greg Stemp (S&T OnSite)
Compact Disc Testing: Data Dimensions, Inc.
Courseware Testing: Data Dimensions, Inc.
Production Support: Carolyn Emory (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulation and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

This module provides students with an opportunity to learn how to design a server to meet their existing network needs. They will learn about workload balancing and documentation, routine maintenance tasks, and typical server roles and needs. They will learn how to design and configure file servers and print servers. They will also learn how to implement Microsoft® Windows® 2000 Professional on client computers and how to address automated installations and customization issues.

At the end of this module, students will be able to:

- Describe common implementation features.
- Implement a file server.
- Implement a print server.
- Implement an application server.
- Implement a Web server.
- Describe routine administration tasks.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following:

- Microsoft PowerPoint® file 2152B_16.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Become familiar with all of the tasks associated with deploying a server.
- Review all of the labs for course 2152B, *Implementing Microsoft Windows 2000 Professional and Server*.

Other Activities

This section provides procedures for implementing interactive activities to present or review information, such as games or role playing exercises.

Classroom Discussion

► **To prepare for the activity**

1. Read over the discussion questions and answers.
2. Brainstorm a possible list of alternative answers and their advantages and disadvantages.

Module Strategy

- Common Implementation Features

  This section covers the common implementation features in Windows 2000. Briefly discuss differences between server roles in various size network environments and common member server types. Discuss the importance of documenting configuration and day-to-day management as a key element of server maintenance. Discuss the need for strategies and standard policies for user interface and access. Give examples of typical strategies and policies used by administrators. Discuss the overall process in implementing a member server.

- Implementing a File Server

  Discuss the unique aspects of implementing a file server. Describe the common hardware considerations and configuration priorities. Emphasize the importance in maintaining data integrity through the use of fault tolerance, organizing data for user accessibility, and establishing clear access policies for users. Also, discuss the impact of a failed file server on users in a network environment.

- Implementing a Print Server

  Discuss the unique aspects of implementing a print server. Discuss common hardware and software configurations. Review the common print management tasks and smart practices for implementing print servers, such as distributing print devices across multiple print servers.

- Implementing an Application Server

  Discuss the unique aspects of implementing an application server. Discuss the complexity and performance issues of application servers. Emphasize the impact of a failed application server on users in a network environment. Also, discuss the different variations of application servers.

- Implementing a Web Server

  Discuss the unique aspects of a Web server and the required configuration information. Discuss the interaction of a Web server in relation to other servers in the network environment.

- Routine Administration Tasks

  Describe the day-to-day administrative tasks performed on all servers. Discuss methods of implementation to achieve high reliability and server availability.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

There are no labs in this module, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about implementing file and print servers in Windows 2000.

- Common Implementation Features
- Implementing a File Server
- Implementing a Print Server
- Implementing an Application Server
- Implementing a Web Server
- Routine Administration Tasks

**********ILLEGAL FOR NON-TRAINER USE**********

As an administrator in a large network environment, you are usually responsible for implementing a server based on the network design team's decisions, but in a small networking environment, you may be expected to make those decisions. The skills and information gained in this course enable you to build member servers in a Microsoft® Windows® 2000 environment. In this module, you apply the individual skills learned in previous modules to implement common types of servers.

Other job duties of an administrator include performing day-to-day maintenance tasks, addressing policy issues, and configuring existing resources in the event of a failure. In this module, you learn about distributing workload and documentation and the types of concerns that are relevant to the common types of member servers.

At the end of this module, you will be able to:

- Describe common implementation features.
- Implement a file server.
- Implement a print server.
- Implement an application server.
- Implement a Web server.
- Describe routine administration tasks.

Common Implementation Features

Topic Objective
To list the features common to implementing member servers.

Lead-in
Looking at the overall concerns of implementing servers helps to understand the management of particular server types.

- Available Server Functions
- Balancing Workloads
- Documenting Your Support Activities
- Common Implementation Steps

**********ILLEGAL FOR NON-TRAINER USE**********

In preparing to configure and manage an individual server, your network engineer and design team will have considered the workload of each server in your networking environment, thus simplifying the management decisions about the individual server you are configuring. In a large environment, there will be network designers that will decide how to configure each server and you will need to implement a server based on their decisions. In a small company, with limited information technology staff, you may need to do it all.

Many of the skills needed to implement a network are relatively complex and can only be learned by experience, but documenting, creating checklists, and following a planned deployment are also vital to a successful implementation. When implementing a server, there are some tasks that are common to all servers and others that are specific to an individual server, based on the tasks that it will perform.

In the early stages of server installations, designing default user and group settings, and planning a strategy for giving users limited access based on their needs, simplifies management over the long-term.

Available Server Functions

Topic Objective
To list typical server functions in a network.

Lead-in
In large environments, individual servers are often dedicated to specific tasks. These are examples of some of the more traditional server functions.

- File Server
- Print Server
- Web Server
- Application Server
- Domain Controller
- DNS Server
- WINS Server
- DHCP Server

**********ILLEGAL FOR NON-TRAINER USE**********

You can configure a number of server functions on a computer running Windows 2000 Server, but the way each server is configured and the tasks it performs determine what type of server it is. A server can perform several functions, such as being a domain controller and a print server. In some cases, however, it is better to configure a server to perform only one function. Configuring a server to perform more than one task can have a negative impact in overall network performance if the server does not have enough capacity to perform multiple tasks efficiently.

Although this module focuses on the configuration concerns of four typical types of member servers, the following list summarizes some traditional server functions. Understanding the wide variety of possible server roles helps you to recognize the various roles of member servers in a larger networking scheme.

- *File server*. A file server functions as a repository for data that needs to be accessed by users across the network. While processor speed and available RAM affect the speed and efficiency of disk access, generally the safe, secure, and fault-tolerant storage of data is the greatest priority.
- *Print server*. A print server processes print requests from users to shared printers. When users send a print request to a printer, the printer sends the file to the Spool folder on the print server. The print server then sends the print job to the print device. While the Spool folder requires sufficient disk space for efficient operation, the print server relies on having sufficient RAM to process print requests efficiently.
- *Web server*. In Windows 2000, a Web server acts as a host for one or more Web sites. It may function within an intranet, as a host for an internal Web site, or on the Internet, as an external Web site. A Web server can also provide other Internet-based services, such as File Transfer Protocol (FTP) and Telnet.

- *Application server*. An application server supports client/server applications that run on the computer. With client/server applications, the client forms a request, such as a query for a database and sends the request to the server. The server performs the task or retrieves the information on behalf of the client, and then sends the information or answer back to the client. This allows less capable client computers to gain access to information that would otherwise require a new computer. It also has the added benefit of centralizing applications so that the applications and associated data can reside on and be maintained on a single computer.

  An application server can also provide other services, such as file and print services, but these tasks will affect its performance as an application server. For example, an application server may be used to provide office productivity suites (such as the Microsoft BackOffice® family, Microsoft SQL Server™, and Exchange) to a wide range of users without having to install the whole application on their desktops.

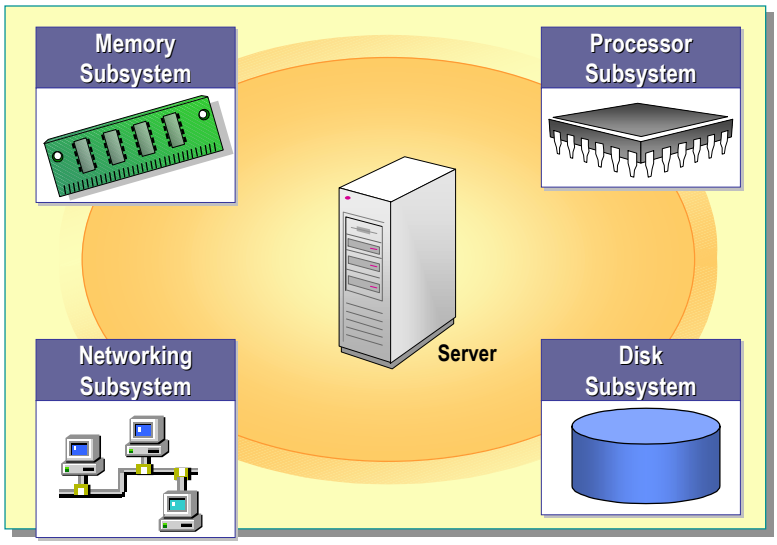
- *Domain controller*. In a Windows 2000-based domain, a domain controller is a computer running Windows 2000 Server that manages user accounts and authenticates users.
- *Domain Name System (DNS) server*. In Windows 2000, a DNS server hosts the DNS Server service, which provides host name resolution and service location, including locating domain controllers for the logon process.
- *Windows Internet Name Service (WINS) server*. In Windows 2000, a WINS server hosts the WINS Service, which provides NetBIOS name resolution and the service location for clients with NetBIOS names. This is used mainly for clients running earlier versions of Microsoft Windows NT®.
- *Dynamic Host Configuration Protocol (DHCP) server*. The DHCP server provides centralized management of Internet Protocol (IP) addresses that are used on the network. Computers configured to obtain an IP address automatically can then request and obtain a lease of an IP address from a DHCP server as part of their network initialization process. The DHCP server provides the IP addresses to other computers on the network.

Note For more information on server types, see course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Balancing Workloads

Topic Objective
To illustrate the impact of specific functions on server resources.

Lead-in
Various server roles rely on different server resources. If you consider combining server roles on a single server, you want to consider the impact each function will have on the server.



**********ILLEGAL FOR NON-TRAINER USE**********

In a larger network environment, you dedicate a server to a particular purpose. For example, you can have one or more servers acting as file servers, one or more servers whose sole function may be to act as a domain controller, and a smaller server acting solely as a print server.

However, in smaller networking environments, you can configure servers to function in multiple roles. In this case, you need to balance the roles so that no server becomes overloaded.

One way to divide these roles is to divide the various functions that servers perform into tasks that affect the generalized categories of subsystems: memory, processor, disk, and network. Although most tasks performed on a server will have some impact on each subsystem, each task impacts certain areas more than others. System performance tools should be used to determine the actual workload placed on a server to support a specific task. The following table illustrates this topic.

Typical server function	Primary subsystems impacted
Domain controller	Processor, network
File server	Memory, disk
Print server	Memory, processor
Application server	Processor, memory

(*continued*)

Typical server function	Primary subsystems impacted
Web server	Memory, disk
DNS server	Processor, network
DHCP server	Processor, network

Delivery Tip
Discuss with students possible combinations of server types that would work well together.

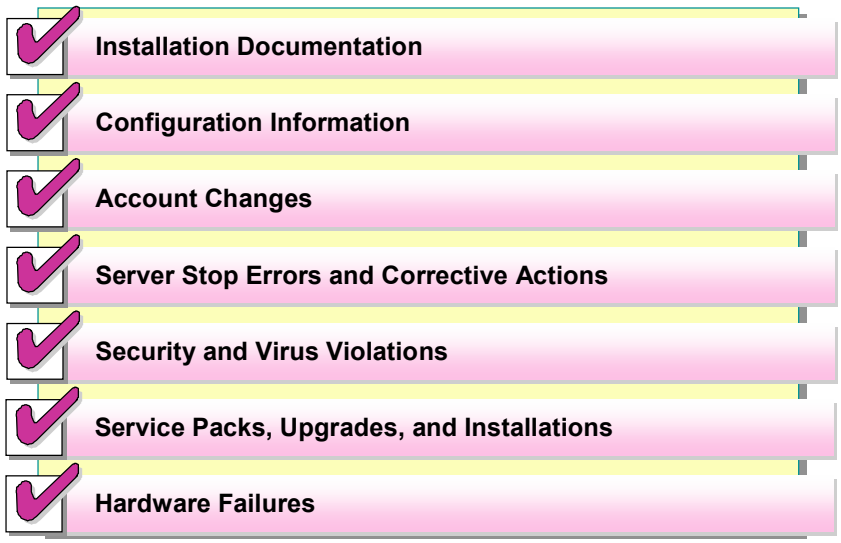
Although you plan server functions when you design the network infrastructure, you should also consider function and load balancing at an individual server level. At the individual server level, you need to decide whether a particular server will perform more than one function or be a dedicated server.

Note For more information on implementing a networking infrastructure, see course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Documenting Your Support Activities

Topic Objective
To list the types of information to document.

Lead-in
Documentation plays a vital role in the administration of a server.



**********ILLEGAL FOR NON-TRAINER USE**********

Effective documentation of your network environment often makes the difference between a well-run, secure network environment and a crisis. Documentation is one of the most important tasks that you will perform. The network should be well documented and a log book should be kept for each server, detailing any problems or changes made to a particular computer, such as applying a *hot fix*. A hot fix is a piece of software meant to replace an existing portion of the operating system that does not work properly. It is a temporary fix; the permanent replacement comes in the form of a service pack release.

Purpose Of Documentation

Many administrators find themselves unable to practice proactive server management and instead find themselves addressing one crisis after another to the detriment of their networking infrastructure. Documentation helps to prevent this self-defeating approach to network administration. Beginning the practice of documenting at an individual server level sets the precedent to continue as you move into developing an infrastructure.

Documentation Topics

You want hard copy documentation in a centralized location that describes the following:

- Installation documentation. In the event of a catastrophic server failure, you need to have installation information in order to recreate your server environment. This includes documenting licensing mode, server name, protocols, and services that you need to install.
- Configuration information. To rebuild a server, you need specific disk configuration information, such as whether you have configured fault-tolerant striped volumes and mirrored volumes. You also need configuration information for particular services installed on this server, such as DHCP scope ranges.

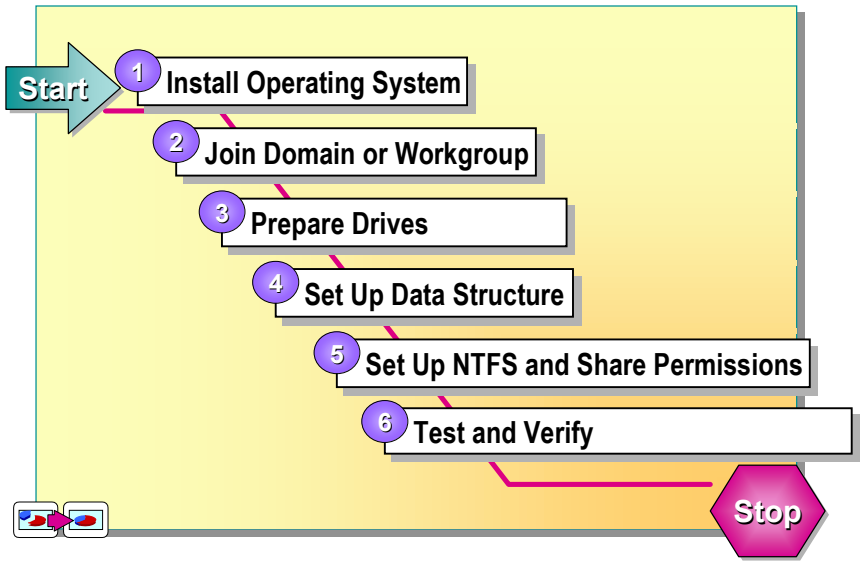
- Account changes. You need to track newly created or altered users and groups in the event that you need to undo an action or track a problem that may have occurred due to an account change that you made at some earlier point. In addition, you may want to use information from this category to track user or group activity.
- Server Stop errors and corrective actions. Despite the best precautions, servers will occasionally fail to start properly or will experience a critical Stop error that causes an interruption in service. Logging these events and the actions that you take to correct them can help in determining long-term patterns of failure or failed corrective actions.
- Security and virus violations. Each environment has different security risks. Logging security violations and the actions taken to address them enables you to proactively plan long-term policy changes and to address security risks as they occur. In addition, logging violations caused by viruses and other malicious code enables you to establish a coherent plan of action in the event of a major incident and to minimize down time in the event of an infection.
- Service packs, upgrades, and installations. Changes to a functioning server create the possibility for catastrophic failure. Documenting your changes to a server provides you with a method for undoing the installation or upgrade in the event that the change proves incompatible with your system.
- Hardware failures. You track hardware failures to plan for future resources and to consider underlying problems that may be the cause of failed hardware.

Tip Create a single documentation notebook for each server. This notebook should be a written record. Place each notebook in a location accessible to everyone who administers your server and train everyone to log server modifications into the notebook to facilitate communication between multiple administrators.

Common Implementation Steps

Topic Objective
To list the common stages of member server implementation.

Lead-in
Regardless of the type of member server you are implementing, you will consistently consider each of the following stages.



**********ILLEGAL FOR NON-TRAINER USE**********

The slide for this topic includes animation. Click the build icon on the slide or press the SPACEBAR to advance the animation.

After you verify that your equipment is on the Hardware Compatibility List (HCL), you implement a server using a number of steps. Certain tasks are performed on any computer or server, and other tasks are specific, based on the type of server being configured. Configuring security, fault tolerance, and NTFS permissions should be completed on all servers, regardless of the type server being deployed. The variation occurs in the priority given to each stage based on the given needs of the member server. The following table illustrates the basic stages involved in implementing a member server.

Stage	Process
Install operating system	Based on your networking infrastructure, decide on the most appropriate installation method. Consider the advantages and disadvantages of the methods of installation and choose the most efficient one. Many organizations have a standard installation procedure they follow on all server installs.
Join domain or workgroup	Consult with your larger information technology team for the standard server naming conventions and domain or workgroup information. Have this information available before you begin the installation process.
Prepare drives	Decide on the configuration of drives. Consider fault tolerance needs and whether this will be a hardware- or software-based solution. Many administrators, as standard policy, choose to mirror the system and boot partitions on all servers.
Set up data structure	Decide on the structure and organization of shared folders. Decide which shared folders should be drive paths and which should be mount points. Decide whether Encrypting File System (EFS) or Distributed file system (Dfs) is necessary, based on the server function.

(continued)

Stage	Process
Set up NTFS to limit access	Using a combination of user accounts, Domain global groups, domain local groups, and possibly universal groups, establish a set of security parameters to define which groups have access to various folders. Depending on server function, most administrators disable the Guest account and remove the Everyone group from their network shared folders.
Set up shared folder permissions to provide access	Decide on the appropriate shared folder permissions to provide access to groups of people. Remember that, when users access an NTFS partition across a network through a share, the most restrictive of the cumulative share and cumulative NTFS permissions are the user's effective permission.
Test and verify	Based on server function, verify that each stage of implementation works as it is intended. Try to access your server from accounts with different privileges and from different clients.

Important After implementing a member server, create a backup schedule and test your backups regularly to ensure safe and reliable data recovery for all member servers.

◆ Implementing a File Server

Topic Objective
To list the tasks for implementing a file server and present the class discussion.

Lead-in
The process of implementing a specific type of server breaks down into stages. These stages are of particular importance when implementing a file server.

- **Preparing Disks For File Servers**
- **Setting Up a Data Structure**
- **Setting Up NTFS and Shared Folder Permissions**
- **Class Discussion: Configuring a File Server**
- **Using File Servers**

**********ILLEGAL FOR NON-TRAINER USE**********

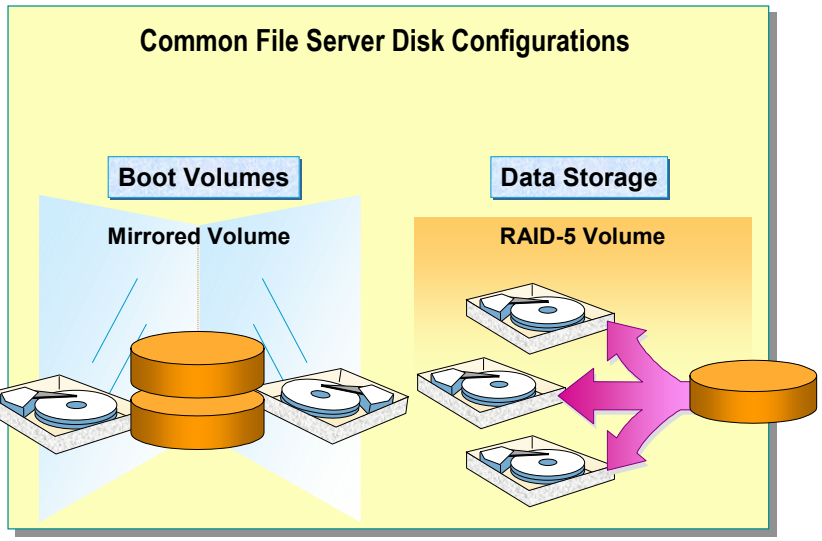
Key Points
The steps for installing a file server are more detailed than that of other server types. Cover the file server topic in detail. When covering the print server, application server, and Web server topics, refer back to the commonalities with file servers.

A file server provides access to data across the network. File servers are typically expected to be available at all times. As such, your main concerns should focus on data integrity and controlling and organizing appropriate access to data. The process of implementing a file server breaks down into several stages. After you complete these stages, you should implement a plan for keeping the server running smoothly, with a minimum amount of time when the system is unavailable, and make contingency plans in the event of a system failure.

Preparing Disks For File Servers

Topic Objective
To illustrate common file server disk configurations.

Lead-in
Fault tolerance is highly desirable in a file server because preserving data integrity is one of your primary concerns. The System and Boot partitions are often converted to mirrored volumes and data is usually stored on a RAID-5 volume to provide fault tolerance.



**********ILLEGAL FOR NON-TRAINER USE**********

With a file server, it is absolutely essential that you provide file protection, sufficient storage space, and the ability to recover files in the event of a disk failure. To do this, you should implement a fault-tolerant disk configuration that maximizes disk usage, access speed, and performance.

The Windows 2000 Setup program automatically installs disk and file management features, but you must manually configure the file server disks and shared resources to make the appropriate data available to users on the network.

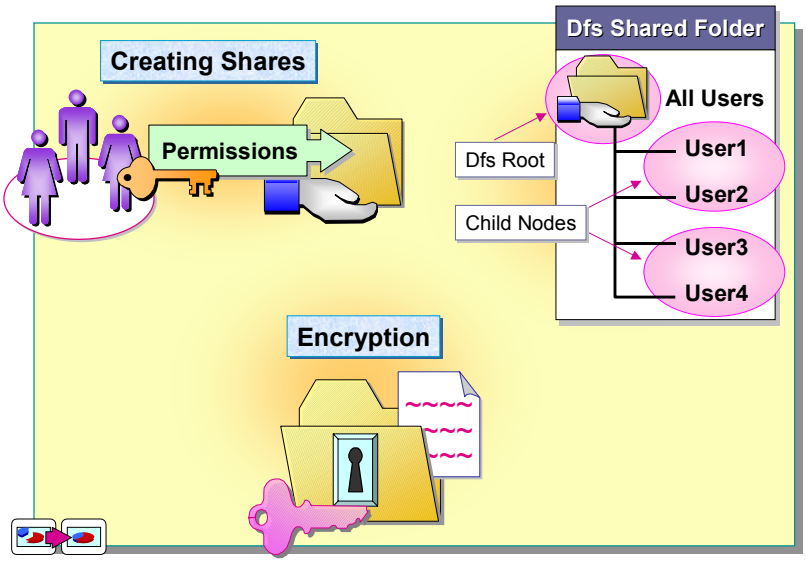
Explain why the disk subsystem is so critical for a file server. Mention that, for most companies, the data stored on a file server is the greatest asset a company has and that its loss could cause the company to fail.

With Windows 2000 you must decide on disk configuration. With a file server, you should implement fault tolerance. A typical approach is to mirror the system and Boot partition configured as a mirrored or redundant array of independent disks (RAID-5) volume. For the remainder of the disks, creating a RAID-5 striped volume allows the most efficient use of disk space while allowing full access to data in the event of a single disk failure within the striped volume.

Setting Up a Data Structure

Topic Objective
To illustrate some of the tools for structuring data for user access.

Lead-in
Windows 2000 provides great flexibility through several tools that help to structure data access for users. These tools are of particular importance when implementing a file server.



**********ILLEGAL FOR NON-TRAINER USE**********

Quiz the students to ensure that they understand what Dfs provides and that both stand-alone and domain-based Dfs can be configured. Ensure that they understand what the purpose of disk quotas and EFS is.

When implementing a file server, you will design a shared folder structure that uses drive letters and mount points to create a structure that is logical and based on intuitive names. Through the use of the Active Directory™ directory service and Dfs links, you should design a transparent organization that allows users access to files regardless of the server and folder in which the data resides. Consider implementing encryption to further protect and limit access to data.

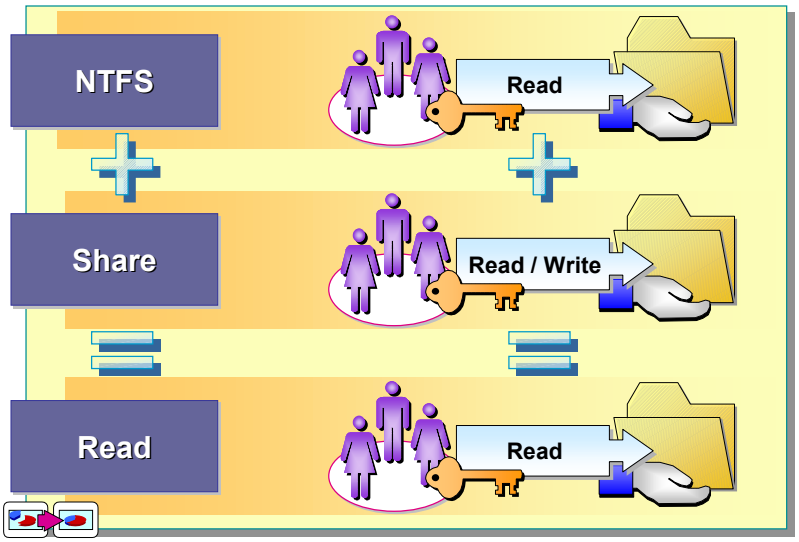
Note For more information on using Active Directory and Dfs links to design a transparent organization, see module 14, "Managing a Windows 2000 Network," in course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Enabling disk quotas and disk compression on data and archive files are important considerations when setting up data structure. Depending on whether your server merely serves files to clients or acts as a repository for user data, you may choose to limit storage.

Setting Up NTFS and Shared Folder Permissions

Topic Objective
To illustrate NTFS and shared folder permissions to provide access.

Lead-in
NTFS permissions are used to limit access. Use shared folder permissions to provide access. When you combine shared folder permissions with NTFS permissions, you get a different combination of access to files and folders.



**********ILLEGAL FOR NON-TRAINER USE**********

Remind students that Windows 2000 combines NTFS and shared folder permissions and that the most restrictive permission takes precedence.

In Windows 2000, NTFS permissions and shared folder permissions are highly adaptable and can be used to limit or grant access based on group membership.

Designing Groups

After determining default user settings, you must then design logical groups based on security as well as organizational needs. Domain local groups are the foundation of your file server because these groups provide access to the data on this server. Although there are a variety of possible strategies, the following strategy provides the most flexibility for network growth and reduces the number of permission assignments.

Delivery Tip
You may want to quiz students on the A G DL P strategy to ensure that students have an understanding of how permissions are provided to end users.

Place user accounts (A) in global groups (G), place the global groups in the domain local groups (DL), and then assign permissions (P) to the domain local groups.

Setting Up Shared Folder Permissions

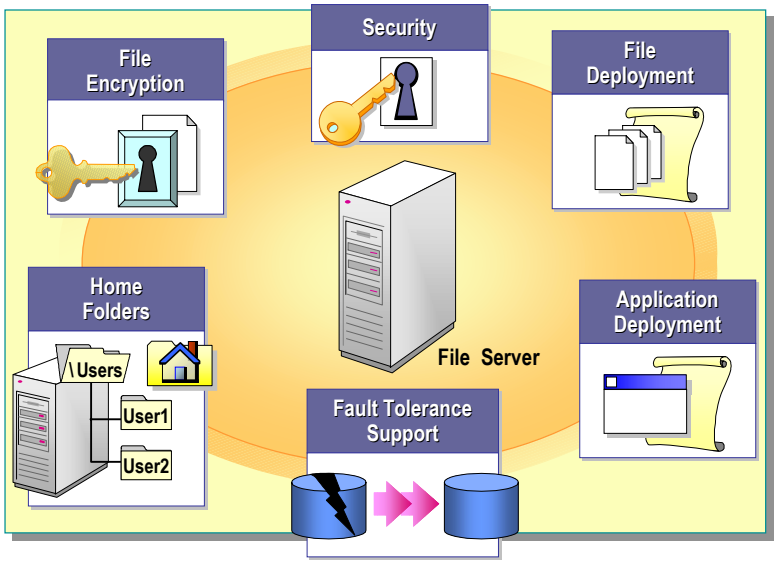
Make resources on file servers available to network users by determining which groups need access to the different resources. At this point, you have already organized users into groups and granted user rights based on group membership to limit their access. Shared folders provide users with access to resources across the network. When you combine NTFS permissions with shared folder permissions, the access permissions merge to create a combination of permissions. When accessing the shared folder across a network, remember that the user's effective rights will be the most restrictive combination of the cumulative NTFS permissions and the cumulative shared folder permissions.

As you create shared folders on the member server, you should also consider how the users interact with the shared folders. While in earlier versions of Windows NT, organization of shared folders was restricted to one configuration; Dfs and Active Directory provide administrators with the ability to use multiple schemes for organizing shared folders and making them available to users. For example, shared folders can be published to Active Directory where Dfs allows users to connect to a single share point. In this way, users can access folders on several servers across a network environment. This flexibility increases user productivity and satisfaction because users are no longer limited to non-intuitive organizational structures based on drive letters. These options also make it easier for users to locate network-based resources.

Class Discussion: Configuring a File Server

Topic Objective
To illustrate the different factors involved in implementing a file server.

Lead-in
When configuring a file server, you need to consider what features of Windows 2000 you will implement.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Discuss the following questions with students. Compare and contrast the advantages and disadvantages of different answers. Try to identify different choices administrators may make based on the environment and needs of the users.

You support a medium-sized network and need to install a new server that will be used as a file server. Users will connect to the server to install standard applications that all users require access to in addition to specific job-related applications. Users will also be provided limited space on that server to store personal data files in addition to public files related to their applications. The server is a mission-critical server for your network and the data must be available at all times.

1. Would you implement the file allocation table (FAT) or NTFS file system? Explain your answer.

   You would select NTFS because it provides file and folder security, encryption (if needed), the ability to implement software-based fault tolerance, and the ability to configure disk quotas.

2. What fault tolerance method(s) would you implement to ensure data availability? Explain your answer.

   You would base your fault tolerance selection on your available disk space and would only implement software fault tolerance if you did not have a hardware solution. With mirroring, the overhead in disk space is 50 percent; with striping with parity, the overhead is approximately 25 percent.

3. How would you organize the application folders and the data folders?

   First, you would separate your folders into an application folder and a data folder. In the application folder you would separate by common application (that everyone uses) and job-related applications. In the data folder, you would set up a public folder and provide everyone limited access to it. You would also set up private folders for individual users. You could implement domain-based Dfs to provide users with a fault-tolerant, single point connection to gain access to application and data folders.

4. What would you do to limit the amount of space available to users for data storage?

   On an NTFS partition, you would enable disk quotas, and then set a quota for all users and configure specific users with specialized quotas based on their needs. If you use disk quotas and disk compression, the quotas are based on uncompressed space.

5. How would you combine NTFS and shared folder permissions to provide limited access to users?

   For NTFS and shared folder permissions, you would remove the default permissions of the Everyone group (Full Control). You would provide access to data by creating shared folders. You would limit the access to these folders through NTFS permissions.

Using File Servers

Topic Objective
To list other possible applications of a file server.

Lead-in
A file server can also serve other purposes besides storing user files or data.

You Can Use a File Server:

- **To Store Applications for Older Clients With Limited Storage Space**
- **To Minimize Multiple Application Installations on Multiple Clients**
- **To Centralize Application Access**
  - As a distribution server for client applications.
  - To store compact disc programs for centralized access.

**********ILLEGAL FOR NON-TRAINER USE**********

You typically use a file server to provide access to data files, but you can also use them to store common applications, like a map program or file compression utility. This can prevent the need to store applications on each client machine. You can also use file servers as distribution servers and common access servers for compact disc-based applications and similar information-based applications.

Application Storage Server

In some cases, such as when working with older client computers that have limited disk space, you may choose to install client applications to a shared folder on the file server and enable clients to connect to the shared folder and use these applications from the client desktop. The advantage to this approach is two-fold. You can limit access to a particular application based on network access permissions and by implementing a disk duplication procedure, and you can also eliminate the need for multiple installations on individual clients. Storing client applications on a file server also allows these older client computers access to multiple applications despite limited storage capacity on the clients.

Distribution Server

You may use part of your file server as a *distribution server*. A distribution server is a type of file server that is used to facilitate distribution of applications. As a distribution server, the server would function as a distribution point from which to install client applications. This eliminates the need for distribution of installation software throughout a building and allows users to install applications based on their privileges.

Centralized Application Access

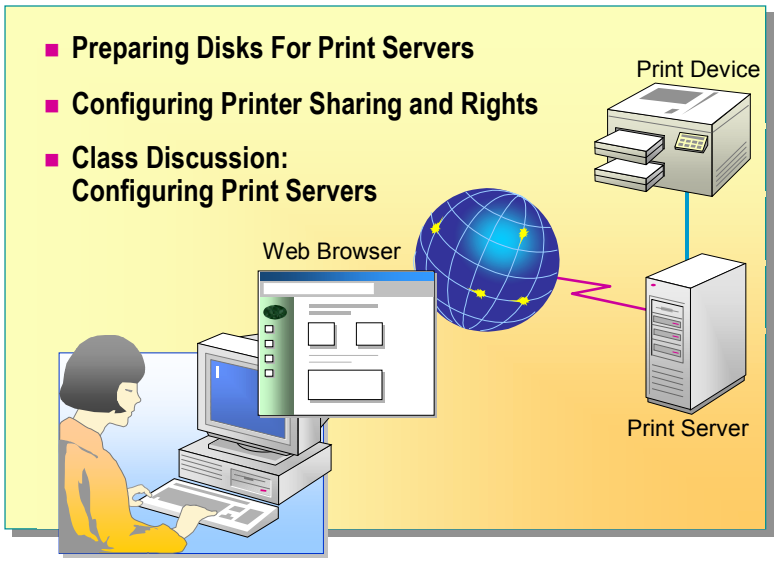
Lastly, you may choose to use a file server as an access point for programs that are usually stored on compact disc, such as encyclopedia and atlas programs. Although you can share the CD-ROM drive directly from the server, improved performance often occurs by copying the CD-ROM to a network shared folder and providing access through the server directly. Although this uses more storage space on a server, you improve performance by eliminating the bottleneck created by slower CD-ROM access speeds. The advantage of using a file server as an access point for CD-ROM is that it eliminates the need for software to travel throughout the building. It also enables you to monitor usage and to provide access to multiple users through a single installation process.

Important In using a file server for these applications, it is essential that administrators implement a third party application or program, such as Microsoft System Management Server, that allows you to monitor and limit the number of users to ensure that the organization complies with all licensing and copyright laws.

◆ Implementing a Print Server

Topic Objective
To describe the primary implementation stages of configuring a print server and to present the class discussion.

Lead-in
Provided that you reserve enough disk space and memory to handle print jobs, print servers do not take a lot of resources or time to manage.



**********ILLEGAL FOR NON-TRAINER USE**********

You use a print server to manage the print requests submitted by users on your network. This allows multiple users to print documents on the same print device.

To implement a print server, install the operating system, join the domain or workgroup, configure your disks, set up your printers and assign permissions. You may also choose to implement a Web-based user interface to provide access to the printers. The printer devices can be attached directly to the print server or connected directly to the network. Many organizations delegate day-to-day management tasks to users located in close proximity to the individual print devices.

In addition to configuring the computer and print devices, you should also be familiar with the process for fixing jammed print devices and for scheduling regular maintenance for these devices. You must also plan for the consumption of printer materials such as paper and toner cartridges.

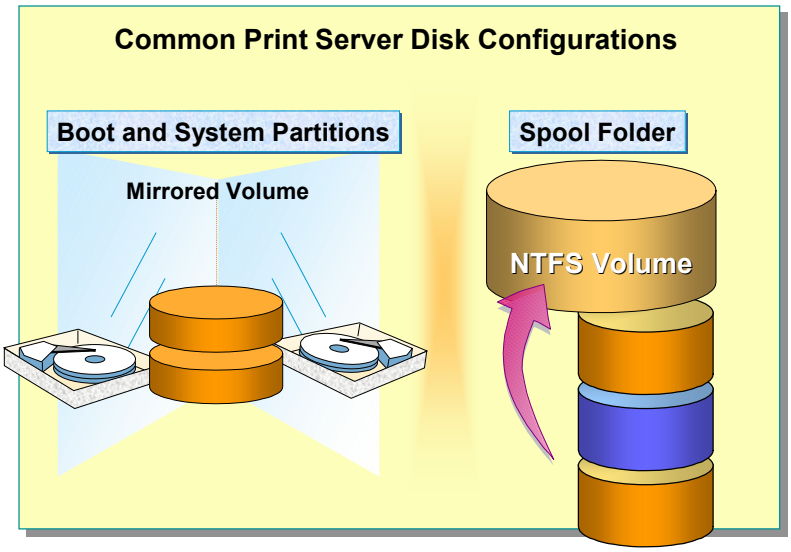
Even though managing printers can consume a large portion of the day, you can reduce this time by configuring a print server properly and granting the right to manage the printer to a local user. This allows the total time spent managing printers to be greatly reduced while providing the client with better printer support and service.

Tip Many administrators choose to have multiple print servers in a network environment so that in the event of a single print server failure, users can still print to other print devices on the network. Because print servers do not require a large amount of server resources, administrators frequently combine print servers with other server roles, or reconfigure older servers as print servers when they are retired from other uses.

Preparing Disks For Print Servers

Topic Objective
To illustrate common print server disk configurations.

Lead-in
While fault tolerance is desirable for any Startup disk, fault tolerance is not essential to print servers. Moving the Spool folder to a separate physical disk, however, will enhance performance.



**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Discuss the practice of moving the Spool folder to a separate physical disk to improve performance. Make sure the students understand why placing the Spool folder on a separate drive from the operating system protects the operating system and improves performance.

Print servers must have sufficient disk space and RAM to manage print jobs. Ideally, plan to have a minimum of two disks, one for the operating system, the startup files, and the paging file, and another one that holds the Spool folder. This isolates the Spool folder from the operating system, which increases performance and improves stability. To increase efficiency, add one or more drives for the paging file.

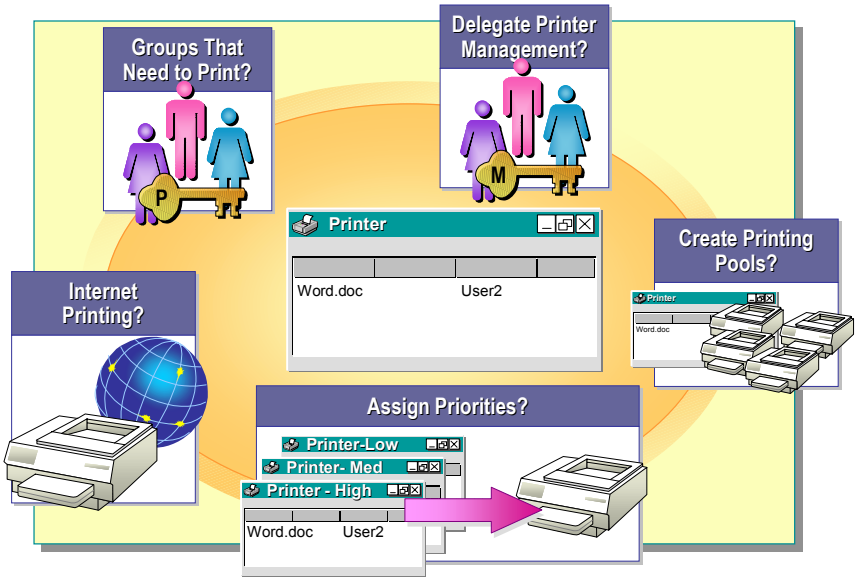
Print servers create a print queue to manage print requests. Documents can easily be 20 megabytes (MB) in size if they include embedded graphics. As such, you should use disk space on a drive other than the one being used for the operating system. This helps ensure you do not use all the free disk space on the system or boot partitions, which can cause difficulties with the swap file. If you configure the print queue on the same disk as the operating system, Windows 2000 will not have sufficient disk space to write the swap file, which can cause the computer to crash.

In general, you should monitor print queues daily to make sure that they are running and track the drive space used for print queues.

Configuring Printer Sharing and Rights

Topic Objective
To illustrate the issues surrounding printer sharing and management.

Lead-in
When implementing a print server, you will share the printers from the server and then provide user rights to different groups. You may also choose to implement Internet printing.



**********ILLEGAL FOR NON-TRAINER USE**********

Although in some networking environments you may not choose to modify access to printers, Windows 2000 allows you to modify access according to groups and to establish printing priorities or printer pools.

Key Points
Remind the students of the terminology used with printing in Windows 2000. Make sure that they understand the concepts of creating multiple printers, setting different priorities on each, and the purpose of a printer pool.

After installing and sharing the printer, you need to decide who will be allowed to use the printer, and who you want to designate to maintain the printer. The following table describes some of the decisions you must make, and some of the criteria you should consider to make those decisions.

Decision	Rational
Which groups need to gain access to this printer?	Most users are given the ability to print to the printer in question in addition to managing their own documents.
Do you want to delegate printer management?	You may choose to make one user located in the general physical vicinity of the print device a power user with the ability to manage all print jobs on that printer or print server.
Do you need to create a printer pool?	Some environments require multiple print devices in a single physical location. If this is the case, create a printer pool where a single printer is associated with multiple print devices to allow users to make maximum use of the devices. If one print device is busy, print jobs can be routed to another print device.

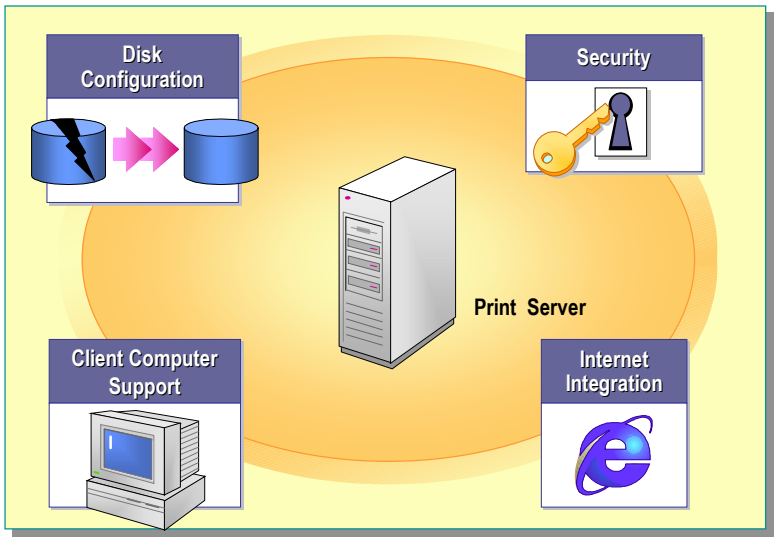
(continued)

Decision	Rational
Do you want to assign different print priorities based on group membership?	You may want to create multiple printers and associate them with a single print device. By doing this, you can then assign different priorities to each printer and assign different groups the right to print to the different printers. The end result is that the print requests of a particular group always take priority over another group.
Do you want to use Internet printing and take advantage of Active Directory to simplify printer access for your users?	You may choose to use Windows 2000 Internet printing and Active Directory to create a more user-friendly interface for managing print jobs. For example, create a Web page that includes a map of your building and the location of all available print devices. Users can then click on the icon representing the print device that they want to use to print a document.

Class Discussion: Configuring Print Servers

Topic Objective
To illustrate the different factors involved in implementing a print server.

Lead-in
When configuring a print server, you need to consider what features of Windows 2000 you will implement.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Discuss the following questions with students. Compare and contrast the advantages and disadvantages of different answers. Try to identify different choices administrators can make based on the environment and the needs of users. During the classroom discussion, try not to lead the students to the answers, but encourage them to review previous modules to find answers to the questions.

You are installing a computer running Windows 2000 Server that will act as a print server for three print devices for the Research and Development group. One of the print devices will be connected to a printer port on the back of the computer. The other two print devices have network adapter cards installed, but will be managed by printers on the server you are installing.

1. How could you minimize your workload while providing the Research and Development group with better support for the printers you are installing in their area?

   You could assign one or two local users to act as print managers for the printers in that area. You need to train them on using the print devices in addition to installing printers, managing printers, and performing simple print device maintenance tasks, such as replacing toner cartridges and clearing paper jams.

2. What could you do to help protect the partition or volume the operating system is on? Could this have any effect on performance? If so, would it be a negative or positive impact?

   You could place the Spool folder on a separate partition or volume from the operating system. To increase performance, you would place the Spool folder on a different physical disk.

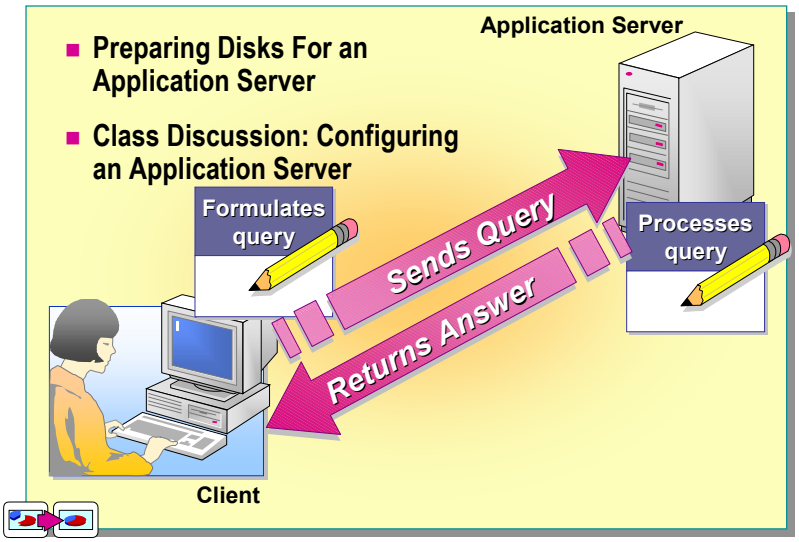
3. If you were going to upgrade some of the components in the print server, which ones would you consider upgrading first? Why?

   The disk and memory subsystems would be the first two subsystems to consider upgrading. Print jobs are spooled on a disk while waiting to be printed, and must be placed in memory to be sent to a print device. Therefore, you would want to make sure you had enough disk capacity to store print jobs and enough memory for the system to perform efficiently. Printing is not processor-intensive and does not place a significant burden on the network subsystem; therefore those two subsystems would be secondary when considering an upgrade.

◆ Implementing an Application Server

Topic Objective
To illustrate primary elements of implementing an application server and to present the class discussion.

Lead-in
Application servers host client/server applications. Processing occurs on the server instead of the client computer.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Provide the students with an overview of how an application server works and what overall benefits this type of server provides.

An application server hosts client/server applications. On an application server, the server performs the computation on behalf of the client computer's request. This offloads the processing activities from the client computer to the server, allowing you to use older or less powerful clients for processor-intensive tasks.

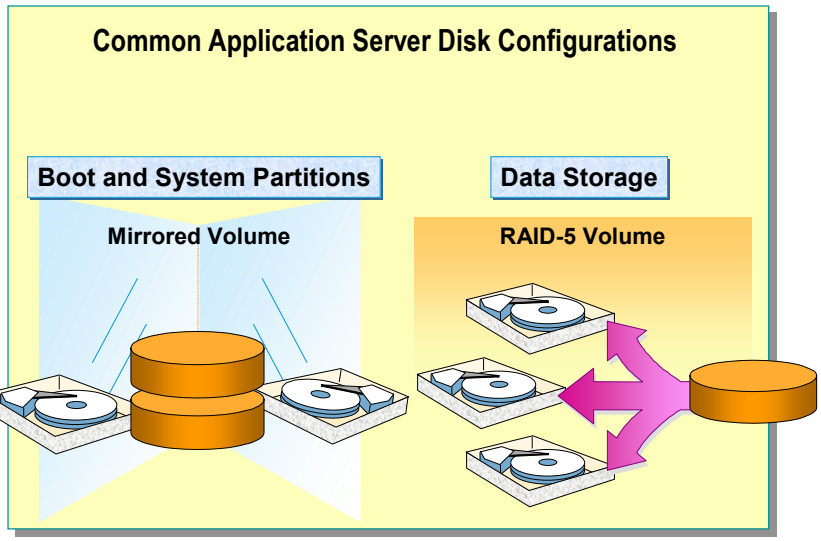
For example, a client computer accessing a SQL database on a Microsoft SQL Server™ runs a program that provides a graphic interface on the client computer. The client queries the SQL server. The SQL server performs the query on the database, and then sends the answer back to the client computer.

Application servers rely on the processor and memory subsystems to perform well. Having an application server perform other network tasks, such as acting as a domain controller or print server, can affect its ability to efficiently perform as an application server.

Preparing Disks For an Application Server

Topic Objective
To illustrate common application server disk configurations.

Lead-in
Fault tolerance is highly desirable in an application server because preserving data integrity is one of your primary concerns. Boot and system partitions are often converted to mirrored volumes and applications are usually stored on a RAID-5 volume to provide fault tolerance.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Emphasize the similarities of and differences between a file server and an application server. With both, data integrity is paramount, but the responsibility of backing up and maintaining the data may be different.

Initially, configuring an application server closely parallels configuring a file server. Data integrity is paramount. The same disk configuration concerns affect both types of member servers. With an application server, the data backup is critical, but is typically the responsibility of the application administrator.

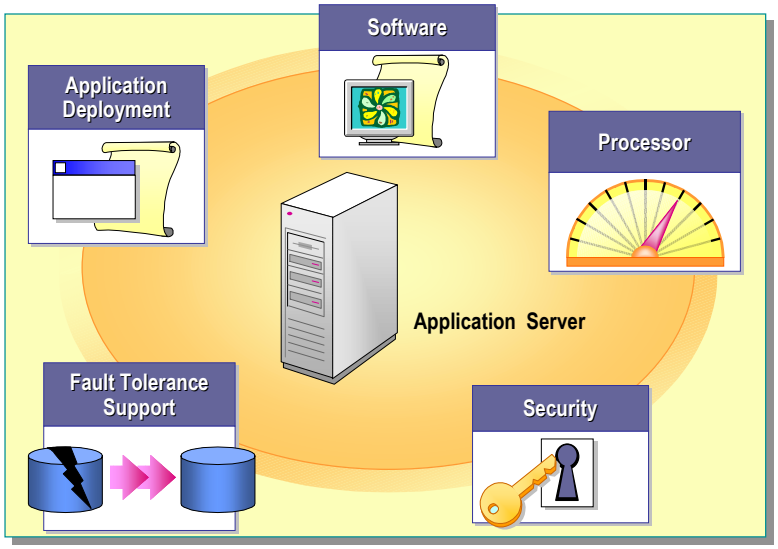
As with a file server, it is absolutely essential that you provide file protection, sufficient storage space, and the ability to recover files in the event of a disk failure. However, the backup process is quite different from that of a file server. An application server requires several backups a day to account for the more fluid exchange of data. Most client/server applications are written to be able to take full advantage of a system with multiple processors. Therefore, adding additional processors as opposed to adding a single processor might be a good idea.

You need to determine which groups in your organization require access to which applications. You also need to secure the applications so that no user can accidentally delete or corrupt application files. Typically in a large environment, you will have an individual administrator that will resolve security issues for each client/server application. In a smaller environment, you may need to design security for these applications.

Class Discussion: Configuring an Application Server

Topic Objective
To illustrate the different factors involved in implementing an application server.

Lead-in
When configuring an application server, you need to consider what features of Windows 2000 you will implement.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Discuss the following questions with students. Compare and contrast the advantages and disadvantages of different answers. Try to identify different choices administrators may make based on the environment and needs of the users.

You have an application server that will be used to support an SQL database. The database provides the Order Processing group with access to inventory records so that they can fulfill sales orders. You are also installing a server that will be used as a file server. One computer is a dual processor Pentium computer with four 4-gigabyte (GB) hard disks, and the other computer is a single processor Pentium with four 4-GB hard disks.

1. Which computer would you choose to install as the file server, and which would you use as the application server? Why?

   You would use the dual processor computer as the application server because an application server is more processor-intensive.

2. Given the number of disks available, how would you suggest the disk drives be configured? Why?

   The system and boot partitions should be mirrored on two drives, and a stripe with parity should be created across the three disks. This would provide fault tolerance and efficiency when retrieving data.

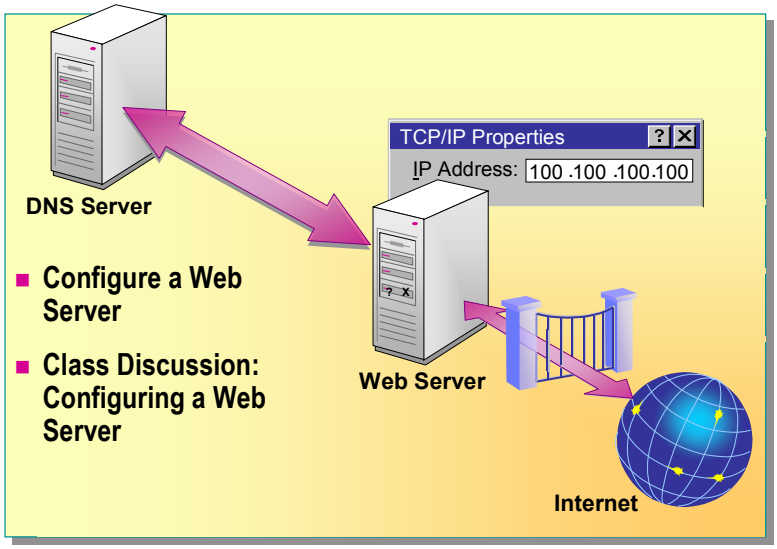
3. To create a backup schedule for the application server, would you suggest the same backup schedule as that of a file server? Why or why not?

   The data should be backed up several times a day. Because the data changes throughout the day and is used to determine the amount of stock on hand, you would want to be able to restore data to a point more current than the previous day.

Implementing a Web Server

Topic Objective
To illustrate the criteria for configuring a Web server and to present the class discussion.

Lead-in
Web servers act as intermediaries between your organization's intranet and the Internet. Configuring a Web server is dependent upon having other services configured and working on your network.



**********ILLEGAL FOR NON-TRAINER USE**********

The process for creating a Web server closely parallels that of creating a file server. As with other member servers, you begin by installing the operating system, joining the domain or workgroup, and configuring the disks. The primary concerns of a Web server consist of installing and configuring the appropriate services and setting up appropriate access.

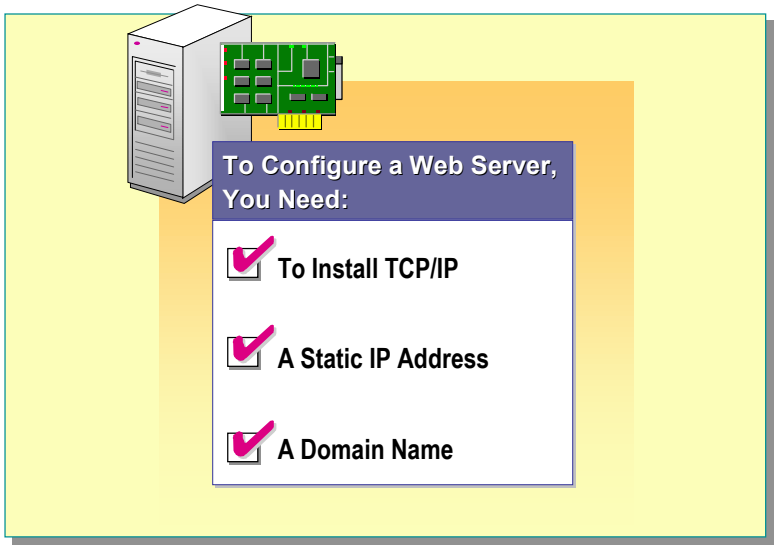
A Web server provides Web page content that essentially fulfills a client's request for files. A Web server also processes form requests to access large client/server databases on behalf of the client. Windows 2000 Server and Advanced Server integrate Web publishing into the operating system with a built-in Web server, Internet Information Services (IIS) 5.0. The integrated Web publishing environment provided by Windows 2000 makes it easier for an organization to publish and host Web content over a corporate intranet or the Internet.

IIS installs by default as a networking service when you run the Windows 2000 Setup program. IIS is designed to support multiple Web server scenarios, including simple Web sites on a corporate intranet. It can be installed on a Web server on the Internet; however, it can also be installed to provide Web access to internal resources and to support Internet printing.

Configuring a Web Server

Topic Objective
To list the criteria for configuring a Web server.

Lead-in
In order to configure a Web server, you must implement TCP/IP, the Web server must use a static IP address, and a DNS server must be present on your network.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Emphasize the significance of having each of these configured. Ask whether there are instances where any of the three might not be needed.

You need the following network services and information to successfully implement IIS 5.0 on a member server:

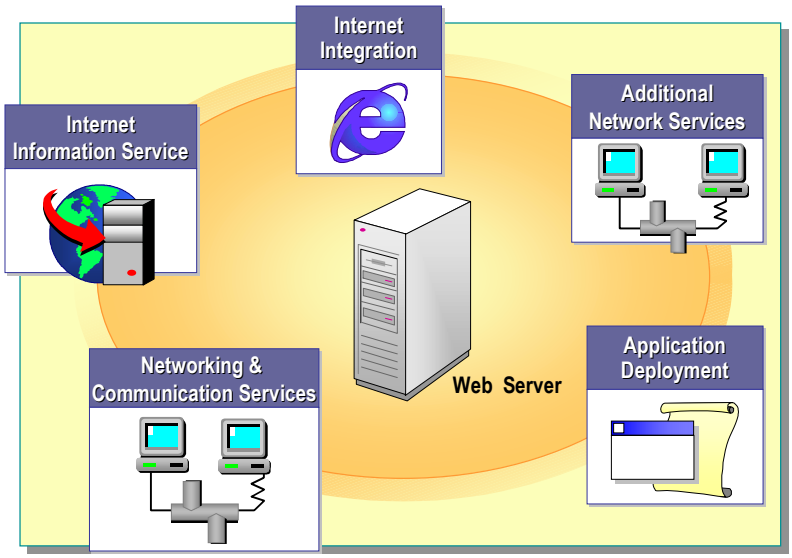
- *Transmission Control Protocol/Internet Protocol (TCP/IP)*. You must install TCP/IP before installing IIS to provide the connectivity necessary for transmitting data.
- *Internet Protocol (IP) address*. You must use a static IP address for your server.
- *Domain name*. If you intend to have users access your site by a domain name instead of an IP address, you will need to have a Domain Name System (DNS) server configured on your network to provide name resolution.

Note For more information on configuring a Web server, see module 4, "Configuring Web Services," in course 2153A, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Class Discussion: Configuring a Web Server

Topic Objective
To illustrate the different factors involved in implementing a Web server.

Lead-in
When configuring a Web server, you need to consider what features of Windows 2000 you will implement.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Discuss the following questions with students. Compare and contrast the advantages and disadvantages of different answers. Try to identify different choices administrators can make based on the environment and needs of users.

You have been asked to install a server that will be used as an internal Web server. This server will provide your internal network users with Internet printing support and access to Web-based company policies, documentation, and help documents for performing daily tasks. The human resources department will perform the Web page management, but you will be responsible for configuring Internet printing.

1. If you installed the server with the standard networking components, would you need to install any additional components in order to configure this server? Why?

   No. TCP/IP and IIS are installed by default. You might need to perform additional configuration of the server, but not install additional networking components.

2. Two of the printers that you need to configure for Internet printing are connected directly to the network. Can you still configure the printers to be managed by this server?

   Yes. The printers do not need to be directly connected to the computer in order to use Internet printing.

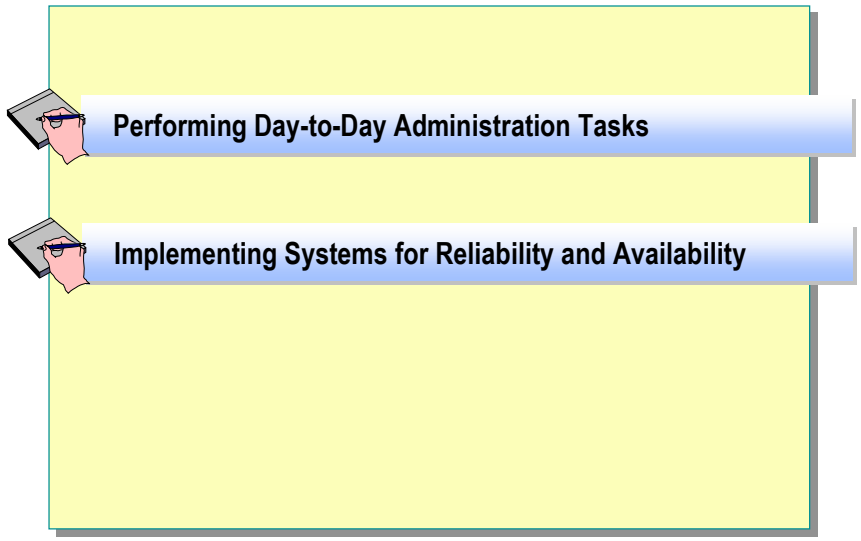
3. Do the clients need to have IIS installed on their computers to take advantage of Internet printing? What information does the client need in order to locate and connect to the Web server?

   No. The clients use a Web browser, such as Internet Explorer 5, to connect to the Web server that is managing the printers. The clients must have the computer name or IP address of the printer (or DNS must be implemented on both network and clients and the Web server must be configured to use DNS) in order for the client to locate the Web server.

Routine Administration Tasks

Topic Objective
To list the major categories of network administration.

Lead-in
Server administration consists of day-to-day administrative tasks in addition to implementation of systems to ensure reliability and availability.



**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Ask the students what tasks they think should be performed on a daily basis in order to maintain high reliability and availability. Emphasize the need to keep documentation current.

Administering Windows 2000 involves post-installation and day-to-day tasks. Administrators find most of their time is spent on day-to-day administration tasks. These day-to-day tasks can be broadly classified into five different categories. In addition to these daily tasks, some administrators strive to implement a system of high reliability and availability. In order to accomplish this, the administrator develops long-term strategies and tasks.

Performing Day-to-Day Administration Tasks

Topic Objective
To list the different categories of day-to-day server administration tasks.

Lead-in
Day-to-day server administration breaks down into five general categories of tasks.

**********ILLEGAL FOR NON-TRAINER USE**********

Delivery Tip
Ask students what other tasks they might add to the list.

Administrators face a number of routine tasks they must perform in order to keep network servers operating efficiently. You will find that as your experience and skills grow, your list of routine tasks will grow as well.

The following table describes some of the day-to-day tasks associated with maintaining the network.

This category	Includes these 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 access necessary resources.
Printer administration	Setting up local and network printers and troubleshooting common printing problems. This ensures that users can connect to and use printer resources easily.
Security administration	Planning, implementing, and enforcing a security policy for protecting data and shared network resources, including folders, files, and printers.
Monitoring network events and resources	Planning and implementing a policy for tracking security breaches, and monitoring and controlling resource usage.
Backing up and restoring data	Planning, scheduling, and performing regular backups to protect important data. Having a good backup plan ensures that you can quickly locate and restore critical data.

Tip Experienced network administrators sometimes develop a monthly calendar of routine tasks that incorporate tasks from each of these categories to help track and implement each responsibility. Neglecting any one of these categories can lead to decreased performance, security risks, or failed servers.

Implementing Systems for Reliability and Availability

Topic Objective
To list the primary features of implementing systems for reliability and availability.

Lead-in
Planning for a system failure allows you to be much better prepared in the event of a problem.

**********ILLEGAL FOR NON-TRAINER USE**********

Key Points
Even if you are not responsible for a specific task, such as designing the network, you should have a good understanding of how the entire network functions and who is responsible for the different areas. Emphasize that recovery from a failure is made easier by proper documentation. Ask the students what the benefits are of performing a test restore from tape.

In general, the larger the network environment, the more resources you have on hand to meet and resolve problems as they arise. Administrators in small to mid-size networks often characterize their job as one of reacting to crisis. Administrators of larger networking environments automate many of their routine administrative tasks and therefore have more time to plan for contingencies.

As an administrator, your goal is to maintain servers that achieve high reliability and availability. Regardless of server function, you will want your servers to be reliable and to provide their intended service to your users, consistently and accurately. Reliability and availability center around the following skills and activities: good planning and design, automated monitoring and analysis, a skilled help desk, accurate recovery procedures, and an analysis of root causes.

Planning and Design

You should plan operational procedures using clearly defined availability goals. In addition, you should base these goals on the relative importance of the business functions that you support.

Monitoring and Analysis

Use some form of automated procedure to monitor the availability of your servers. Automated monitoring is a key best practice that enables identification of failure conditions and potential problems. Monitoring can also help reduce the time needed to recover from a failure.

One reason monitoring is so important is the simple fact that operators need to know a failure has occurred before they can initiate procedures to restore service. Monitoring alerts administrators to these problems.

Additionally, some administrators choose to monitor the performance characteristics of their servers in order to spot usage trends. This is a proactive best practice that allows you to identify the conditions that contribute to system failure and take action to prevent those conditions from occurring. Monitoring strategies vary depending on the type of service that the customer provides.

Help Desk

In the event of a failure, you should develop a clearly defined process to obtain help and direct problems to increasingly skilled groups of people.

Recovery Procedures

Naturally, you should develop procedures to prevent failures that lead to loss of data. These procedures will enable you to quickly and correctly recover from failures. Exact recovery procedures are unique to the type of service each server performs; however, common recovery strategies include keeping a stock of spare hardware parts and multiple copies of critical data in read-only format.

Root Cause Analysis

Many administrators agree that determining the root cause of failures instead of treating symptoms is important. However, few administrators have time to implement a thorough analysis of root causes. Developing analytical skills that allow you to analyze problems and their root causes will help you recover from computer problems more quickly.

Note For a complete study on implementing systems for reliability and availability, see the white paper, *Microsoft Windows NT Product Group High Availability Operations Guide*, located on the Web page on the Student Materials compact disc.

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Common Implementation Features
- Implementing a File Server
- Implementing a Print Server
- Implementing an Application Server
- Implementing a Web Server
- Routine Administration Tasks

**********ILLEGAL FOR NON-TRAINER USE**********

1. What are some of the tasks that are common to any server deployment?

   Tasks that are common to any server deployment include installing the operating system, joining a workgroup or domain, preparing the disk drives, configuring the data structure on the partitions, and configuring NTFS and shared folder permissions.

2. You are installing a file server and have a limited amount of disk space available. You have ordered a hardware RAID-5 solution, but will not have it for approximately three months. You want to implement some form of software disk fault-tolerance, but cannot afford to lose half of your available disk space implementing mirroring. What other option is available?

   You can implement disk striping with parity (RAID-5). The amount of usable disk space available when implementing striping with parity is approximately 75 percent of the overall disk space.

3. You are installing a print server. What is one way to ensure that a print spool file cannot exceed a certain size? How can you configure the Spool file to increase overall performance of the print server?

   You can place the Spool file on it's own partition. This will limit the amount of space the spooler can use to the partition size. By placing the spool file on a separate disk drive, you would increase overall system performance.

4. You need to configure a file server, a print server, and an application server that will be running SQL 7.0. You only have two computers to perform these three tasks. You need to decide which servers will perform these tasks. Which two tasks would you implement on the same computer?

   You would configure one server to support the file server and print server tasks, and the other server to support the application server task.

5. You are configuring IIS on your print server so that users can use Internet Explorer 5 to view the printers and manage the documents they are printing. What three things must be configured for the server to support this task?

   You must configure the server with the TCP/IP protocol, configure the server with a static IP address, and if the users will connect to the server by its computer host name, you must configure the clients and servers to use DNS for name resolution.

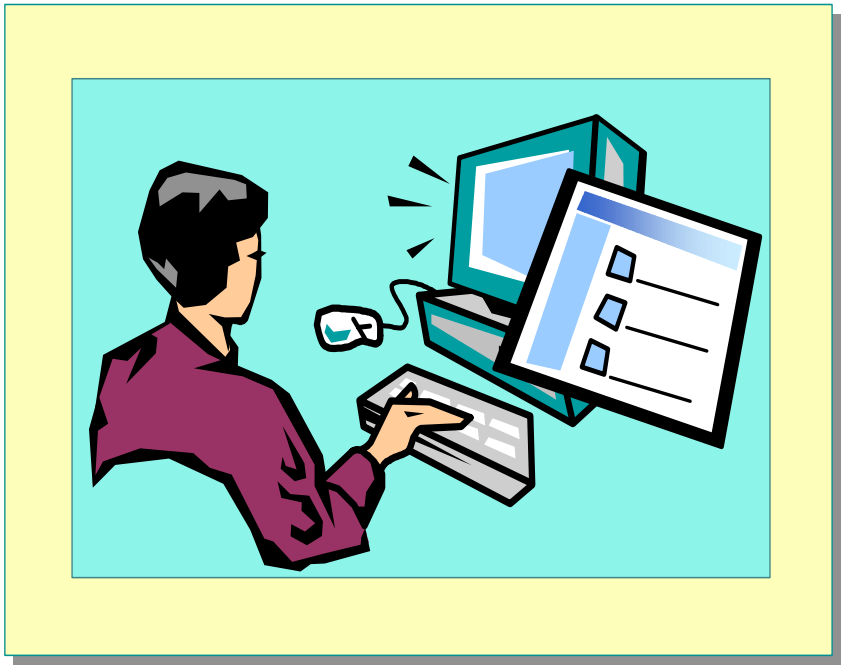
6. You have hired a new employee that will help maintain a number of servers. What are some of the day-to-day tasks you would expect that employee to be able to perform to support the server?

   You would want the employee to be able to administer users and groups, manage printers, configure security settings, monitor network events and resource utilization, and backup and restore files.

Course Evaluation

Topic Objective
To direct students to a Web site to complete a course evaluation.

Lead-in
Go to the Web site listed on this page to complete a course evaluation.



**********ILLEGAL FOR NON-TRAINER USE**********

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

To complete a course evaluation, go to http://www.metricsthatmatter.com/survey.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.